

**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

№ 7 (липень)

Київ – 2026

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. К., 2026. № 7 (липень). 117 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 гібридних 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 онлайн-новими інформаційними ресурсами можна за адресою: проспект Голосіївський, 3, м. Київ, 03039.

ЗМІСТ

Світові тенденції в галузі кібербезпеки	4
Сполучені Штати Америки, Канада та Мексика	22
Країни ЄС та Великобританія.....	31
Австралія та Нова Зеландія.....	39
Китай, Індія, Японія, Південна Корея та країни Іndo-тихоокеанського регіону	43
Ізраїль, Туреччина та країни Близького сходу	46
Країни Африки	48
Кібервійни та протидія зовнішній кібернетичній агресії.....	53
Кіберзахист критичної інфраструктури.....	60
Кіберзахист промислових об'єктів та об'єктів будівництва.....	63
Кіберзахист закладів охорони здоров'я	64
Захист персональних даних та соціальні мережі	67
Масштабні витоки персональних даних	67
Кібербезпека Інтернету речей. Штучний інтелект	68
Штучний інтелект, як інструмент боротьби із кіберзлочинністю	80
Штучний інтелект, як зброя кіберзлочинців	82
Кіберзлочинність та кібертероризм.....	83
Діяльність хакерів та хакерські угруповування.....	94
Вірусне та інше шкідливе програмне забезпечення	97
Фішингові атаки	108
Операції правоохоронних органів та судові справи проти кіберзлочинців.....	110
Технічні аспекти кібербезпеки	111
Виявлені вразливості технічних засобів та програмного забезпечення	111
Технічні та програмні рішення для протидії кібернетичним загрозам	116
Основи кібергігієни.....	117

«...Кібербезпека залишається одним із найперспективніших ринків праці в сфері технологій, що характеризується стабільним попитом, значним дефіцитом кадрів та великою кількістю вакансій, відкритих для кандидатів, які працюють віддалено. Оскільки ця галузь пропонує безліч шляхів входження, оптимальний варіант залежить від досвіду людини, її бюджету та часових рамок. Сертифікація часто є найшвидшим варіантом і особливо корисна для тих, хто вже має певні технічні знання та хоче швидко спеціалізуватися; вона дає найкращі результати, коли її обирають стратегічно з огляду на цільову посаду, наприклад, починаючи з базових сертифікатів, а потім додаючи більш спеціалізовані... Отримання офіційного диплома займає більше часу і коштує дорожче, але забезпечує глибші технічні знання і часто є кращим варіантом для більш просунутих посад, пов'язаних з архітектурою, управлінням або керівництвом, особливо в галузях, що підлягають регулюванню. Буткемпи пропонують золоту середину, забезпечуючи інтенсивне, орієнтоване на роботу навчання з практичними заняттями та підтримкою у кар'єрному зростанні, що робить їх практичним вибором для тих, хто змінює сферу діяльності та прагне структурованого й відносно швидкого шляху до посади початкового рівня в галузі безпеки. На практиці багато людей з часом поєднують ці шляхи, але найефективнішою стратегією є обдуманий вибір кваліфікації, виходячи з конкретної професійної мети, оскільки роботодавці, що пропонують дистанційну роботу, шукають чітких, надійних і підтверджених навичок, а не лише ентузіазму...» (*Certs, Degrees or Bootcamps: The Real Roadmap Into Remote Cybersecurity // TechRound* (<https://techround.co.uk/cybersecurity/certs-degrees-bootcamps-real-roadmap-remote-cybersecurity/>). 06.07.2026).

«У міру того як кіберзагрози стають дедалі більш витонченими — використовуючи тактики маскування, такі як безфайлове шкідливе програмне забезпечення, крадіжка облікових даних та складні стійкі загрози — традиційні реактивні заходи безпеки, такі як брандмауери та антивірусне програмне забезпечення, вже не є достатніми. Щоб протидіяти цьому, організації впроваджують «полювання на загрози» — проактивну практику кібербезпеки, в рамках якої аналітики активно шукають приховані загрози, підозрілу поведінку та індикатори компрометації в мережах, на кінцевих точках та в хмарних середовищах, не чекаючи на спрацьовування автоматичних сповіщень. Виходячи з припущення, що зловмисники, можливо, вже проникли за периметр, «полювання на загрози» значно скорочує час перебування зловмисників у системі, мінімізує потенційний збиток та виявляє «сліпі зони» безпеки...

Процес пошуку загроз має чітко структурований характер і, як правило, починається з гіпотези, що ґрунтується на аналітичних даних про загрози або відомих моделях поведінки зловмисників. Далі команди з безпеки збирають обширні телеметричні дані, аналізують шаблони на наявність аномалій, досліджують підозрілу активність, щоб виключити помилкові спрацьовування, та

застосовують протоколи оперативного усунення порушень. Зрештою, результати цих пошуків використовуються для вдосконалення та поліпшення майбутніх правил автоматичного виявлення. Для проведення таких розслідувань фахівці з пошуку загроз застосовують різні методології — зокрема, підходи, що базуються на аналітичних даних, аналітиці та поведінці, — спираючись на надійний набір інструментів безпеки, включаючи платформи SIEM, XDR, EDR, NDR та SOAR...

Незважаючи на свою ефективність, ручний пошук загроз стикається зі значними оперативними викликами, серед яких — «втома від сповіщень», розрізнені «силоси» даних та загальногалузевий дефіцит кваліфікованих фахівців. Щоб подолати ці перешкоди, штучний інтелект революціонує цю галузь, швидко корелюючи величезні масиви даних, виявляючи ледь помітні аномалії в поведінці та різко зменшуючи кількість помилкових спрацьовувань. Користуючись цією технологічною зміною, постачальник послуг з кібербезпеки Saseon пропонує уніфіковану платформу Open Threat Management на базі штучного інтелекту, яка об'єднує ці складні функції безпеки. Завдяки інтеграції аналітики на базі штучного інтелекту з всебічною міждоменною видимістю та можливостями автоматизованого реагування, Saseon надає підприємствам та постачальникам керованих послуг з безпеки можливість проактивно виявляти приховані загрози, оптимізувати розслідування та зміцнювати свою загальну кіберстійкість проти сучасних, важко виявляємих атак». *(Pushpendra Mishra. Threat Hunting: How AI-Powered Threat Hunting Helps Organizations Detect Hidden Cyber Threats // Techstrong Group Inc. (<https://securityboulevard.com/2026/07/threat-hunting-2/>). 03.07.2026).*

«Дискусія щодо кібербезпеки зміщується від традиційного акценту на захисті інфраструктури шляхом блокування загроз та зменшення вразливостей у бік більш глибокої занепокоєності питаннями контролю та стійкості в умовах нестабільності цифрового середовища. По всій Латинській Америці — де модернізація значною мірою залежала від глобальних хмарних сервісів, платформ для співпраці, систем цифрової ідентифікації та екосистем штучного інтелекту — організації досягли прискорення роботи, економії коштів та оперативної ефективності, але водночас накопичили залежності, які лише зараз стають очевидними... Масштабні збої в роботі хмарних сервісів, перебої у роботі глобальних провайдерів та геополітичний тиск на критичну інфраструктуру продемонстрували, що безперебійність бізнесу більше не залежить лише від внутрішніх засобів захисту; такі компанії, як банки, лікарні, аеропорти та енергетичні системи, дедалі більше покладаються на ланцюги постачання та технологічних провайдерів, над якими вони мають обмежений контроль та недостатню прозорість. Водночас сучасні кіберзагрози часто мають тривалий характер і зосереджуються на ланцюгах постачання, маючи на меті зривати операції, маніпулювати інформацією та спричиняти економічні й операційні втрати навіть без прямої участі в геополітичному конфлікті... Саме тому поняття «цифрового суверенітету» виходить за межі політики й переходить у сферу корпоративної стратегії — маючи на увазі здатність організації здійснювати

автономний та ефективний контроль над тим, як розміщуються та захищаються критично важливі дані, як приймаються рішення під час криз, як зменшується залежність від третіх сторін і як розвиваються власні можливості — не плутаючи при цьому суверенітет із повною технологічною ізоляцією. Виклик полягає в тому, щоб залишатися частиною взаємопов'язаних екосистем, водночас підвищуючи автономність та адаптивність у несприятливих умовах. У відповідь на це центри оперативної безпеки (SOC) еволюціонують від локалізації інцидентів до операційної стійкості, використовуючи штучний інтелект, автоматизацію, прогнозу аналітику та розширену кореляцію для зміцнення довгострокової безперервності роботи, виявлення ризиків залежності, забезпечення прозорості та підтримки швидшого реагування завдяки прогнозуванню на основі сценаріїв... Відповідно змінюються й інвестиційні цілі: замість того, щоб намагатися усунути всі ризики, організації дедалі частіше прагнуть зберегти оперативну спроможність навіть у разі виникнення проблем — тож вирішальними факторами стають прозорість, автономність та контроль в умовах невизначеності, а не просто кількість впроваджених інструментів. Хоча Латинська Америка ще перебуває на початковому етапі цього переходу, організації, які створюють прогнозні архітектури, орієнтовані на автономність, мають всі шанси отримати значні переваги, оскільки стратегія кібербезпеки дедалі частіше розглядає прогнозування на основі штучного інтелекту та постійну оцінку ризиків як єдиний рівень, що забезпечує стабільну діяльність бізнесу». *(Erik Moreno. Why Digital Sovereignty Is Shaking Up Cybersecurity in Latam // Mexico Business Company (<https://mexicobusiness.news/cybersecurity/news/why-digital-sovereignty-shaking-cybersecurity-latam>). 06.07.2026).*

«Компанія Fortinet зазначає, що прискорення еволюції кіберзагроз супроводжується постійним дефіцитом кваліфікованих фахівців з кібербезпеки, що знову підкреслює актуальність питань формування та підтримки кадрового резерву, а також підкреслює стратегічну важливість збільшення участі жінок у сфері інженерії та інформаційних технологій для зміцнення цифрової стійкості. У своєму «Глобальному звіті про дефіцит кваліфікованих кадрів у сфері кібербезпеки до 2026 року», підготовленому на основі даних від лідерів IT-галузі та сфери кібербезпеки з Мексики та Латинської Америки, компанія Fortinet виявила, що 86% організацій повідомляють про принаймні один дефіцит кваліфікованих кадрів у сфері кібербезпеки, а серед них 56% вказують на недостатній рівень кваліфікації у сфері кібербезпеки як головний чинник, що підвищує вразливість до загроз... У звіті стверджується, що ці прогалини створюють реальні операційні навантаження — уповільнюють час реагування, послаблюють виявлення загроз, збільшують вразливість до сучасних загроз, таких як програми-вимагачі та атаки з піддробкою особи, і, зрештою, підвищують витрати на відновлення. Компанія Fortinet пов'язує підвищення ефективності роботи з більшою гендерною різноманітністю, посиляючись на галузевий аналіз, згідно з яким більш гетерогенні команди можуть покращити вирішення проблем, прискорити усунення інцидентів та підвищити стійкість

процесу прийняття рішень завдяки різноманітним аналітичним перспективам... З метою вирішення проблем нестачі кадрів та гендерного дисбалансу компанія Fortinet розширює партнерські відносини з організаціями громадянського суспільства та міжнародними організаціями, зокрема з WOMCY — некомерційною організацією, що зосереджується на розширенні можливостей жінок та підвищенні гендерного різноманіття у сфері інформаційної безпеки в Латинській Америці. Завдяки цьому партнерству члени WOMCY отримують безкоштовний доступ до структурованих навчальних програм через Навчальний інститут Fortinet, зокрема до спеціалізованих курсів, практичних семінарів та програм сертифікації, розроблених з урахуванням потреб як студентів, так і фахівців, які переходять у сферу кібербезпеки... Компанія Fortinet також співпрацює з університетами з метою підтримки розвитку талантів на початковому етапі в Мексиці та підвищення доступності знань у сфері кібербезпеки, приділяючи особливу увагу прикладному навчанню та чіткості викладу — зосереджуючись на критичному мисленні, емпатії та аналітичному мисленні, щоб зменшити бар'єри, пов'язані з побоюваннями, та розвіяти міфи щодо цієї галузі. Загалом компанія розглядає розвиток кадрів у сфері кібербезпеки як оперативну необхідність і як структурну перевагу в плані безпеки, позиціонуючи різноманітність як ключовий компонент стратегії безпеки, а не як другорядну мету, і прагне розширити ці освітні та партнерські ініціативи на всю Мексику та ширший регіон, щоб створити більш інклюзивну та сталу екосистему робочої сили, яка сприятиме цифровій трансформації та довгостроковій стійкості».

(Diego Valverde. Fortinet Urges Women to Study Cybersecurity Amid Skills Gap // Mexico Business Company (<https://mexicobusiness.news/cybersecurity/news/fortinet-urges-women-study-cybersecurity-amid-skills-gap>). 06.07.2026).

«Рада з прав людини Організації Об'єднаних Націй на своїй 62-й сесії одногolosно ухвалила резолюцію, подану Саудівською Аравією, щодо «Розширення прав і можливостей жінок у сфері кібербезпеки». Ця резолюція є результатом глобальної ініціативи, започаткованої саудівським наслідним принцом Мухаммедом бін Салманом, яка має на меті збільшити участь жінок у секторі кібербезпеки, підвищити їхні професійні навички та сприяти їхньому просуванню на керівні посади. Вирішуючи проблему глобального дефіциту кваліфікованих кадрів у сфері кібербезпеки, ця ініціатива спрямована на зміцнення кіберстійкості в усьому світі... Посол Абдулмохсен бін Хотайла наголосив, що одностайна підтримка свідчить про прихильність Саудівської Аравії до міжнародної співпраці та розбудови потенціалу. Реалізацію цієї ініціативи контролює Інститут Глобального форуму з кібербезпеки (GCF) у партнерстві зі спеціалізованими агентствами ООН».

(UN Human Rights Council Unanimously Adopts Saudi-Drafted Resolution on Women Empowerment in Cybersecurity // Al-Yamamah Press Establishment (<https://www.alriyadhdaily.com/article/c4a7320293af4c2c846697c139a6ad9e>). 07.07.2026).

«Сектор квітникарства дедалі частіше стає жертвою кіберінцидентів, і, на думку виробників та покупців, єдине питання, яке зараз стоїть на порядку денному, — це коли саме відбудеться атака, саме тому сектор повинен зміцнити свою стійкість до настання кризи. Флоріс Клоег із компанії Ter Laak Orchios згадує інцидент, пов'язаний із фішингом, що стався 8 квітня 2026 року, коли співробітник компанії Riza Growers натиснув на шахрайське посилання, і зловмисники отримали доступ до його електронної пошти, після чого відправили листи від його імені приблизно 125 контактам, поширивши фішинг по всій галузі... На щастя, оперативні дії — блокування зламаного облікового запису та негайне інформування одержувачів — допомогли обмежити збитки, а згодом компанія Royal FloraHolland за підтримки національних експертів з кібербезпеки встановила зв'язок цього інциденту з іншими кіберінцидентами. Слідчі дійшли висновку, що це був випадок компрометації ділової електронної пошти — загроза, яка легко могла спричинити більш значні економічні збитки та шкоду репутації, а також підвищила ризик подальших атак, оскільки злочинці отримали більш глибоке уявлення про те, як виробники та покупці спілкуються між собою... Компанія Ter Laak Orchios реагує на це, надаючи пріоритет кібербезпеці в рамках свого переходу до повністю циркулярної тепличної системи з цифровим управлінням до 2030 року, створюючи численні «захисні бар'єри» навколо своїх даних та операцій, включаючи обов'язкову двофакторну автентифікацію та чіткі процедури дій у разі порушення цих бар'єрів. Не менш важливо, що компанія проводить навчання персоналу за допомогою регулярних тестів із «імітацією фішингу», презентацій та внутрішніх інформаційних кампаній, нагадуючи співробітникам, що фішинг може бути спрямований проти будь-кого — особливо зараз, коли штучний інтелект робить шахрайські схеми все більш реалістичними, — тому здоровий глузд і здатність оцінювати ситуацію за контекстом залишаються надзвичайно важливими... Вони також наголошують на підході «зупинитися — перевірити — повідомити», який викладається у вебінарах та рекомендаціях Royal FloraHolland: зупинитися, коли щось здається підозрілим, перевірити це та негайно повідомити про це, щоб зменшити збитки та захистити ширшу спільноту. Головною темою є співпраця, а не конкуренція: виробники діляться знаннями через Royal FloraHolland, використовують такі інструменти, як передплата на галузеві аналітичні звіти про загрози, та працюють разом, щоб забезпечити кіберстійкість квітникарської галузі». (*Cybersecurity Lessons from a Floriculture Phishing Attack // Meister Media Worldwide* (<https://www.greenhousegrower.com/technology/cybersecurity-lessons-from-a-floriculture-phishing-attack/>). 06.07.2026).

«Оцінка стану кібербезпеки Bitdefender за 2026 рік, проведена на основі опитування 1 200 фахівців у галузі ІТ та кібербезпеки з усього світу, висвітлює критичний розрив між високим рівнем усвідомлення кіберризиків та фактичною операційною стійкістю. Хоча організації розуміють загрози, з якими вони стикаються, їм важко впоратися зі складнощами сучасної кібербезпеки через чотири основні суперечності. По-перше, існує значний розрив у рівні прозорості

щодо штучного інтелекту: хоча понад половина керівників вважає, що вони повністю контролюють використання ШІ співробітниками, майже 47% респондентів — особливо фахівців, які працюють на передовій — визнають, що мають обмежену або взагалі відсутню інформацію про «тіньовий ШІ» або особисті інструменти ШІ, які використовуються в роботі... По-друге, хоча команди з безпеки погоджуються з нагальною необхідністю зменшити площу атаки, їх часто паралізують брак ресурсів, труднощі з дотриманням політик зміцнення безпеки та побоювання порушити повсякденну ділову діяльність. По-третє, надмірна увага галузі до нових загроз, пов'язаних зі штучним інтелектом — таких як самотутуюче шкідливе програмне забезпечення та витік даних з великих мовних моделей (LLM) — створює небезпечну «сліпу зону» щодо більш поширених, традиційних методів атак... Наприклад, надзвичайно руйнівні атаки типу «Living off the Land» (LOTL) привертають дуже мало уваги, незважаючи на те, що на них припадає 84% інцидентів високого рівня серйозності. Нарешті, незважаючи на усвідомлення важливості прозорості після порушення безпеки, 55,2% фахівців, які стикалися з порушенням безпеки протягом останнього року (у США цей показник сягає 68,6%), повідомляють, що їхні організації тиснули на них, щоб вони зберігали інцидент у таємниці, навіть коли закон вимагав його повідомлення. Зрештою, у звіті робиться висновок, що головним викликом 2026 року є не просто усвідомлення цих кіберризиків, а успішне застосування цих знань на практиці для досягнення балансу між безпекою, продуктивністю, дотриманням нормативних вимог та прозорістю». *(2026 Cybersecurity Assessment: The Gap Between Awareness and Resilience // The Hacker News (<https://thehackernews.com/2026/07/2026-cybersecurity-assessment-gap.html>). 01.07.2026).*

«Старе правило кібербезпеки «думай як хакер» залишається актуальним, але ключовий нюанс полягає в тому, що ви повинні мислити, виходячи за межі власної внутрішньої мережі, оскільки хакери дедалі частіше діють у рамках розгалуженої, взаємопов'язаної екосистеми, а не атакують окрему «фортецю». Традиційні стратегії безпеки, засновані на захисті периметра, передбачали чітке розмежування між «своїми» та «чужими» — підхід, який досить добре працював, коли організації покладалися на централізовану локальну інфраструктуру. Сьогодні хмарні обчислення, аутсорсинг та поширення автономних «агентних» систем штучного інтелекту ще більше розмивають ці межі: зовнішні інструменти, API та дозволи сторонніх розробників можуть уможливити атаки, поки ви спите, зокрема сценарії типу «введення підказки», які перетворюють легітимні інструменти на несвідомих спільників... Проте найнебезпечніші слабкі ланки часто не є суто технічними; вони мають структурний характер, особливо це стосується ланцюга поставок, що включає сторонніх постачальників та підрядників, на яких покладаються підприємства. Великі організації мають багато партнерів — бухгалтерські фірми, постачальників CRM, юридичних та ERP-інтеграторів — кожен із яких має власний рівень безпеки, що робить слабкі місця постачальників «шляхом найменшого опору». Дослідження показали, що значна і дедалі більша частка інцидентів у великих організаціях походить від контрагентів

та третіх сторін, що означає, що периметр фактично більше не існує... Хоча інструменти управління ризиками третіх сторін (TPRM) можуть надавати оцінки постачальників, вони часто дають абстрактні результати, а не практичні заходи захисту, засновані на конкретних сценаріях, тому вони можуть не допомогти передбачити, як і де найімовірніше відбудеться злом. Підхід, більш схожий на хакерський, вимагає видимості «всієї екосистеми» — моніторингу не лише самої компанії, а й мережі дочірніх підприємств, партнерів, підрядників та постачальників. Це можна зробити шляхом агрегування зовнішніх кіберсигналів (таких як витоки, нові експлойти, витік облікових даних та фішингові домени як в організації, так і у її партнерів) та перетворення їх на конкретні сценарії атак і цілеспрямовані заходи з мінімізації ризиків, по суті створюючи прогнози «кіберпогоди», які показують, де вразливості можуть перетинатися... Висновок полягає в тому, що ефективний захист тепер залежить від комплексного, прогностичного моніторингу та оперативного усунення вразливостей у всій екосистемі, оскільки зловмисники аналізують ситуацію в пошуках найпростішого шляху проникнення — чи то всередині основної організації, чи то через периферійного постачальника. Тому захисники повинні застосовувати такий самий панорамний підхід і забезпечувати безпеку екосистеми в цілому». **(Viacheslav Vasipenok. To Catch a Hacker, Think Like One: The Nuance in Modern Cybersecurity // QUASA News (<https://quasa.io/media/to-catch-a-hacker-think-like-one-the-nuance-in-modern-cybersecurity>). 05.07.2026).**

«...Для малих та середніх підприємств (МСП) значний кіберризик часто криється не в їхніх власних офісах, а у їхніх сторонніх постачальників, таких як компанії, що надають послуги з розрахунку заробітної плати, фірми з ІТ-підтримки та хмарні сервіси. Якщо у важливого постачальника трапляється порушення безпеки або збій системи, це може призвести до витоку даних, простою послуг та шкоди репутації, що, у свою чергу, може серйозно вплинути на доходи та діяльність МСП. Тому надзвичайно важливо проводити практичні та пропорційні оцінки кіберризиків, пов'язаних із сторонніми постачальниками...

Замість складного процесу, що вимагає великого обсягу паперової роботи, малі та середні підприємства (МСП) повинні класифікувати своїх постачальників залежно від впливу на бізнес та доступу до даних, зосереджуючи свої зусилля з оцінки насамперед на постачальниках «високого ризику», які працюють з конфіденційними даними або критично важливими для бізнесу системами. Процес оцінки повинен передбачати постановку чітких запитань щодо того, як постачальник захищає дані, управляє доступом, здійснює резервне копіювання та повідомляє про інциденти. Залежно від рівня ризику постачальника, підтверджуючі документи можуть варіюватися від простого опитувальника до незалежних звітів про перевірку... Якщо постачальник не відповідає стандартам безпеки, МСП може знизити ризик за допомогою практичних заходів, таких як обмеження доступу до даних, скасування непотрібного віддаленого доступу або додавання до договору суворих вимог щодо безпеки. Впровадивши простий, повторюваний процес — зосередившись на постачальниках із значним впливом, ведучи чіткий облік

прийнятих рішень та проводячи щорічні перегляди — МСП можуть ефективно управляти кіберризиками, пов'язаними з третіми сторонами, та захищати свою господарську діяльність без необхідності володіння глибокими технічними знаннями...» (*Third-party cyber risk assessments for SMEs: a practical guide for UK businesses // Techstrong Group Inc. (<https://securityboulevard.com/2026/07/third-party-cyber-risk-assessments-for-smes-a-practical-guide-for-uk-businesses/>). 03.07.2026*).

«У міру того як малі та середні підприємства стають дедалі більш залежними від цифрових технологій, вони також стикаються з дедалі більшою вразливістю до кіберзагроз, таких як програми-вимагачі, фішинг та витоки даних. Замість того щоб розглядати кібербезпеку виключно як витрати, організації дедалі частіше визнають кіберстійкість стратегічною інвестицією, яка сприяє як захисту, так і зростанню бізнесу. Кіберстійкість зосереджується не лише на запобіганні атакам, а й на підготовці до інцидентів, реагуванні на них та відновленні після них, забезпечуючи при цьому безперебійність бізнесу...

Ефективна стратегія кіберстійкості допомагає зменшити фінансові втрати завдяки мінімізації часу простою та витрат на відновлення, зміцнює довіру клієнтів завдяки надійному захисту конфіденційної інформації та підвищує операційну ефективність, сприяючи вдосконаленню практик технічного обслуговування систем та забезпечення їхньої безпеки. Вона також може створити конкурентні переваги, оскільки багато великих організацій зараз вимагають від постачальників дотримання стандартів кібербезпеки, водночас сприяючи дотриманню мінливих нормативних вимог щодо захисту даних та зменшенню юридичних ризиків...

Зрештою, інтеграція кіберстійкості в бізнес-стратегію дає малим та середнім підприємствам можливість краще адаптуватися до мінливих загроз, захищати свою репутацію та забезпечувати сталий розвиток. Розглядаючи кібербезпеку як рушійну силу стійкості та створення цінності, а не лише як оборонний захід, підприємства можуть підвищити прибутковість та забезпечити довгостроковий успіх у середовищі, що дедалі більше переходить у цифровий формат». (*Naveen Goud. How Cyber Resilience can help SMBs in building Profits // Cybersecurity Insiders (<https://www.cybersecurity-insiders.com/how-cyber-resilience-can-help-smbs-in-building-profits/>). 08.07.2026*).

«Кібербезпека вступає в новий етап, на якому акцент зміщується з простого запобігання проникненню в мережі на забезпечення операційної стійкості в разі, коли зловмисники неминуче проникають у систему. Цей перехід є особливо важливим для сектору фінансових послуг, який залишається головною мішенню для кіберзлочинців через наявність у ньому конфіденційних економічних даних та значну залежність від взаємопов'язаних ланцюгів постачання сторонніх постачальників, що може перетворити компрометацію одного постачальника на масштабну кризу безперервності бізнесу... Ситуація з кіберзагрозами різко загострилася: програмне забезпечення для вимагання викупу

перетворилося на складну екосистему, що базується на багатоетапному вимаганні, моделях «вимагання як послуга» (RaaS) та генеративній штучній інтелекції. Ці сучасні інструменти дають зловмисникам змогу автоматизувати розвідку, створювати надзвичайно переконливі фішингові кампанії та здійснювати шифрування за лічені години, а не тижні. Підтвердженням цього стрімкого зростання є те, що лише у 2024 році INTERPOL зафіксував понад 135 000 інцидентів із використанням програм-вимагачів у Азії та Південному Тихоокеанському регіоні, що спонукало до скоординованих міжнародних заходів з ліквідації шкідливої інфраструктури... Оскільки традиційних заходів профілактики вже недостатньо, кібербезпека перетворилася з суто технічної проблеми на один із найважливіших пріоритетів керівництва, що охоплює організаційну культуру, управління та кризове управління. Сьогодні успіх організації в сфері кібербезпеки вимірюється не лише її здатністю блокувати загрози, а й її спроможністю розраховувати на можливе порушення безпеки, швидко локалізувати інциденти за допомогою сегментації мережі та незмінних резервних копій, оперативно відновлювати критично важливі функції та зберігати довіру клієнтів у умовах сильного тиску». **(Tim Sandle. Ransomware without borders: Why cyber resilience has become a global business imperative // Digital Journal Inc. (<https://www.digitaljournal.com/article/ransomware-without-borders-why-cyber-resilience-has-become-a-global-business-imperative/>). 06.07.2026).**

«Нове дослідження компанії з кібербезпеки VikingCloud виявляє серйозний розрив між уявленнями та реальністю щодо кібербезпеки в галузі ресторанів швидкого обслуговування та ресторанів формату «fast-casual». Хоча 94% лідерів галузі висловлюють високу впевненість у своїх заходах безпеки, 80% насправді зазнали принаймні одного кіберінциденту протягом минулого року, що призвело до витоку конфіденційних даних — зокрема, платіжних реквізитів та даних про заробітну плату — у 76% операторів. Ця вразливість значною мірою зумовлена складним та фрагментованим характером мереж із численними закладами, де одне слабе місце може поставити під загрозу все підприємство, проте лише 36% з них забезпечують стандартизований цілодобовий моніторинг у всіх закладах...

Практики галузі часто посилюють ці ризики, оскільки 78% керівників ресторанів зізнаються, що відкладають встановлення важливих оновлень програмного забезпечення, аби уникнути перебоїв у роботі, ставлячи оперативність вище за безпеку. Крім того, мережі ресторанів стикаються зі стрімким розширенням площі атаки через значну залежність від сторонніх постачальників, широке впровадження пристроїв Інтернету речей (IoT) та систем замовлення на основі штучного інтелекту, а також різке зростання кількості витончених шахрайських схем із використанням соціальної інженерії, зокрема «діпфейків», згенерованих штучним інтелектом, які використовуються для авторизації шахрайських платежів. Фінансові та операційні наслідки цих прогалин у безпеці є серйозними: вони обходяться більшості операторів у понад 1 000 доларів на годину під час пікових перебоїв у роботі систем і змушують 10% з них повністю закривати

зклади. Розуміючи, що внутрішні команди не в змозі забезпечити безпеку цих складних, децентралізованих цифрових екосистем, 30% ресторанних мереж планують найняти зовнішніх партнерів з кібербезпеки в найближчий рік, щоб усунути прогалини у виявленні загроз і перетворити цифрову стійкість на конкурентну перевагу...» (*Ninety-Four Percent of Restaurant Chains Feel Confident in Their Cyber Defenses. Seventy-Six Percent Had Sensitive Data Leaked Anyway, According to New VikingCloud Research // Cision US Inc. (<https://www.prnewswire.com/news-releases/ninety-four-percent-of-restaurant-chains-feel-confident-in-their-cyber-defenses-seventy-six-percent-had-sensitive-data-leaked-anyway-according-to-new-vikingcloud-research-302819879.html>). 08.07.2026*).

«Згідно з доповіддю «Wavestone Cyber Benchmark 2026», в якій було проаналізовано понад 200 глобальних організацій, що використовують такі стандарти, як «NIST Cybersecurity Framework 2.0» та ISO 27001/27002, середній рівень кіберзрілості великих компаній зріс до 55,3 відсотка. Цей прогрес значною мірою зумовлений суворими регуляторними вимогами, причому фінансовий сектор є лідером у цій сфері, оскільки кібербезпека дедалі більше перетворюється з простого завдання ІТ-відділу на стратегічний пріоритет керівництва. У відповідь на ці виклики компанії розширюють свої кадрові ресурси та зараз інвестують у середньому 6,7 відсотка своїх ІТ-бюджетів у кібербезпеку, що дозволяє досягти помітних покращень у сфері управління, управління ризиками та виявлення загроз...

Однак, незважаючи на ці досягнення, залишаються значні вразливості. У той час як штучний інтелект дедалі ширше інтегрується в бізнес-процеси, рівень зрілості безпеки ІІІ залишається на рівні лише 38 відсотків; хоча багато компаній мають політики щодо безпечного використання ІІІ, лише 10 відсотків впровадили технічні заходи захисту від конкретних загроз, таких як введення підказки. Крім того, загальна стійкість організацій продовжує відставати: категорія «Відновлення» має найнижчий рівень зрілості — 44 відсотки, що свідчить про те, що компанії все ще стикаються з труднощами у швидкому відновленні критично важливих бізнес-процесів після атаки. Зрештою, експерти Wavestone роблять висновок, що сталий успіх у бізнесі та конкурентна перевага залежатимуть від того, чи зможуть компанії постійно адаптувати свої стратегії кібербезпеки для забезпечення дотримання нормативних вимог, безпечної інтеграції нових технологій ІІІ та суттєвого покращення своїх можливостей щодо відновлення після інцидентів». (*Cyber Benchmark 2026: Regulation Strengthens Cyber Defense – AI Shifts the Security Agenda // MQ Management and Quality (<https://www.m-q.ch/en/cyber-benchmark-2026-regulation-strengthens-cyber-defense-ai-shifts-the-security-agenda/>). 06.07.2026*).

«У сучасній цифровій економіці кібербезпека вже не є лише завданням ІТ-відділу, а є самою основою виживання компанії. Кіберзлочинці все частіше обирають невеликі підприємства як легкі цілі, особливо в таких юрисдикціях, як

Кіпр, який приваблює хакерів завдяки високій концентрації міжнародного капіталу, транспортних компаній та фінансових установ. Офіційні дані свідчать, що понад 53% кіпрських підприємств зазнали цифрового інциденту або витоку даних протягом минулого року, причому компанії на острові стикаються з атаками в середньому кожні вісім днів. Ця загроза має глобальний характер: за прогнозами, збитки від кіберзлочинності з 2026 року будуть зростати на 2,47% щорічно, досягнувши майже 12 трильйонів доларів до 2031 року. Щоб адаптуватися до цих несприятливих умов та захистити свої активи й репутацію, підприємства повинні відмовитися від застарілих, реактивних методів і впровадити багаторівневі, проактивні лінії захисту...

Значна частина сучасних кіберризиків пов'язана з переходом на дистанційну роботу, що призвело до розширення площі атаки. Для забезпечення безпеки віддалених операцій компанії надають пріоритет захисту даних на рівні кінцевих точок, гарантуючи моніторинг кожного пристрою та застосовуючи суворі засоби контролю доступу, такі як багатофакторна автентифікація. Щоб шифрувати віддалений трафік і захищати внутрішню мережеву інфраструктуру від сканування хакерами, підприємства все частіше використовують приватні проксі-сервери для створення безпечних тунелів для передачі конфіденційних даних. Крім того, надійні стратегії резервного копіювання мають вирішальне значення для забезпечення швидкого відновлення бізнесу та запобігання паралічу операційної діяльності у разі атаки програм-вимагачів...

Однак, оскільки, за даними Verizon, приблизно 60% усіх цифрових інцидентів пов'язані з людською помилкою — наприклад, слабкими паролями або випадковим розголошенням інформації — одних лише технологій недостатньо. Отже, найкращі практики корпоративної безпеки повинні надавати пріоритет постійному практичному навчанню співробітників з питань кібербезпеки, щоб перетворити персонал на активний захист від фішингу та соціальної інженерії. Зрештою, формування стійкої кіберстійкості — це безперервний процес поєднання надійних технічних засобів, зокрема шифрування трафіку, антивірусних програм нового покоління та автоматичних оновлень, із суворими організаційними заходами безпеки. Для регіонів, що є привабливими цілями для атак, таких як Кіпр, цей комплексний підхід є не лише стратегічним вибором, а й фундаментальною вимогою для виживання бізнесу». (*How Cyprus businesses adapt to rising cybersecurity threats // Cyprus Mail (<https://cyprus-mail.com/2026/07/13/how-cyprus-businesses-adapt-to-rising-cybersecurity-threats>). 13.07.2026*).

«Забезпечення безпеки величезних стадіонів, на яких проходитиме Чемпіонат світу з футболу 2026 року в Північній Америці, є величезним викликом у сфері кібербезпеки, оскільки об'єкти, що вміщують понад 80 000 уболівальників, повинні безпечно інтегрувати десятки тисяч некерованих особистих пристроїв із критично важливою інфраструктурою, що забезпечує здійснення платежів, трансляції та оперативну діяльність. Оскільки контролювати кожен окремий пристрій уболівальника неможливо, ІТ-команди стадіонів повинні надати пріоритет суворій сегментації мережі, перенаправляючи

всі пристрої уболівальників на публічну мережу Wi-Fi та за замовчуванням розглядаючи їх як загрозливі... Щоб ефективно управляти цією величезною площею атаки, стадіони повинні впровадити архітектуру «Zero Trust», підкріплену надійними інструментами управління ідентифікацією та доступом (IAM), які використовують адаптивну багатофакторну автентифікацію (MFA) та умовний доступ на основі ролей для запобігання поперечному переміщенню зловмисників. Крім того, постійна видимість мережі в режимі реального часу та централізований моніторинг кінцевих точок є необхідними для виявлення аномалій та швидкої ізоляції скомпрометованих пристроїв... Для підтримки цих зусиль стадіони значною мірою покладаються на платформи управління інформацією про безпеку та подіями (SIEM), які використовують поведінкову аналітику для автоматизації виявлення загроз, запуску робочих процесів реагування на інциденти та забезпечення дотримання суворих нормативних вимог щодо даних, таких як PCI-DSS та GDPR. Зрештою, з огляду на підвищений ризик атак з боку хактивістів та злочинців, що діють за підтримки держави, під час цього широко висвітлюваного, цифрового інтегрованого глобального заходу, IT-персонал стадіонів повинен проводити ретельні симуляції інцидентів та застосовувати комплексні рішення з безпеки, щоб забезпечити безперебійну та безпечну роботу». **(John Donegan. When 80,000 fans log on at once: The 2026 World Cup's unique cybersecurity issues // FoundryCo, Inc. (<https://www.csoononline.com/article/4196827/when-80000-fans-log-on-at-once-the-2026-world-cups-unique-cybersecurity-issues.html>). 15.07.2026).**

«Чемпіонат світу з футболу ФІФА, що охоплює три країни, 16 міст-господарів та 104 матчі, функціонує як масштабна тимчасова цифрова економіка, яка об'єднує стадіони, телерадіокомпанії, транспортні мережі, системи продажу квитків та платіжні платформи. Ця надзвичайно складна, взаємопов'язана інфраструктура є важливим прикладом для вивчення цифрових ризиків, що відображає значний операційний тиск, з яким стикаються сучасні підприємства. Вразливість таких масштабних спортивних екосистем нещодавно продемонстрував незалежний дослідник у сфері безпеки, який обійшов блокування на стороні клієнта під час входу в обліковий запис агента, зареєстрованого у ФІФА, щоб отримати доступ до панелі управління стримінгом ФІФА, викривши інструменти, пов'язані з даними про матчі в прямому ефірі та виробництвом відеопотоків. Ця вразливість нагадує шкідливе програмне забезпечення «Olympic Destroyer», яке порушило роботу IT-систем під час церемонії відкриття Зимових Олімпійських ігор 2018 року. Вона також узгоджується з дослідженням Darktrace, яке показує, що 84% професійних спортивних організацій зазнали кіберінциденту протягом останніх 12 місяців, причому 57% з них зазнали декількох порушень безпеки...

Ці загрози активно посилюються через розвиток штучного інтелекту. Зловмисники використовують ШІ для виявлення незахищених систем, створення надзвичайно переконливих повідомлень та прискорення початкових етапів атак. Як наслідок, 83% команд з кібербезпеки у сфері спорту повідомили про виявлення атак на основі ШІ протягом минулого року, а 72% очікують, що ШІ збільшить їхні

ризика протягом наступних 12 місяців. У внутрішньому плані спортивні організації також стикаються з ризиками, пов'язаними зі ШІ, оскільки 47% фахівців з кібербезпеки висловлюють занепокоєння щодо створених співробітниками ШІ-агентів, яким бракує людської розсудливості. Незважаючи на те, що експерти з безпеки вказують на роботу стадіонів як на сферу, де компрометація систем спричинить найбільший операційний вплив, понад третина спортивних організацій уже використовує або планує використовувати ШІ-агентів у системах стадіонів...

Щоб адаптуватися до цих швидкозмінних загроз, організації можуть застосувати три основні уроки, винесені з цифрових операцій під час Чемпіонату світу з футболу. По-перше, стійкість має охоплювати всю екосистему. Сучасні операції значною мірою залежать від систем постачальників, а це означає, що керівники повинні перевіряти доступ постачальників та впроваджувати суворі заходи контролю, щоб забезпечити безперебійну роботу бізнесу у разі збою зв'язку з партнером. По-друге, управління ідентифікацією має розширюватися для моніторингу людей, машин та агентів штучного інтелекту. Організації повинні впровадити поведінкове виявлення для виявлення аномалій — таких як несподівані зміни в системі або запити на дані — замість того, щоб покладатися виключно на статичні списки затверджених користувачів. Нарешті, плани реагування необхідно активно тестувати в умовах реального оперативного навантаження. Оскільки людські команди з безпеки можуть бути перевантажені під час пікових періодів, організації повинні визначити, які системи є найважливішими, та встановити, де автономні засоби локалізації можуть миттєво утримати ситуацію під контролем, поки дослідники-люди проводять більш глибоке усунення проблем». *(Nicole Carignan. Three lessons on cybersecurity and digital risk from the World Cup // World Economic Forum (<https://www.weforum.org/stories/cybersecurity/cybersecurity-digital-risk-fifa-world-cup/>). 14.07.2026).*

«Так само, як і в медицині, профілактика в сфері кібербезпеки є набагато економічно вигіднішою та дає кращі результати, ніж очікування, поки проблему буде усунено, проте сучасна галузь безпеки занадто сильно схилилася в бік виявлення порушень після їхнього вчинення. Хоча ранні заходи безпеки в 1990-х роках були зосереджені на блокуванні несанкціонованого доступу та виконання шкідливого коду за допомогою брандмауерів та антивірусів, зростаюча складність мереж зрештою призвела до появи моделі, що ставить на перше місце виявлення, зосередженої на агрегації журналів, оповіщенні та швидкому реагуванні. Однак, незважаючи на покращення показників видимості, таких як середній час виявлення та середній час реагування, глобальні показники порушень безпеки та витрати, пов'язані з ними, залишаються неприйнятно високими. Це пов'язано з тим, що засоби виявлення активуються лише після того, як порушення безпеки вже сталося, і не роблять нічого для запобігання початковому порушенню, яке зазвичай виникає через типові слабкі місця, такі як відомі вразливості, викрадені облікові дані та неправильні налаштування системи...

Ця структурна залежність від виявлення призвела до створення незбалансованого ринку; за останні три роки понад 70 відсотків із понад 500 стартапів у сфері кібербезпеки, які брали участь у конкурсі RSAC, випустили на ринок саме засоби виявлення, а не технології запобігання. Цей надлишок рішень для моніторингу в кінцевому підсумку посилює серйозну «втому від сповіщень», перевантажуючи обмежені команди з безпеки зайвою інформацією та помилковими спрацьовуваннями. Покладатися переважно на швидше оповіщення особливо небезпечно, оскільки зловмисники починають діяти зі швидкістю машин, використовуючи штучний інтелект для автоматизації експлуатації вразливостей та масштабування фішингових кампаній. Новітні передові моделі штучного інтелекту, такі як Mythos від Anthropic та GPT-5.5 від OpenAI, дедалі краще здатні виявляти невідомі ризики «нульового дня» та об'єднувати дрібні вразливості, тоді як квантові обчислення одночасно загрожують стійкості криптографії. Реагування на ці високоавтоматизовані загрози, що стрімко розмножуються, за допомогою швидших сповіщень є недостатнім захистом...

Щоб повернути перевагу в «захисній економіці» на бік захисників, галузь повинна активно перерозподілити свої ресурси на користь проактивних, превентивних архітектур. Впровадження багатофакторної аутентифікації, стійкої до фішингу, блокування виконання шкідливого коду, сегментація мереж та дисципліноване управління вразливостями за принципами «нульової довіри» суттєво зменшать площу атаки організації. Такий рівень превентивної зрілості природним чином знижує загальний обсяг сповіщень, зменшуючи «шум», завдяки чому необхідні засоби виявлення можуть працювати набагато ефективніше. Замість того, щоб визначати успіх за тим, наскільки ефективно аналітики з безпеки виявляють порушення, або збільшувати штат для обробки зростаючого обсягу сповіщень, новатори у сфері кібербезпеки та венчурні інвестори повинні надавати пріоритет масштабованим превентивним заходам, щоб блокувати точки входу ще до того, як ними зможуть скористатися зловмисники». ***(Rich Baich and Hugh Thompson. Cybersecurity needs more prevention and less reliance on cure // FoundryCo, Inc. (<https://www.csoonline.com/article/4196818/cybersecurity-needs-more-prevention-and-less-reliance-on-cure.html>). 15.07.2026).***

Згідно зі звітом Arctic Wolf «Стан поверхні атаки в сфері кібербезпеки у 2026 році» (2026 State of the Cybersecurity Attack Surface), в якому було проаналізовано анонімізовані дані щодо понад 800 000 ІТ-активів, що перебувають під моніторингом за допомогою Aurora® Exposure Management, прогалини в основних заходах безпеки та видимості активів залишаються поширеною проблемою для організацій будь-якого розміру. Звіт показав, що 33% моніторованих ІТ-активів не мають принаймні одного критичного засобу контролю безпеки; зокрема, 18% не охоплені корпоративним управлінням виправленнями або конфігурацією, 10% не мають захисту кінцевих точок, а 17% невидимі для застарілих інструментів управління вразливостями. Ці прогалини не є поодинокими випадками, а, як правило, є наслідком фрагментованих ІТ-операцій, розрізнених інвентаризацій та надмірного розширення інструментарію, що виникає

внаслідок управління безпекою кінцевих точок, встановленням оновлень, ідентифікацією та безпекою хмарних середовищ на окремих, не пов'язаних між собою платформах...

Ця відсутність прозорості ще більше посилюється через збереження технологій, термін експлуатації яких закінчився (EOL): 19% ІТ-активів наразі не підтримуються оновленнями безпеки від постачальників. Ці застарілі активи часто залишаються активними, оскільки від них залежать критично важливі додатки або тому, що організації помилково вважають, що міграція повністю завершена. В одному з моніторованих середовищ завдяки масштабній міграції вдалося зменшити кількість активів EOL на 41%, проте 8% цих активів залишилися без підтримки, незважаючи на внутрішнє підтвердження того, що проект завершено. Ця розбіжність підкреслює необхідність для команд з безпеки постійно та незалежно перевіряти ефективність своїх заходів з усунення вразливостей, а не покладатися на самозвіти чи припущення...

У міру того, як організації вдосконалюють захист своїх периметрів, зловмисники пристосовуються, обираючи шлях найменшого опору. Частка випадків реагування на інциденти, зареєстрованих компанією Arctic Wolf, що були спричинені зовнішніми експлойтами, знизилася з 29% до 11%, тоді як зловживання службами віддаленого доступу різко зросло і склало 65% випадків реагування на інциденти, не пов'язані з ВЕС, порівняно з 24% три роки тому. Ця тенденція супроводжується різким зростанням кількості випадків зловживання довірчими відносинами та інцидентів, пов'язаних із неправильною конфігурацією. Примітно, що для кожної з десяти найчастіше експлуатованих вразливостей у випадках реагування на інциденти Arctic Wolf за 2025 рік існував доступний патч, причому найчастіше експлуатувалася вразливість CVE-2024-40766, що впливає на SonicWall SonicOS. Ці дані свідчать про те, що основним викликом у сфері безпеки вже є не просто виявлення вразливостей, а виявлення та усунення ризиків, що приховані в некерованих сегментах мережі...» (*Your attack surface is bigger than you think // TechTarget, Inc. (<https://www.cybersecuritydive.com/spons/your-attack-surface-is-bigger-than-you-think/825160/>). 20.07.2026*).

«Згідно з результатами щорічного опитування «Data Health Check 2026», проведеного компанією Databarracks серед 500 керівників ІТ-підрозділів, 26% підприємств за останній рік зазнали кіберінциденту, джерелом якого став їхній ланцюг поставок. Незважаючи на високу обізнаність щодо цих ризиків, 48% організацій продовжували співпрацювати з постачальниками, незважаючи на відомі проблеми з стійкістю до зловживань або безпекою, головним чином через відсутність реальних альтернатив; дійсно, 26% респондентів визначили свою залежність від постачальників як головну перешкоду для підвищення загальної стійкості до зловживань. Небезпека такої залежності є очевидною: організації, які свідомо співпрацювали з ризикованими постачальниками, мали у понад чотири рази вищу ймовірність зазнати кіберінциденту, джерелом якого став постачальник (43% порівняно з лише 10% тих, хто цього не робив). Щодо майбутнього, 23% організацій визначили вразливості ланцюга поставок як одне з трьох головних

викликів на найближчі п'ять років, поступившись лише кіберзагрозам на основі штучного інтелекту (46%) та програм-вимагачів (26%)...

Хоча 89% підприємств оцінюють стійкість постачальників під час їхнього залучення, а 61% проводять такі оцінки щорічно, щоквартально або на постійній основі, традиційні методи оцінки часто виявляються недостатніми. Кріс Батлер, директор з питань стійкості компанії Databarracks, зазначає, що стандартні анкети щодо відповідності вимогам перетворилися на процедуру «відмічання галочок», яка створює хибне відчуття впевненості, а не забезпечує справжню стійкість. Крім того, хоча компанії можуть добре розуміти своїх основних партнерів, рівень прозорості зазвичай значно знижується на нижчих рівнях ланцюга поставок. Щоб забезпечити справжню безперервність діяльності, Батлер радить керівникам підприємств ставитися до критично важливих постачальників як до продовження власної діяльності. Якщо ключовий постачальник не має власного досвіду в сфері забезпечення безперервності діяльності, організації повинні активно допомагати йому, залучаючи цих зовнішніх партнерів до спільних репетицій забезпечення безперервності діяльності та навчань з реагування на надзвичайні ситуації, щоб відпрацювати узгоджену координацію дій». ***(1 in 4 businesses hit by cyber attacks through their supply chain in the last year // yahoo! finance (<https://finance.yahoo.com/technology/ai/articles/1-4-businesses-hit-cyber-080000145.html>). 21.07.2026).***

«У світі ІТ «ефект кавуна» — зелена панель управління, що приховує хаотичну, «червону» реальність, — підкреслює зростаючий ризик для лідерів технологічного сектору. Раніше це помилкове відчуття безпеки, засноване на неврахованих застарілих боргах та «тіньових» ІТ-системах, часто можна було виправдати; порушення безпеки розглядалося як непередбачувана трагедія, яку можна було вирішити за допомогою страхування та зв'язків з громадськістю. Однак цей корпоративний захист зараз втрачає свою ефективність через більш суворі регуляторні вимоги, зокрема директиви ЄС DORA та NIS2, а також правила Комісії з цінних паперів та бірж США (SEC) щодо розкриття інформації про кібербезпеку. Ці нормативні акти покладають на керівництво остаточну відповідальність не лише за забезпечення контролю, а й за те, щоб після інциденту довести, що їхні рішення відповідали наявним на той момент даним про ризики. Справжня небезпека для сучасного керівника ІТ-відділу полягає в неможливості узгодити те, що було представлено інвесторам та регуляторним органам, із внутрішніми даними про відомі ризики...

Отже, традиційні артефакти відповідності, такі як щорічні звіти SOC 2, вже не є достатніми, оскільки вони є лише історичними знімками, які не відображають динамічне середовище ризиків. Очікування змістилися від статичної відповідності до стану постійних викликів та активного управління. Щоб витримати перевірку після інциденту, яка зосереджується на тому, чи були відомі ризики проігноровані або недооцінені, керівникам потрібен простежуваний ланцюг управління. Рішення полягає в переосмисленні ролі відділу ІТ-аудиту: з перешкоди для дотримання вимог він має перетворитися на «незалежний механізм збору доказів», який

допомагає побудувати цей захисний ланцюжок. Така співпраця має привести до створення документів, що не підлягають обговоренню, таких як реєстри ризиків для ради директорів із чіткою історією ескалації, детальні записи про прийняття ризиків, докладні журнали моделювання та настільних навчань, інвентаризації управління штучним інтелектом та синхронізовані передачі контролю за розкриттям інформації. Мета полягає не в тому, щоб запобігти кожному інциденту, а в тому, щоб створити незалежний запис, який демонструє, що ризики активно виявлялися, аналізувалися, ескалувалися та відповідально управлялися, що може стати вирішальною відмінністю між провалом, який можна пояснити, та тим, що вважається недбалістю». (*Ravi Sharma. The audit trail CIOs need before the next cyber crisis // FoundryCo, Inc. (<https://www.cio.com/article/4198467/the-audit-trail-cios-need-before-the-next-cyber-crisis.html>). 19.07.2026*).

«Традиційна стратегія кібербезпеки, що зосереджується виключно на профілактиці та використовує брандмауери й посилений контроль доступу для запобігання проникненню зловмисників, вже не є достатньою. Оскільки сучасні кіберзагрози стають дедалі витонченішими та наполегливішими, успішні прориви тепер є питанням «коли, а не чи». Ця реальність зумовила фундаментальний перехід до концепції кіберстійкості, яка розглядає безпеку не як захисний мур, а як проактивну здатність, призначену для передбачення, поглинання та адаптації до загроз. Замість того, щоб лише блокувати атаки, кіберстійкість наголошує на ранньому виявленні, рішучій реакції та швидкому відновленні, ставлячи безперервність бізнесу та стабільність операцій у центр стратегії...

Справжньою загрозою кібератаки часто є пов'язаний з нею простой, що призводить до зростання витрат через втрату доходів, штрафи з боку регуляторних органів та шкоду репутації. Організація, що має високу стійкість до збійних ситуацій, прагне запобігти такому операційному паралічу, забезпечуючи можливість швидкого відновлення критично важливих сервісів. Однак створення таких можливостей власними силами є складним завданням через необхідність наявності спеціалізованих навичок та постійного моніторингу, що створює операційний пробіл, який можуть заповнити ІТ-консультанти та постачальники керованих послуг безпеки (MSSP). MSSP забезпечують структуру, створюючи та тестуючи посібники з реагування на інциденти, і гарантують, що процеси відновлення розглядаються як основна бізнес-стратегія, а не лише як технічний резерв. Зрештою, цей проактивний підхід переосмислює поняття кіберзрілості, зміщуючи акцент із здатності організації протистояти атакам на її здатність передбачати та випереджати їх, перетворюючи стійкість на ключову стратегічну перевагу». (*Ivaan Captieux. When the cyber lock fails, what happens next? // ITWeb Limited (<https://itweb.africa/article/when-the-cyber-lock-fails-what-happens-next/RgeVDqPRmgj7KJN3>). 20.07.2026*).

«Хоча керівники компаній часто вважають, що кіберзагрози походять переважно від зовнішніх суб'єктів, нещодавнє дослідження компанії Fastly показує, що програмні помилки стали причиною 54% кіберінцидентів у Азіатсько-Тихоокеанському регіоні у 2025 році, випередивши зовнішні атаки, частка яких склала 43%. Ця вражаюча зміна пропорцій підкреслює зростаючу вразливість компаній: чим швидше організації розробляють продукти, тим більше вони наражаються на технічні ризики, спричинені власними діями. Швидке впровадження розробки з використанням штучного інтелекту, яку часто називають «vibe coding», скоротило цикли випуску, водночас створивши безпрецедентну операційну складність. Під сильним тиском щодо швидкого випуску продуктів інженерні команди регулярно відкладають на другий план перевірку коду, тестування та управління конфігурацією, що дозволяє дефектам потрапляти у виробництво. За іронією долі, значна частина продуктивності, отриманої завдяки штучному інтелекту, наразі втрачається, оскільки розробники витрачають значний час на діагностику та виправлення помилкового коду, який спочатку був згенерований саме штучним інтелектом...

Ця самопричинена вразливість значно посилюється масштабами організації та складністю середовища. У 2025 році великі підприємства з чисельністю персоналу понад 10 000 співробітників зазнали в середньому 57 кіберінцидентів — це майже на 40% більше, ніж загальний середній показник, — що доводить: навіть великі бюджети та складні засоби безпеки не можуть компенсувати принципово хибні практики розгортання. У розгалужених корпоративних середовищах, що складаються з хмарних платформ, API та автоматизованих конвеєрів, навіть одна програмна помилка або помилка конфігурації може спричинити серйозні перебої в роботі, витік даних та штрафи з боку регуляторних органів навіть без втручання зовнішніх зловмисників. Ці технічні вразливості посилюються серйозними прогалинами в управлінні; компанія Fastly виявила, що понад 31% організацій, які ставлять штучний інтелект на перше місце, досі не мають чіткого уявлення про те, хто саме відповідає за реагування на інциденти, що залишає їх вкрай вразливими до тривалих операційних та репутаційних наслідків, коли системи неминуче виходять з ладу...

Щоб мінімізувати ці ризики, організації повинні відмовитися від традиційних централізованих моделей безпеки, що базуються на периметральному захисті, та інтегрувати заходи безпеки безпосередньо в процеси розробки програмного забезпечення, проектування платформ та робочі процеси DevOps. Цей перехід вимагає запровадження чітких політик управління, згідно з якими код, згенерований ШІ, підлягатиме таким самим суворим процесам тестування та перевірки, як і код, написаний людиною. Крім того, організації повинні застосовувати проактивний підхід «безпека за задумом», розглядаючи системи ШІ як привілейовані активи з жорстким контролем доступу та постійним моніторингом з першого дня. Це є особливо нагальним з огляду на попередження компанії Gartner про те, що до 2027 року понад 40% випадків витоку даних, пов'язаних зі штучним інтелектом, будуть спричинені неналежним транскордонним використанням генеративного ШІ. Зрештою, розгляд програмних помилок як першочергових ризиків для безпеки та інтеграція безпеки в життєвий цикл розробки не

перешкоджають інноваціям; навпаки, це забезпечує стабільну основу, яка дозволяє компаніям безпечно прискорювати темпи випуску нових версій, зберігаючи при цьому життєво важливу довіру клієнтів». (*Rachel Ler. Why software bugs now pose the biggest cyber risk // Frontier Enterprise (<https://www.frontier-enterprise.com/why-software-bugs-now-pose-the-biggest-cyber-risk/>). 15.07.2026*).

Сполучені Штати Америки, Канада та Мексика

«Адміністрація Трампа скасувала обмеження щодо останніх версій чат-бота Claude від компанії Anthropic після кількатижневої заборони, пов'язаної з проблемами кібербезпеки. Компанія Anthropic повідомляє, що Claude Fable 5 тепер широко доступний, а доступ до його більш потужної моделі, Mythos 5, відновлюється, але лише для обмеженого кола організацій, що базуються в США та схвалені федеральним урядом. 12 червня Міністерство торгівлі заблокувало доступ іноземним громадянам до обох моделей, що, за словами Anthropic, змусило компанію вивести продукти з експлуатації для всіх користувачів незабаром після їхнього випуску... Компанія Anthropic пов'язує занепокоєння уряду зі звітом дослідників з кібербезпеки компанії Amazon — її головного постачальника хмарних послуг — які, як повідомляється, виявили спосіб обійти захисні механізми в моделі Fable 5, що потенційно дозволяє цій моделі виявляти та використовувати вразливості програмного забезпечення. Цей випадок став черговим підтвердженням більш загальних побоювань щодо того, що модель Mythos від Anthropic здатна виявляти недоліки програмного забезпечення таким чином, що це може бути використано як зброя для створення загрози критично важливим комп'ютерним мережам...

Тим часом головний конкурент Anthropic, компанія OpenAI, також заявила, що обмежить випуск своєї нової моделі штучного інтелекту GPT-5.6 Sol, зробивши її доступною лише для тимчасової групи клієнтів, затвердженої урядом. Такий підхід пов'язаний із нещодавнім указом президента Трампа, який встановлює механізм, за яким федеральний уряд має оцінювати ризики для національної безпеки, пов'язані з найсучаснішими системами штучного інтелекту, протягом 30 днів до їхнього публічного випуску; участь розробників у цьому процесі визначена як добровільна, оскільки процедура перевірки ще перебуває на стадії розробки...» (*Trump Administration Lifts Restrictions on Anthropic's Claude Models After Cybersecurity Alarm // Wired Business Media Publication (<https://www.securityweek.com/trump-administration-lifts-restrictions-on-anthropics-claude-models-after-cybersecurity-alarm/>). 02.07.2026*).

У 2026 році уряд Карні запровадив далекосяжні правила у сфері кібербезпеки, прийнявши законопроект С-8, яким запроваджується Закон про захист критично важливих кіберсистем (CCSPA); законопроект отримав королівське схвалення 15 червня 2026 року, і уряд планує поступово вводити

його положення в дію у терміни, встановлені наказом Губернатора в Раді. Після повного введення в дію закон покладатиме суворі та широкі зобов'язання у сфері кібербезпеки на «визначених операторів», відповідальних за критичні кіберсистеми, що регулюються на федеральному рівні, — системи, які мають важливе значення для національної безпеки та громадської безпеки... Визначені оператори будуть зобов'язані впроваджувати комплексні програми кібербезпеки (включно з управлінням ризиками ланцюга постачання та ризиками, пов'язаними з третіми сторонами), повідомляти про істотні зміни у своїх системах — особливо ті, що мають наслідки для національної безпеки — та негайно повідомляти про інциденти кібербезпеки, причому порушення можуть тягнути за собою суворі фінансові санкції, зокрема штрафи для організацій у розмірі до 15 мільйонів доларів на день. Оскільки очікується, що значна частина оперативних деталей CCSPA буде визначена в майбутніх нормативних актах — при цьому Губернатор у Раді може також видавати обов'язкові та конфіденційні «вказівки щодо кібербезпеки» без необхідності попередніх консультацій з операторами — організації повинні вже зараз розпочати підготовку, проводячи картографування та інвентаризацію критично важливих систем, вивчаючи нові повноваження регулятора, посилюючи кіберуправління та навчання, а також формуючи потенціал реагування не лише на порушення, а й на інспекції, аудити та розпорядження щодо дотримання вимог... Нагляд здійснюватиметься за конкретними секторами: наприклад, Управління з нагляду за фінансовими установами (OSFI) — у банківській сфері, Банк Канади — щодо клірингових та розрахункових систем, Канадський регулятор енергетики — щодо певних трубопроводів та ліній електропередач, Канадська комісія з ядерної безпеки — у сфері ядерної енергетики, а також відповідні міністри — у сфері телекомунікацій та транспорту, що регулюється на федеральному рівні. Закон також знову запроваджує значні адміністративні грошові штрафи та надає регуляторним органам розширені інструменти забезпечення дотримання законодавства, такі як право на вхід до приміщень для перевірки документації (з урахуванням обмежень), призначення внутрішніх аудитів, видача обов'язкових розпоряджень щодо дотримання вимог, а також запит або обмін інформацією, включаючи конфіденційну інформацію... З огляду на загальний характер закону, відсутність вимог щодо консультацій до його прийняття та можливість видачі конфіденційних регуляторних вказівок, практична рекомендація для операторів інфраструктури, що підпадають під федеральне регулювання, полягає в тому, щоб оцінити, чи поширюється на них дія Закону, визначити відповідний регуляторний орган, впровадити процеси управління та документування, що відповідають очікуваним нормам (включно з повідомленням про інциденти до CSE (Агентство з безпеки комунікацій) протягом 72 годин та веденням обліку), а також розглянути можливість раннього взаємодії з регуляторними органами для управління ризиками недотримання вимог та забезпечення безперебійності діяльності, готуючись вже зараз, щоб уникнути штрафних санкцій та посилити кіберстійкість у міру еволюції загроз». *(Hélène Deschamps Marquis, Matt Saunders, Chloe Hughes-Légaré, Aaron Grech. Critical Cyber Systems Protection Act: Bill C-8 is adopted // Borden Ladner Gervais LLP*

("BLG") (<https://www.blg.com/en/insights/2025/07/bill-c8-revives-canadian-cyber-security-reform-what-critical-infrastructure-sectors-need-to-know>). 02.07.2026).

«Агентство з кібербезпеки та безпеки інфраструктури США (CISA) має намір у вересні остаточно затвердити давно відкладене правило щодо повідомлення про інциденти в сфері кібербезпеки. Це правило, яке втілює в життя Закон про повідомлення про кіберінциденти щодо критичної інфраструктури 2022 року (CIRCA), зобов'яже суб'єктів критичної інфраструктури повідомляти CISA про значні кіберінциденти протягом 72 годин, а про будь-які виплати викупу за програмним забезпеченням-вимагачем — протягом 24 годин... Отримавши значну кількість відгуків від громадськості щодо свого початкового пропозиції, в якій передбачалося зменшення навантаження, пов'язаного зі звітуванням, та краща узгодженість з іншими федеральними вимогами, CISA наразі враховує ці зауваження для доопрацювання остаточного варіанту нормативного акту. Прийняття цього нормативного акту неодноразово відкладалося, і початковий термін — жовтень 2025 року — не було дотримано, проте наразі агентство продовжує роботу над ним після проведення додаткових зустрічей із зацікавленими сторонами». (*Lisbeth Perez. CISA Eyes September Date for Final Cyber Incident Reporting Rule // MeriTalk* (<https://www.meritalk.com/articles/cisa-eyes-september-date-for-final-cyber-incident-reporting-rule/>). 07.07.2026).

«Нещодавно армія США вимкнула та відновила роботу двох своїх веб-сайтів на базі WordPress — «Open Innovation Lab» та «AI Integration Center» — після того, як хакери змінили вміст їхніх сторінок помилок, розмістивши на них прокурдські повідомлення та грубі образи на адресу президента Дональда Трампа. Як виявив дослідник у сфері безпеки Рональд Лавелейс і про що вперше повідомило видання Cyberscoop, ці зламані сторінки з'являлися щоразу, коли користувач намагався перейти за неіснуючим URL-адресою... У зміненому тексті містився заклик до створення «вільного Курдистану», згадувався нинішній посол США в Туреччині Том Баррак, а президента Трампа називали «злодієм» і «педофілом» — ймовірно, маючи на увазі його часті згадки в матеріалах Міністерства юстиції щодо Джеффри Епштейна. Хоча досі залишається незрозумілим, як саме хакери отримали доступ до сайтів і чи були викрадені якісь дані, армія наразі розслідує цей інцидент... Цей випадок вандалізму є останнім у серії хактивістських атак, спрямованих проти систем федерального уряду; раніше цього року хакери оприлюднили конфіденційні дані про контракти Міністерства внутрішньої безпеки (DHS) на знак протесту проти депортацій, що здійснюються Імміграційною та митною службою (ICE), а саме цього тижня DHS підтвердило ще один випадок порушення безпеки, пов'язаний з однією з його платформ обміну розвідданими, якою користуються федеральні, штатні та місцеві органи влади». (*Zack Whittaker. Hacktivists call out Trump by hacking and defacing US Army websites // TechCrunch Media LLC.* (<https://techcrunch.com/2026/07/07/hacktivists-call-out-trump-by-hacking-and-defacing-us-army-websites/>). 07.07.2026).

«Канадське агентство з безпеки комунікацій (CSE) повідомило, що ситуація з кіберзагрозами в країні загострюється, а іноземні супротивники та кіберзлочинці дедалі частіше націлюються на критичні системи та ключові служби, що мають життєво важливе значення для національної безпеки та економічної стабільності. У своєму щорічному звіті за 2025–2026 роки CSE наголосило на розширенні співпраці з урядом, промисловістю та міжнародними партнерами з метою зміцнення кіберстійкості, зазначивши, що Канадський центр кібербезпеки відреагував на понад 3 200 кіберінцидентів, провів 522 зустрічі з зацікавленими сторонами у сфері критичної інфраструктури та випустив численні публікації з кібербезпеки, оцінки загроз та оперативні брифінги, щоб допомогти організаціям захищатися від нових загроз. У звіті підкреслюються зростаючі ризики, з якими стикається промислова база Канади, зокрема розслідування складних операцій з використанням програм-вимагачів як послуги, що стали причиною понад 25 інцидентів у транспортній, медичній, фармацевтичній та бізнес-галузях...

Протягом 2025–2026 років CSE зміцнило свої партнерські відносини завдяки численним зустрічам, виступам, галузевим заходам та настільним навчанням, спрямованим на підготовку до нових загроз, таких як квантові обчислення. Агентство продовжує інвестувати в потенціал кіберзахисту, безпечну цифрову інфраструктуру, штучний інтелект та спільні наукові дослідження, одночасно плануючи створення нових центрів обробки даних і тісніше співпрацюючи з промисловістю та науковими колами для протидії складним загрозам...

Діяльність CSE спрямована на підтримку національної оборони та безпеки; агентство співпрацює з Канадськими збройними силами, Міністерством національної оборони, Канадською береговою охороною та іншими федеральними відомствами з метою зміцнення глобального авторитету Канади як надійного партнера шляхом обміну розвідданими та оперативної підтримки, зокрема в рамках альянсу «Five Eyes». У рамках свого мандату агентство через Канадський центр кібербезпеки надає важливі рекомендації урядовим та приватним структурам, сприяючи підвищенню обізнаності, стійкості та готовності по всій країні...

Агентство відреагувало на понад 3 200 кіберінцидентів, що зачепили федеральні установи та критично важливі сектори, надавши технічні оцінки, рекомендації щодо управління інцидентами та аналітичні дані для мінімізації збитків та підвищення стійкості систем. Телекомунікаційні мережі, що мають життєво важливе значення для інтернет-інфраструктури Канади, залишаються головними цілями шпигунства, що спонукає CSE до постійних зусиль із посилення безпеки мереж 3G, 4G та 5G в рамках Програми кіберстійкості телекомунікацій. Агентство також займалося питаннями ризиків у сфері морського транспорту та водної інфраструктури, публікуючи оцінки загроз та практичні рекомендації, щоб допомогти операторам захиститися від кіберзагроз, які можуть порушити роботу портів, судноплавство та надання життєво важливих послуг...» **(Anna Ribeiro. Canada's CSE report details rising cyber threats, ransomware investigations, critical infrastructure protection efforts // Industrial Cyber (<https://industrialcyber.co/threats-attacks/canadas-cse-report-details-rising-cyber-threats-ransomware-investigations-critical-infrastructure-protection-efforts/>). 08.07.2026).**

«Фінансовий сектор Мексики стикається з серйозною проблемою кібербезпеки на двох фронтах, оскільки як банківська інфраструктура, так і клієнти банків стикаються з дедалі більш витонченими атаками, що базуються на штучному інтелекті. За даними Банку Мексики (Banxico), у 2025 році щонайменше три фінансові установи зазнали прямих кібератак, що призвело до перебоїв у роботі та збитків на суму понад 1,8 млн доларів США. Хоча великі банки збільшують інвестиції в інфраструктуру безпеки, середні та дрібні установи часто відстають за швидкістю реагування та рівнем готовності, намагаючись не відставати від зловмисників, які використовують автоматизовані інструменти та програми-вимагачі...

Водночас стрімке поширення онлайн-фінансових послуг спричинило значний сплеск цифрового шахрайства щодо споживачів. Кількість заяв про шахрайство щодо комерційних банків на початку 2026 року зросла на 18%, тоді як кількість заяв щодо інших фінансових установ різко зросла майже на 49%. Кіберзлочинці активно використовують штучний інтелект для проведення персоналізованих кампаній з фішингу, вішингу, створення «діпфейків» та спуфінгу. Як наслідок, змінюється демографічний склад жертв: хоча люди похилого віку залишаються вразливими, кількість скарг на шахрайство найшвидше зростає серед осіб віком від 18 до 29 років, які активно користуються мобільним банкінгом... Щоб протидіяти цій мінливій загрозі, експерти з кібербезпеки наголошують на необхідності переходу банків від реактивних заходів захисту до проактивного забезпечення стійкості шляхом посилення аутентифікації користувачів, мікросегментації та впровадження систем виявлення загроз на основі штучного інтелекту, здатних одночасно аналізувати тисячі сповіщень. Крім того, посилення співпраці між регуляторними органами та фінансовими установами — наприклад, нещодавні ініціативи CONDUSEF щодо виявлення шахрайських телефонних номерів — має вирішальне значення для пом'якшення наслідків кризи, яка, за оцінками, у 2025 році коштуватиме Мексиці 7,9 млрд доларів США у вигляді збитків, пов'язаних із шахрайством». *(Diego Valverde. AI-Driven Cyberattacks, Fraud Pressure Mexico's Banks // Mexico Business Company (https://mexicobusiness.news/cybersecurity/news/ai-driven-cyberattacks-fraud-pressure-mexicos-banks). 08.07.2026).*

«Міністерство війни на чолі з Пітом Хегсетом призупинило впровадження другої фази Сертифікації моделі зрілості кібербезпеки (СММС), відклавши запланований на листопад 2026 року перехід до обов'язкового дотримання вимог. Відповідно до меморандуму, підписаного головним інформаційним директором Крістен Девіс, міністерство призупинило виконання запланованих етапів, обмежило нові закупівлі самооцінками рівнів 1 та 2, а також створило 60-денну робочу групу з реформування СММС для перегляду структури сертифікації. Заступник міністра оборони з питань закупівель та забезпечення Майкл Даффі пояснив, що ця реформа має на меті зменшити паралізуючі витрати, пов'язані з СММС, зберігаючи при цьому інновації та розширюючи участь усього оборонно-

промислового комплексу. Девіс також зазначила, що існуючу модель стало складно масштабувати, оскільки оцінку потребують понад 100 000 підрядників, але нинішня екосистема має лише частку цієї пропускну здатності, незважаючи на те, що понад 1 200 організацій уже успішно пройшли сертифікацію...

Це несподіване призупинення спричинило значні короткострокові порушення на ринку кібербезпеки. Оскільки термін у листопаді 2026 року виступав головним каталізатором, що зумовлював терміновість дій, очікується, що його скасування сповільнить прийняття рішень щодо закупівель, затримає процес сертифікації та створить фінансову невизначеність для оборонних підрядників, постачальників програмного забезпечення та сторонніх організацій з оцінки СММС, які узгодили свої плани найму персоналу та операційні моделі з урахуванням початкового графіку...

Важливо, що підрядники оборонної галузі не повинні помилково тлумачити цю затримку у впровадженні як призупинення їхніх основних обов'язків щодо забезпечення безпеки. Міністерство чітко зазначило, що існуючі договірні вимоги щодо кібербезпеки залишаються в силі в повному обсязі. Це включає обов'язкове дотримання Спеціального видання NIST 800-171, редакція 2, пункту 252.204-7012 DFARS, планів безпеки систем, а також зобов'язання точно відображати стан кібербезпеки за допомогою самооцінок у рамках Системи оцінки ризиків ефективності постачальників (Supplier Performance Risk System). Крім того, Ініціатива Міністерства юстиції щодо боротьби з цивільним кібершахрайством продовжує діяти. Замість того, щоб призупиняти інвестиції в безпеку, організаціям настійно рекомендується розглядати цей додатковий час як можливість усунути прогалини в готовності, зменшити технічний борг, покращити управління ідентифікацією та повністю впровадити 110 обов'язкових заходів контролю безпеки, щоб бути готовими незалежно від того, як буде перероблена остаточна система сертифікації СММС». *(Emil Sayegh. The Pentagon Just Paused Its Cybersecurity Certification Program. Here's What Everyone Is Missing // Forbes Media LLC (<https://www.forbes.com/sites/emilsayegh/2026/07/14/the-pentagon-just-paused-its-cybersecurity-certification-program-heres-what-everyone-is-missing/>). 14.07.2026).*

«Федеральне агентство США з кібербезпеки CISA нещодавно визнало у звіті про аналіз інциденту, що не мало готового плану реагування після того, як у травні співробітник підрядника публічно оприлюднив конфіденційні ключі та облікові дані для систем уряду США у загальнодоступному репозиторії GitHub. Цю витік спочатку виявив дослідник з компанії з кібербезпеки GitGuardian, який, не отримавши відповіді від підрядника, повідомив про це незалежному журналісту Браяну Кребсу. Лише після того, як Кребс зв'язався з CISA, агентство вимкнуло репозиторій, анулювало та замінило викриті облікові дані, а згодом підтвердило, що дані клієнтів чи операції не були скомпрометовані...

У своєму аналізі подій CISA визнала, що на початкових етапах кризи її співробітникам довелося імпровізувати та розробляти посібник з реагування на інциденти, підкресливши нагальну необхідність заздалегідь встановлених

протоколів реагування замість того, щоб поспіхом вирішувати проблеми в режимі реального часу. Агентство також зазначило, що його канали комунікації з дослідниками у сфері безпеки були недостатньо чітко визначені, і з того часу їх було оновлено для прискорення процесу оповіщення. Цей збій в роботі стався у складний для CISA період: з початку другого терміну президентства Дональда Трампа у січні 2025 року агентство не мало постійного директора та стикалося з скороченням бюджету, відпустками без збереження зарплати та звільненнями, що торкнулися приблизно третини його персоналу». (*Zack Whittaker. US cyber agency CISA had to build its incident playbook during the incident, agency reveals // TechCrunch Media LLC. (<https://techcrunch.com/2026/07/10/us-cyber-agency-cisa-had-to-build-its-incident-playbook-during-the-incident-agency-reveals/>). 10.07.2026*).

«Адміністрація малого бізнесу США (SBA) позитивно оцінила рішення Міністерства оборони (DoW) призупинити застосування вимог другої фази Сертифікації за Моделлю зрілості кібербезпеки (СММС), які мали набути чинності 10 листопада 2026 року. Адміністратор SBA Келлі Леффлер високо оцінила це рішення, зазначивши, що, хоча малі підприємства віддані справі забезпечення національної кібербезпеки, пов'язані з цим бюрократичні витрати не повинні унеможливлювати діяльність життєво важливих компаній, які підтримують оборонну промислову базу... Програма СММС, розроблена для захисту конфіденційної федеральної інформації за допомогою багаторівневої системи сертифікації, зіткнулася з гострою критикою після того, як аналіз SBA показав, що дотримання вимог — включаючи оцінки, що проводяться сторонніми організаціями — може обійтися малим підприємствам у суму до 600 000 доларів. Впровадження фази II згідно з планом вимагало б дотримання вимог понад 120 000 малих оборонних підрядників, що загрожувало перевантаженням приблизно 100 наявних затверджених оцінювачів, створенням серйозних вузьких місць, а також значними втратами доходів і перебоями в ланцюгах постачання... Це призупинення стає приводом для проведення Міністерством оборони (DoW) всебічного перегляду, спрямованого на переорієнтацію програми з метою збереження високих стандартів кібербезпеки, одночасно спрощуючи процеси забезпечення відповідності вимогам та зменшуючи витрати для малих підприємств. Зрештою, така спільна пауза надає малим виробникам вкрай необхідну перепочинку від обтяжливих нормативних вимог і має на меті сприяти створенню більш гнучкого, інклюзивного та конкурентоспроможного ланцюга поставок для оборонної галузі». (*Sarah Lewis. SBA Applauds Suspension of Costly Cybersecurity Requirements for Small Firms // Small Business Trends LLC. (<https://smallbiztrends.com/sba-applauds-suspension-of-costly-cybersecurity-requirements-for-small-firms/>). 16.07.2026*).

«Нещодавній звіт Управління з питань урядової підзвітності (GAO) виявляє значні прогалини в кібербезпеці та плутанину в нормативно-правовій базі як в Адміністрації транспортної безпеки (TSA), так і у Федеральному управлінні цивільної авіації (FAA). За даними цього наглядового органу, TSA діє

на основі застарілої «Дорожньої карти з кібербезпеки» 2018 року, яка вже не відповідає поточним стратегіям Міністерства внутрішньої безпеки. Крім того, нездатність TSA чітко визначити внутрішні функції у сфері кібербезпеки спричинила значну плутанину серед зацікавлених сторін авіаційної галузі щодо меж компетенції обох відомств, що змусило деяких представників галузі засумніватися в ресурсах, повноваженнях та регуляторній компетентності TSA... Хоча FAA чіткіше визначила свої обов'язки, у інших критично важливих сферах вона не відповідає федеральним стандартам. План впровадження моделі «нульової довіри» (Zero Trust) цього відомства не змінювався з серпня 2023 року і не відповідає більш ніж половині вимог, встановлених урядом. Крім того, FAA не має системи кібермоніторингу в режимі, близькому до реального часу, для більшості своїх критично важливих систем управління повітряним рухом, що створює потенційні ризики для 44 000 рейсів та 3 мільйонів пасажирів, які щодня покладаються на цю інфраструктуру... У звіті також висвітлюються питання фінансової прозорості: зазначається, що Федеральне управління цивільної авіації (FAA) не надало Управлінню з питань управління та бюджету повних даних про свої витрати на кібербезпеку за фінансові роки з 2024 по 2026, через що Конгрес не мав повного уявлення про бюджет. Ці тривожні висновки були передані комітетам Конгресу лише за кілька годин до того, як Девід Каммінс, кандидат президента Трампа на посаду голови Адміністрації транспортної безпеки (TSA), дав свідчення перед Сенатом». *(Mary McCue Bell. Aviation cybersecurity has key shortfalls, watchdog warns Congress // The Washington Times, LLC (https://www.washingtontimes.com/news/2026/jul/16/aviation-cybersecurity-key-shortfalls-watchdog-warns-congress/). 16.07.2026).*

«Комітет Сенату США з питань навколишнього середовища та громадських робіт одногolosно схвалив двопартійний «Закон про розвиток водних ресурсів 2026 року» (WRDA 2026), поданий сенаторами Шеллі Мур Капіто, Шелдоном Вайтхаусом, Кевіном Крамером, Анджелою Олсобрукс та Адамом Шиффом. Цей закон санкціонує проведення 61 техніко-економічного обґрунтування та реалізацію 15 нових або модифікованих будівельних проєктів Корпусу інженерів армії США, спрямованих на управління ризиками повеней, навігацію та відновлення екосистем, а також поновлює дію програм Агентства з охорони навколишнього середовища (EPA) щодо інфраструктури питної води та стічних вод, таких як Державні оборотні фонди. Закон WRDA, вперше прийнятий у 1974 році з метою створення програм у сфері водних ресурсів та надання допомоги Корпусу інженерів армії США у розвитку торгівлі на водних шляхах, підлягає періодичному поновленню. Версія 2026 року активно реагує на сучасні виклики, запроваджуючи комплексні положення, спрямовані на посилення кібербезпеки у критично важливих системах водопостачання, що переживають цифрову трансформацію...

З метою протидії зростаючим кіберризикам, пов'язаним із підключеними оперативними технологіями, віддаленим доступом та хмарними сервісами у водогосподарському секторі, закон WRDA 2026 розширює сферу дії існуючих

програм забезпечення стійкості водогосподарської інфраструктури, щоб чітко включити до них зменшення вразливостей у сфері кібербезпеки поряд із захистом від природних небезпек. Згідно з оновленою системою, заявники, які претендують на федеральне фінансування водогосподарської інфраструктури, повинні виявити потенційні кібервразливості та пояснити, як їхні пропонувані проєкти сприятимуть зменшенню цих ризиків; при цьому критерії планування та оцінки оновлено з метою аналізу інцидентів у сфері кібербезпеки в рамках більш широкого розгляду проєктів. Законопроект передбачає виділення 25 мільйонів доларів щорічно на фінансові роки з 2027 по 2030 для цих ініціатив із забезпечення стійкості, замінивши попереднє фінансування. Він також дозволяє надавати гранти на підтримку впровадження та обслуговування технологій цифрової інфраструктури в сільських районах, що охоплюють об'єкти питного водопостачання, системи відведення дощових вод, опріснення води та накопичення води у водоносних горизонтах. Ці гранти будуть спрямовані на фінансування навчання з кібербезпеки на місцях, технічну допомогу та захисні заходи для керівників і операторів комунальних підприємств...» (*Anna Ribeiro. US Senate committee advances WRDA 2026, expanding cybersecurity support for critical water infrastructure // Industrial Cyber* (<https://industrialcyber.co/utilities-energy-power-water-waste/us-senate-committee-advances-wrda-2026-expanding-cybersecurity-support-for-critical-water-infrastructure/>). 20.07.2026).

«Згідно з нормами, прийнятими Агентством з захисту приватних даних Каліфорнії (CIPA), компанії, що ведуть діяльність у Каліфорнії та відповідають певним критеріям щодо обсягу доходу або обсягів обробки даних, зобов'язані проводити щорічні аудити кібербезпеки. Ці незалежні оцінки, за результатами яких з 1 квітня 2028 року необхідно подавати сертифікат відповідності, мають охоплювати до 18 окремих компонентів програми кібербезпеки організації. Хоча остаточний термін залежить від річного доходу, 2026 рік є вирішальним для організацій, які мають розпочати підготовку. Проактивна підготовка дозволяє підприємствам виявити недоліки, ефективно використовувати наявні інвестиції в безпеку та налагодити ефективний робочий процес аудиту задовго до початку офіційного регуляторного контролю...

Основою ефективної стратегії підготовки у 2026 році є проведення комплексної оцінки прогалин та імітаційного пробного аудиту. Оцінка прогалин визначає сферу охоплення аудиту шляхом виявлення всіх критично важливих систем, допоміжної інфраструктури та хмарних середовищ, у яких зберігаються, обробляються або передаються персональні дані мешканців Каліфорнії. Після визначення сфери охоплення організації повинні оцінити свої поточні заходи безпеки відповідно до 18 обов'язкових напрямків, серед яких — управління доступом, мережева безпека та реагування на інциденти. Цей крок є критично важливим для забезпечення того, щоб існуючі заходи контролю дійсно піддавалися аудиту; організації повинні бути готові надати конкретні операційні докази — такі як звіти про сканування вразливостей, журнали багатофакторної автентифікації та записи про управління виправленнями — а не просто покладатися на письмові

політики. Після цієї оцінки імітаційний аудит відтворює реальний процес перевірки, що дозволяє організаціям підготувати відповідальних за заходи контролю до співбесід, підтвердити, що повсякденні практики відповідають офіційним політикам, та усунути невирішені прогалини в безпеці в умовах, що не несуть серйозних ризиків...

З метою оптимізації ресурсів та зменшення навантаження, пов'язаного з аудитом, організаціям слід визначити, як повторно використовувати доказові матеріали з існуючих систем забезпечення відповідності, таких як перевірки SOC 2, сертифікації ISO 27001 або оцінки за Рамками кібербезпеки NIST, які часто значною мірою збігаються з вимогами CCPA. Крім того, підприємства повинні розпочати процес вибору незалежного аудитора, який не має конфлікту інтересів і володіє технічними та нормативними знаннями, необхідними для оцінки програм безпеки на рівні підприємства. Якщо чекати до року проведення аудиту, щоб розробити заходи контролю та зібрати документацію, це, ймовірно, призведе до перебоїв у роботі та високих витрат на забезпечення відповідності вимогам. Почавши ці підготовчі кроки заздалегідь, організації можуть створити обґрунтовану, чітко структуровану основу для забезпечення відповідності вимогам, яка успішно відповідатиме суворим стандартам Каліфорнії щодо захисту персональних даних». (*Elizabeth Kwok, Ryan Smyth. How To Prepare for a CCPA Cybersecurity Audit // FTI Consulting, Inc. (https://www.fticonsulting.com/insights/articles/how-prepare-ccpa-cybersecurity-audit). 20.07.2026*).

Країни ЄС та Великобританія

«У міру просування процесу перегляду Закону ЄС про кібербезпеку (CSA 2) запропонована система, яка надає Європейській комісії повноваження визначати та виключати з ринку ЄС постачальників ІКТ з третіх країн, що становлять «високий ризик», стикається зі значним опором. Ця пропозиція передбачає запровадження горизонтальної системи, яка вимагатиме виключення таких постачальників із критично важливих секторів, програм фінансування ЄС, процесів стандартизації та державних закупівель. Однак у звіті про хід роботи, опублікованому Радою Європейського Союзу в травні 2026 року, зазначено, що кілька держав-членів ставлять під сумнів методологію пропозиції, її потенційний вплив та правові підстави... Зокрема, держави-члени стурбовані тим, що Комісія втручається у питання національної безпеки — сферу, яка суворо зарезервована для окремих країн. Цю стурбованість значною мірою підкріплює нещодавній висновок генерального адвоката Чапети у справі «Elisa Eesti», в якому було ще раз підтверджено, що Європейський Союз не має повноважень диктувати державам-членам, як їм захищати свою національну безпеку. Надалі ірландське головування в Раді, яке триватиме протягом другої половини 2026 року, матиме завдання просувати це законодавство... Перед головуванням стоїть завдання безпечно інтегрувати правові принципи, висвітлені у справі «Elisa Eesti», у рамки CSA 2, не

чекаючи на остаточне рішення Суду ЄС. Ключові обговорення в рамках робочої групи заплановано на вересень 2026 року з метою досягнення потенційної політичної згоди до кінця року». *(EU Cybersecurity Act 2 Advances Amid Member States' Concerns Over EU Competence // Jones Day (https://www.jonesday.com/en/insights/2026/07/eu-cybersecurity-act-2-advances-amid-member-states-concerns-over-eu-competence). 06.2026).*

«Законопроект Великої Британії про кібербезпеку та стійкість є найзначнішим оновленням законодавства у сфері кібербезпеки з 2018 року. Він розширює коло зобов'язань за межі традиційних суб'єктів, включаючи до них постачальників керованих послуг, центри обробки даних та хмарні платформи, а також посилює безпеку ланцюгів постачання, вимоги щодо повідомлення про інциденти та механізми нагляду. Хоча може здаватися, що цей законопроект спрямований на великі організації, його вплив пошириться й на малі підприємства через договірні вимоги та очікування щодо безпеки, які висувають партнери та клієнти...

Законопроект наголошує на практичній стійкості, заохочуючи організації зосередитися на основних заходах з підготовки, таких як чіткі плани реагування на інциденти, надійні та ізольовані резервні копії, а також здатність оперативно повідомляти про порушення. Він також підкреслює важливість організаційної культури, зокрема створення середовища, в якому співробітники почуватимуться комфортно, повідомляючи про потенційні проблеми без страху. Загалом, законодавство покликане зміцнити всю цифрову екосистему, і підприємства, які проактивно впроваджують основні практики кібербезпеки та інтегрують стійкість у свою діяльність, матимуть кращі можливості для протидії майбутнім загрозам». *(Andrew Ingram. The cyber security and resilience bill: Practical steps to prepare your business //Adjacent Digital Politics Ltd (https://www.openaccessgovernment.org/the-cyber-security-and-resilience-bill-practical-steps-to-prepare-your-business/211211/). 06.07.2026).*

«Понад 60 провідних британських компаній, серед яких M&S, Nationwide, ITV, Microsoft UK та Cloudflare, підписали нову, підтриману урядом «Декларацію про кіберстійкість», спрямовану на посилення захисту від кіберзагроз, що стрімко зростають. Ця ініціатива, що є частиною Національного плану дій у сфері кібербезпеки Великої Британії, відображає зростання масштабів та вартості кіберзлочинності, яка зараз щорічно зачіпає мільйони підприємств і коштує економіці мільярди фунтів. Згідно з цією обіцянкою, організації зобов'язані вжити практичних заходів, таких як перенесення відповідальності за кібербезпеку на рівень правління, використання наданих урядом інструментів моніторингу та підвищення безпеки ланцюгів постачання за допомогою сертифікації...

Цей крок підкреслює зміну підходу до кібербезпеки — її розглядають не лише як технічну проблему, а як ключовий пріоритет бізнесу та керівництва, особливо з огляду на те, що штучний інтелект уможливило здійснення все більш витончених і

масштабних атак. Сприяючи спільній відповідальності та поширенню стандартних практик у різних галузях, уряд прагне підвищити стійкість усієї економіки, а державні посадовці закликають все більше організацій вживати подібних заходів для захисту своєї діяльності, клієнтів та критичної інфраструктури». (***Businesses across Britain sign up to Cyber Resilience Pledge as ministers urge firms to strengthen cyber defences*** // GOV.UK (<https://www.gov.uk/government/news/businesses-across-britain-sign-up-to-cyber-resilience-pledge-as-ministers-urge-firms-to-strengthen-cyber-defences>). 07.07.2026).

«Дослідження HDI «Cyber Study 2026», присвячене кіберризикам, з якими стикаються малі та середні підприємства (МСП) у Німеччині, показує, що, хоча кіберзбитки й досі широко розглядаються як серйозна загроза, середній розмір фінансових втрат від успішної атаки за останні роки різко знизився. Близько 60% респондентів зазначили, що кіберзбитки є важливим ризиком, а приблизно 31% оцінили ймовірність стати жертвою атаки протягом найближчих двох років як високу. Ці дані базуються на відповідях близько 1 100 осіб, які приймають рішення у сфері ІТ та страхування, а також самозайнятих осіб і фрілансерів... Згідно з оцінками дослідження, середній збиток від успішного кіберінциденту становить приблизно 25 000 євро, що є зниженням порівняно з щонайменше 68 000 євро, зафіксованими в кожному попередньому випуску опитування з 2022 року. HDI пояснює це більш звичними та ефективними заходами реагування з боку компаній, зокрема покращеними превентивними заходами та швидшим локалізуванням атак. Проте автори опитування застерігають від самозаспокоєння: якщо кібербезпека перейде з категорії «рутинних заходів» у категорію «недбалості», нові загрози все ще можуть завдати значної шкоди. Важливо зазначити, що кіберризик залишається екзистенційним для багатьох малих підприємств — приблизно кожен третій респондент зазначив, що серйозний інцидент може поставити під загрозу існування їхньої компанії, а малі підприємства (з річним доходом від 2,5 до 10 млн євро) виявилися особливо вразливими до екзистенційного тиску... За останні п'ять років 35% опитаних повідомили, що хоча б раз ставали об'єктом атак, але більшість компаній зазначили, що мають певний рівень підготовки: 87% мали технічні засоби захисту, такі як брандмауери та автоматичне резервне копіювання, 71% проводили навчання персоналу, а 69% вжили організаційних заходів, таких як ІТ-політики чи стратегії безпеки. Ці превентивні заходи корелювали з меншими збитками: компанії, які їх впровадили, повідомили про збитки, що в середньому були на 33% нижчими, ніж у тих, хто цього не зробив... У дослідженні також розглядається хмарні обчислення: з'ясувалося, що 54% компаній використовують хмарні сервіси для частини своєї ІТ-інфраструктури, часто називаючи покращену безпеку головною причиною, яка випереджає гнучкість, мобільність та міркування щодо витрат; однак воно також показує, що хмарні технології можуть створювати хибне відчуття безпеки, якщо не супроводжуються належними заходами контролю, оскільки 31% користувачів хмарних сервісів повідомили про перебої в роботі після інциденту, порівняно з 14% тих, хто не використовує хмарні технології. Що стосується шляхів атак, фішинг

залишився найпоширенішою точкою проникнення (про це повідомили 64% компаній, що зазнали атак), за ним йдуть електронні листи, що містять шкідливе програмне забезпечення (47%), та випадкове завантаження шкідливого програмного забезпечення (30%), що підкреслює важливість обізнаності та навчання персоналу поряд із технічними засобами захисту... У дослідженні також висвітлюються нові загрози, пов'язані зі штучним інтелектом, особливо ті, що спрямовані на соціальну маніпуляцію: 27% респондентів вважають шахрайство, пов'язане з генеральними директорами та платежами, актуальним ризиком, а 24% — атаки з використанням «діпфейків»; при цьому менша частка респондентів повідомила, що вже стикалася з такими атаками. Незважаючи на ці ризики, ставлення до штучного інтелекту загалом було відносно позитивним: 55% респондентів розглядають штучний інтелект як можливість (а 21% — скоріше як ризик), а деякі респонденти навіть вважають, що штучний інтелект підвищує їхню кіберстійкість. Загалом опитування показує, що середні підприємства краще звикли до кіберризиків і зазнають менших середніх збитків, ніж раніше, але не захищені від катастрофічних наслідків — особливо там, де людські помилки, недосконалі процеси або надмірна впевненість у системах, що надаються аутсорсинговими компаніями або працюють у хмарі, створюють прогалини, якими можуть скористатися зловмисники». *(Joseph Gabriel Lagonsin. German SMEs face lower cyber losses, but risks stay high // TechDay (<https://itbrief.co.uk/story/german-smes-face-lower-cyber-losses-but-risks-stay-high>). 08.07.2026).*

«Державний сектор Великої Британії стикається з дедалі складнішою ситуацією у сфері кібербезпеки, де атаки на критично важливі служби, інфраструктуру та ланцюги постачання вже не є поодинокими випадками, а стали постійною оперативною реальністю. Ці інциденти можуть порушити функціонування таких важливих державних служб, як охорона здоров'я та транспорт, через що стійкість до зловживань та безперебійність надання послуг стають не менш важливими, ніж профілактика. Водночас організації змушені боротися зі зростаючими загрозами в умовах обмежених бюджетів, нестачі кваліфікованих кадрів та застарілих систем, що змушує керівників переглянути традиційні стратегії безпеки...

Один із головних ризиків пов'язаний із взаємопов'язаними ланцюгами постачання, де вразливості у сторонніх постачальників можуть поставити під загрозу одразу кілька організацій. Обмежена прозорість цих мереж ускладнює забезпечення послідовної безпеки, особливо з огляду на те, що кіберзлочинці дедалі частіше використовують слабкі ланки. Хоча штучний інтелект сприяє зростанню складності та масштабів атак, багато випадків порушення безпеки все ще зумовлені базовими слабкими місцями, такими як неналежний контроль доступу або системи без встановлених оновлень...

У таких умовах успіх залежить не стільки від ресурсів, скільки від розуміння ризиків та визначення їх пріоритетності. Кібербезпека має стати невід'ємною частиною процесу прийняття рішень в організації, а керівництво повинно розглядати її як ключове оперативне та стратегічне питання. У міру продовження

цифрової трансформації надзвичайно важливо з самого початку інтегрувати заходи безпеки в нові системи та партнерські відносини. Зрештою, найбільш стійкими будуть ті організації, які зосередяться на критично важливих послугах, зміцнять ланцюги постачання та сформуєть потенціал для ефективного реагування у разі порушення безпеки». (*Christine Horton. The new reality for public sector cybersecurity in 2026 // THINK Digital Partners (https://www.thinkdigitalpartners.com/news/2026/07/08/the-new-reality-for-public-sector-cybersecurity-in-2026/). 08.07.2026*).

«Значно відійшовши від суворих післявоєнних норм, які обмежували діяльність розвідувальних служб Німеччини переважно спостереженням та звітуванням, країна готує новий закон, що надасть її розвідувальним службам можливості наступальних дій проти зростаючих кіберзагроз та гібридних загроз, зокрема тих, що пов'язані з Росією. Згідно з пропонованими змінами, німецька розвідка отримає повноваження активно протидіяти іноземним зловмисникам шляхом злому їхніх ІТ-систем, копіювання або видалення даних, виведення з ладу шкідливих інструментів та цілеспрямованого поширення дезінформації. Законопроект запроваджує диференційовані повноваження щодо спостереження залежно від рівня загрози та уточнює правила використання державного шпигунського програмного забезпечення та конфіденційних інформаторів, що потенційно дозволить залучати осіб віком від 16 років для протидії найсерйознішим загрозам... Крім того, проект передбачає суворе дотримання телекомунікаційними, цифровими, транспортними та фінансовими компаніями наказів про розкриття таємної інформації, виконання яких забезпечуватиметься за допомогою перевірок на місцях та штрафів у розмірі до 1 мільйона євро. Щоб збалансувати ці безпрецедентні розширення повноважень, реформа передбачає створення нового, єдиного наглядового органу — Незалежної наглядової ради, — яка замінить нинішні розрізнені органи та буде зобов'язана попередньо схвалювати заходи, що передбачають значне втручання в приватне життя, такі як прослуховування телефонних розмов, тривалі операції під прикриттям та спостереження за помешканнями». (*Markus Wacket. Germany seeks powers for spies to hack and disrupt attackers // Reuters (https://www.reuters.com/technology/germany-seeks-powers-spies-hack-disrupt-attackers-2026-07-02/). 02.07.2026*).

«Велика Британія оголосила про запуск «Cyber Shield» — амбітного проекту з кіберзахисту на національному рівні, який ґрунтується на усвідомленні того, що захист, що діє зі швидкістю людини, вже не є достатнім проти атак, що здійснюються зі швидкістю машин та базуються на штучному інтелекті. Ця ініціатива, очолювана GCHQ, NCSC та DSIT, передбачає розгортання агентних ШІ-помічників «Red» та «Blue», що працюють на основі передових моделей, таких як Mythos від Anthropic та сімейство GPT-5.6 від OpenAI. Агенти «Red» будуть постійно перевіряти національні та критичні інфраструктурні

системи на наявність вразливостей, тоді як агенти «Blue» патрулюватимуть мережі з метою виявлення, локалізації та, зрештою, усунення активних порушень, безперешкодно обмінюючись розвідданими між організаціями...

Однак на даний момент проект є скоріше концептуальним задумом, ніж конкретним планом. Він стикається зі значними труднощами щодо реалізації: не визначено ні термінів, ні бюджету, ні конкретних постачальників технологій. Крім того, передові, «неприв'язані» моделі штучного інтелекту, необхідні для виконання найскладніших завдань «щита», все ще перебувають на стадії закритого тестування, а це означає, що на початковому етапі впровадження, ймовірно, зосередиться виключно на виявленні вразливостей, а не на їх автоматизованому усуненні. Експерти галузі висловили скептицизм щодо реалістичності проекту та швидкості його впровадження... Критики зазначають, що уряд Великої Британії вже стикається з величезним накопиченням застарілих ІТ-систем, які не оновлюються, та відсутністю елементарної наочності щодо мереж критичної інфраструктури. Відповідно, експерти попереджають, що впровадження сучасних агентів штучного інтелекту для захисту мереж, яким бракує елементарних заходів безпеки або базової наочності щодо активів, є вкрай недоцільним, припускаючи, що амбітна ініціатива уряду може реалізовуватися з бюрократичною повільністю і не зможе усунути нагальні, фундаментальні недоліки безпеки, які вже зараз є проблемою для країни». (*Scott Ikeda. "Cyber Shield," Britain's Agentic AI Cyber Defense Project, Prepares for the World of Machine-Speed Attacks // Rezonen Pte. Ltd. (<https://www.cpomagazine.com/cyber-security/cyber-shield-britains-agentic-ai-cyber-defense-project-prepares-for-the-world-of-machine-speed-attacks/>). 15.07.2026*).

«Звіт Wavestone «Огляд британських стартапів у сфері кібербезпеки 2026 року» (2026 UK Cybersecurity Startup Radar) показує, що сектор кібербезпеки у Великій Британії переживає значний сплеск створення нових підприємств, який супроводжується серйозними перешкодами у розширенні діяльності цих компаній. Дослідження, в якому було проаналізовано 235 організацій на ринку, показало, що кількість новостворених компаній зросла на 252% у порівнянні з попереднім роком — з 44 стартапів у минулому році до 155 у 2026 році. Незважаючи на цей стрімкий приплив нових учасників, кількість компаній, що досягли масштабування, у секторі залишилася на рівні всього дев'яти, що підкреслює низький коефіцієнт конверсії між інноваціями на ранніх етапах та зрілою діловою діяльністю. Крім того, у галузі спостерігається значний географічний зсув: 86% нещодавно виявлених стартапів (134 із 155) було засновано за межами Лондона, порівняно з 52% (23 із 44) роком раніше. Хоча Лондон залишається ключовим центром, регіональні технологічні кластери дедалі більше сприяють розповсюдженню підприємництва по всій країні...

Цьому регіональному розширенню протистоїть критичний дефіцит фінансування, який загрожує довгостроковому масштабуванню. Хоча кількість інвестиційних раундів на суму менше 2,5 млн фунтів стерлінгів зросла — головним чином завдяки дуже невеликим раундам на суму менше 100 000 фунтів стерлінгів — обсяг більших раундів фінансування, що перевищують цей поріг, продовжував

скорочуватися. Це позбавляє молоді компанії капіталу для зростання, необхідного для найму персоналу, розширення продажів та орієнтування у тривалих циклах закупівель великих корпоративних та державних замовників. Як наслідок, засновники стикаються з інтенсивним тиском у сфері продажів: 38% з них називають пошук потенційних клієнтів своїм найважливішим викликом, що випереджає технічну реалізацію та розробку продукту. Щоб подолати внутрішні обмеження та шукати більші ринки, 67% цих стартапів уже ведуть міжнародні продажі — це стратегія, яка може забезпечити життєво важливе зростання, але також перевантажує невеликі, недофінансовані команди, що намагаються впоратися з дотриманням транскордонних нормативних вимог та позиціонуванням на ринку...

З технологічної точки зору в цьому секторі спостерігається стрімка інтеграція штучного інтелекту: 62% стартапів у сфері кібербезпеки зараз використовують ШІ у своїх продуктах, тоді як у 2025 році цей показник становив лише 30%. Таке широке впровадження перетворило ШІ з унікальної переваги на стандартну функцію продукту, а це означає, що стартапам доводиться дедалі більше конкурувати за рахунок відносин із клієнтами, каналів збуту та ефективності реалізації, а не лише за рахунок технологічних заяв. Флоріан Пуше, партнер та керівник напрямку кібербезпеки та операційної стійкості у Wavestone, зазначив, що, хоча інновації у сфері кібербезпеки у Великій Британії розвиваються рекордними темпами за межами Лондона, засновники компаній продовжують стикатися з труднощами у пошуку потенційних клієнтів та залученні капіталу для зростання. Він попередив, що для того, щоб Велика Британія змогла створити суверенну систему кібербезпеки, внутрішній ринок повинен активно підтримувати та фінансувати компанії, які успішно розвиваються. Зрештою, величезний розрив між 155 новоствореними стартапами та лише дев'ятьма усталеними компаніями, що розширюють масштаби діяльності, підкреслює, що цей сектор переповнений підприємницькою енергією, але стикається з труднощами на вузькому шляху до зрілості». *(Sofiah Nichole Salivio. UK cybersecurity startups surge as scaleups stay rare // TechDay (<https://itbrief.co.uk/story/uk-cybersecurity-startups-surge-as-scaleups-stay-rare>). 21.07.2026).*

«На ринку, що ґрунтується на довірі, постачальники послуг з кібербезпеки стикаються зі значними комунікаційними викликами через високу важливість технічної точності, про що свідчать дорогоцінні кібератаки 2025 року на великі британські організації, такі як Marks & Spencer, Co-op та Jaguar Land Rover. Нове дослідження, проведене серед 152 фахівців з комунікацій у сфері кібербезпеки у Великій Британії, виявляє поширену проблему перебільшення: 99% респондентів зізналися, що стикалися з такими категоричними формулюваннями, як «100% захист» або «повністю захищений», у своїх маркетингових матеріалах або самі їх використовували. Крім того, понад половина цих фахівців стикалася з безпідставними або оманливими твердженнями, а 30% безпосередньо брали участь у їх використанні. Ця тенденція посилюється помітним розривом у рівні впевненості: хоча 86% фахівців висловлюють абсолютну

впевненість у маркетинговому контенті власної компанії, вони, як і раніше, дуже стурбовані перебільшеними твердженнями в галузі загалом...

Ця тенденція до непорозумінь підсилюється жорсткою глобальною конкуренцією — про що свідчить, зокрема, наявність 2 600 компаній у сфері кібербезпеки, що працюють лише у Великій Британії, — та постійною складністю пояснення надзвичайно складних технологій різноманітній аудиторії, особливо членам правління без технічної освіти, які контролюють бюджети на закупівлі. Ці комунікаційні збої несуть серйозні ризики, оскільки майже половина опитаних організацій зазнала комерційних збитків або репутаційних втрат через надмірно спрощені або неточні повідомлення. Навіть коли компанії проводять юридичну або технічну експертизу перед публікацією, 30% фахівців повідомляють, що їхні маркетингові повідомлення все одно регулярно неправильно розуміються покупцями...

Як наслідок, спостерігається надзвичайний попит на реформу в масштабах усієї галузі: 94% респондентів виступають за запровадження чіткіших стандартів комунікації або добровільного кодексу професійної етики, а 86% підтримують введення акредитації у сфері кібербезпеки для фахівців з комунікацій. Спеціалізований добровільний кодекс професійної поведінки допоміг би сформуванню реалістичні очікування, усунувши категоричні твердження, вимагаючи надійних доказів для маркетингових повідомлень та точно відображаючи можливості продукту. Зрештою, зміна маркетингового нарративу з неможливих обіцянок повної безпеки на конкретні поняття, такі як зниження ризиків, стійкість та швидке відновлення, є надзвичайно важливою для збереження довіри, від якої залежить сектор кібербезпеки». (*Hayley Goff. Lack of trust – why cyber security communications needs clearer standards // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/lack-of-trust-why-cyber-security-communications-needs-clearer-standards/). 19.07.2026).*

«У відкритому листі, опублікованому у квітні, уряд Великої Британії закликав підприємства негайно посилити свою кіберзахист, попередивши, що штучний інтелект прискорює кібератаки набагато швидше, ніж передбачалося раніше, автоматизуючи виявлення вразливостей програмного забезпечення та створення експлойтів у безпрецедентних масштабах. Це попередження підтверджується офіційним «Дослідженням порушень кібербезпеки 2025/2026», опублікованим Міністерством внутрішніх справ та Міністерством науки, інновацій та технологій (DSIT), яке показало, що 43% британських підприємств зазнали порушення або атаки протягом попередніх 12 місяців, причому фішинг залишається домінуючим вектором (38%). Штучний інтелект не створює цілком нових категорій загроз, а знижує бар'єр для входу на ринок, надаючи менш досвідченим зловмисникам доступ до передових засобів автоматизованої розвідки та швидкого використання вразливостей...»

Це прискорення технологічного розвитку значно підвищило вразливість підприємств: згідно з результатами «Глобального опитування з управління ризиками 2026» компанії Aon, кібератаки та витоки даних визнані головним

ризиком для підприємств до 2028 року. Незважаючи на цю загрозу, що насувається, все ще існує значний розрив у рівні готовності. Роб Кемп, генеральний директор Aon з питань комерційних ризиків у Великій Британії, зазначив, що багато компаній оцінюють свою підготовку лише як «дещо достатню» через фрагментованість системи управління, відсутність тестування сценаріїв інцидентів із використанням штучного інтелекту та схильність розглядати безпеку штучного інтелекту як проблему майбутнього. Цю стурбованість підтверджують дані DSIT, які показують, що лише близько 25% британських організацій, які наразі використовують штучний інтелект, впровадили заходи безпеки для управління пов'язаними з ним ризиками...

У відповідь на це зростання прогалин у захисті страхова галузь ретельно переглядає умови страхування від кіберзагроз. Страховики активно оновлюють свої моделі ризиків, щоб врахувати загрози, що посилюються завдяки штучному інтелекту, вимагаючи ретельнішого аналізу багатофакторної аутентифікації клієнтів, своєчасного встановлення оновлень та контролю привілейованого доступу. Для управління цими ризиками деякі страхові компанії вводять спеціальні додаткові умови або виключення щодо атак із використанням штучного інтелекту. Отже, щоб забезпечити можливість поновлення полісів та уникнути звуження варіантів страхового покриття, комерційні клієнти повинні створити на рівні ради директорів інформаційні панелі з ризиками, пов'язаними зі штучним інтелектом, із чітко визначеною відповідальністю за усунення порушень, оновити свої плани реагування на інциденти з урахуванням сценаріїв, пов'язаних зі штучним інтелектом, та активно порівнювати свої заходи безпеки з аналогічними заходами інших компаній у галузі». *(Mark Rosanes. UK cyber breach rate holds at 43% as AI widens attack threat // KM Business Information UK Ltd (<https://www.insurancebusinessmag.com/uk/news/cyber/uk-cyber-breach-rate-holds-at-43-as-ai-widens-attack-threat-582597.aspx>). 16.07.2026).*

Австралія та Нова Зеландія

«Оскільки кіберуразливості становлять дедалі більшу загрозу для критичної інфраструктури, життєво важливих послуг та національної безпеки Австралії, нинішній підхід, що ґрунтується на добровільному дотриманні вимог та ринкових стимулах, вже не є достатнім. Отже, Австралійський центр кібербезпеки (ACSC) повинен перетворитися на офіційний, незалежний регулятор у сфері кібербезпеки, подібний до Управління з контролю за лікарськими засобами у секторі охорони здоров'я. Хоча Австралійське управління радіорозвідки (ASD) продовжуватиме виконувати оперативні функції у сфері кіберзахисту та розвідки, ACSC, наділений відповідними повноваженнями, візьме на себе обов'язки з регулювання та забезпечення дотримання вимог... Цей новий орган буде встановлювати та забезпечувати дотримання обов'язкових стандартів кібербезпеки — таких як принципи «безпеки за рахунок проектування» та багатофакторна автентифікація — у критично важливих секторах державного та приватного

секторів. Що особливо важливо, ACSC буде незалежно сертифікувати технології та програмне забезпечення з високим рівнем ризику перед їх впровадженням у національні системи. Крім того, регулятор матиме повноваження офіційно розслідувати серйозні кіберінциденти, вимагати усунення системних вразливостей та накладати санкції за недотримання вимог... Спираючись на основні зобов'язання, запроваджені Законом про кібербезпеку 2024 року, ця зміна в регуляторній політиці враховує той факт, що кіберзагрози на сьогодні є серйозною проблемою громадської безпеки та питанням національної стійкості, що вимагає суворого нагляду з метою запобігання катастрофічним збоям у функціонуванні австралійської економіки та суспільства». (*Natalie Treloar. The ACSC should become Australia's cybersecurity regulator // The Australian Strategic Policy Institute Blog* (<https://www.aspistrategist.org.au/the-acsc-should-become-australias-cybersecurity-regulator/>). 13.07.2026).

Компанія WatchGuard Technologies попереджає австралійські організації про те, що кіберзлочинці дедалі частіше використовують операційний тиск і стислі терміни, пов'язані з закінченням фінансового року (EOFY) та великими світовими подіями, такими як Чемпіонат світу з футболу ФІФА. За словами Ентоні Деніела, керуючого директора WatchGuard у цьому регіоні, атаки, пов'язані з закінченням фінансового року, вже давно вийшли за межі звичайних підроблених рахунків-фактур; сьогодні надзвичайно витончені атаки на корпоративну електронну пошту та шахрайські схеми з підробкою особи безперешкодно інтегруються в повсякденні робочі процеси, вводячи в оману перевантажені фінансові та кадрові підрозділи, які обробляють великі обсяги запитів... Останні дані підкреслюють цю загрозу: Австралійське податкове управління повідомляє про щомісячне зростання кількості шахрайських дій із використанням підроблених особистих даних на 11%, а Національний центр боротьби з шахрайством зазначає, що у 2025 році через шахрайство було втрачено понад 2 млрд австралійських доларів. Ризик посилюється тим, що, згідно з дослідженням WatchGuard, 75% організацій зазнали кіберінциденту протягом минулого року, тоді як 54% не мають можливостей для безперервного моніторингу...

Ця ж вразливість стосується масштабних, взаємопов'язаних цифрових екосистем, необхідних для проведення таких глобальних подій, як Чемпіонат світу з футболу ФІФА, де будь-які збої в роботі систем продажу квитків, телетрансляцій або функціонування стадіонів можуть миттєво завдати репутаційної та фінансової шкоди. Оскільки неможливо запобігти проникненню кожної шахрайської атаки в мережу, Деніел радить компаніям перенести акцент з простого запобігання на надійне локалізування загроз та забезпечення стійкості. Організації повинні впроваджувати принципи «нульової довіри» (Zero Trust), застосовувати багатофакторну автентифікацію у критично важливих додатках та забезпечувати цілодобовий доступ до систем виявлення загроз на кінцевих точках і оперативного реагування на них. Зрештою, незалежно від того, чи йдеться про тиск у зв'язку з наближенням кінця фінансового року, чи про управління значним сплеском онлайн-трафіку під час глобальних спортивних подій, стійкі підприємства повинні

бути готові запобігти тому, щоб одна-єдина людська помилка переросла у катастрофічний злам у масштабах усієї системи». (*Sofiah Nichole Salivio. EOFY pressures drive cyber risk for Australian firms // TechDay (<https://securitybrief.com.au/story/eofy-pressures-drive-cyber-risk-for-australian-firms>). 06.07.2026*).

«Нещодавній витік даних у благодійній організації з надання кризової підтримки «Lifeline Australia» висвітлив критичні вразливості в некомерційному секторі країни та збігся у часі зі значними змінами в регуляторній та страховій сферах на австралійському кіберринку. 12 липня 2026 року сторонній зловмисник отримав доступ до даних співробітників та волонтерів Lifeline, а зловмисник із даркнету, що діє під ніком «2019», заявив, що викрав понад 10 000 записів — зокрема імена, адреси електронної пошти, дати народження, ідентифікаційні номери клієнтів та номери телефонів. Подальше розслідування Lifeline підтвердило, що доступ до частини інформації про співробітників та волонтерів дійсно був отриманий, хоча частина опублікованого набору даних була підроблена та сфальсифікована. Організація переконалася, що фінансові дані та інформація про осіб, які зверталися за допомогою, не були скомпрометовані, і з того часу почала повідомляти про це постраждалих осіб...

Цей інцидент є частиною більш широкої системної загрози, оскільки з січня 2026 року зловмисник під ніком «2019» активно атакує австралійські організації, зокрема Міжнародний кінофестиваль у Мельбурні, компанію Ochre Health, Австралійський центр рухомого зображення та компанію Hot Toner Australia. Для страховиків і перестраховиків такі серійні атаки на пов'язані між собою організації створюють серйозний ризик виникнення взаємопов'язаних збитків на рівні портфеля в рамках програм спільного перестрахування...

Регуляторні наслідки таких порушень були суттєво переглянуті в жовтні 2025 року, коли Федеральний суд зобов'язав компанію «Australian Clinical Labs» (ACL) сплатити 5,8 млн доларів у рамках перших в історії цивільних штрафів, накладених відповідно до Закону про захист персональних даних 1988 року. Суд наклав на ACL штраф у розмірі 4,2 млн доларів за невжиття розумних заходів для захисту персональних даних, 800 000 доларів за невиконання оцінки порушення протягом 30 днів та 800 000 доларів за неповідомлення Управління австралійського комісара з питань інформації (OAIC) у реалістичний термін від двох до трьох днів після виникнення підстав вважати, що порушення відбулося. Важливо, що розмір штрафу, накладеного на ACL, був обмежений згідно з режимом, що діяв до грудня 2022 року; за чинними правилами максимальні штрафи можуть сягати 50 мільйонів доларів, трикратного розміру отриманої вигоди або 30% річного обороту організації за кожне порушення. Цей прецедент за ACL також встановив, що організації не можуть уникнути відповідальності, надмірно покладаючись на експертизи третіх сторін. Це має велике значення для ситуації Lifeline, оскільки маніпуляції з викраденими даними ускладнюють визначення справжнього масштабу порушення, покладаючи тягар проведення швидкої та обґрунтованої оцінки повністю на саму організацію.

Незважаючи на ці суворі нормативні вимоги та задокументовану частоту кіберзагроз — одна кожні шість хвилин — некомерційний сектор Австралії залишається вкрай вразливим. Дані звіту Infoxchange за 2025 рік показують, що лише 23% некомерційних організацій мають задокументований план кібербезпеки, і цей показник активно стагнує або знижується через брак фінансування. Парадоксально, але попит на кіберстрахування знижується; частка австралійців, які мають кіберстрахування, впала другий рік поспіль — з 4,6% у 2024 році до 3,7% у 2025 році. Ця недостатність страхування зберігається, незважаючи на те, що економіка страхування кіберризиків є високоприбутковою: у кінці 2025 та на початку 2026 року було зафіксовано позитивні результати діяльності, при цьому валові підписані премії у березні 2026 року становили лише 32 мільйони доларів. Щоб усунути ці вразливості та розширити охоплення ринку, Страхова рада Австралії закликала уряд надавати страховикам дані про обов'язкове повідомлення про випадки використання програм-вимагачів, щоб сприяти зміцненню колективних заходів захисту». **(Roxanne Libatique. Lifeline breach exposes widening cyber insurance protection gap // KM Business Information Australia Pty Ltd (<https://www.insurancebusinessmag.com/au/news/cyber/lifeline-breach-exposes-widening-cyber-insurance-protection-gap-582306.aspx>). 14.07.2026).**

«Європейська комісія опублікувала «План дій щодо кібербезпеки та штучного інтелекту» — стратегічний дорожній план, спрямований на посилення контролю за передовими моделями ШІ до їх виходу на ринок ЄС, що зумовлено побоюваннями щодо того, що ШІ прискорює виявлення вразливостей та кібератаки. Хоча цей план не запроваджує нової системи дотримання вимог, він доповнює існуючі рамки, такі як Закон про ШІ та NIS2, передбачаючи створення в ЄС потенціалу для оцінки моделей, контрольоване тестування для критично важливих секторів (енергетика, транспорт, охорона здоров'я, фінанси та державне управління), а також розробку концепції безпечного доступу... Комісія очікує, що до 2027 року запрацює механізм незалежної оцінки для підтримки Європейського офісу з питань штучного інтелекту. Відповідно, під час процедур закупівель та перевірок безпеки підприємства можуть зіткнутися з посиленням тиском щодо ретельного документування поведінки моделей штучного інтелекту, програмних залежностей та заходів контролю з боку постачальників. Конкретні наслідки цього політичного курсу вже помітні у фінансовому секторі: Європейський центральний банк (ЄЦБ) зобов'язав значні фінансові установи до 31 жовтня 2026 року подати комплексні плани дій щодо кібербезпеки ШІ, які охоплюють питання управління, управління вразливостями та ризики, пов'язані з залученням сторонніх організацій... Хоча ця конкретна вимога стосується лише банківської діяльності, що перебуває під наглядом, вона пропонує практичну модель управління для всіх організацій, яка дозволяє відстежувати постачальників штучного інтелекту, контролювати доступ до систем та чітко визначати договірні обов'язки щодо розкриття інформації про вразливості та виправлення помилок». **(EU AI Cybersecurity Plan Brings Model Evaluation Into Enterprise Risk Planning //**

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

«Індійські власті розглядають можливість запровадження єдиної базової системи кібербезпеки для пристроїв «Інтернету речей» (IoT) на тлі зростання занепокоєння щодо розширення площі атаки, що створюється підключеними технологіями. Запропонований підхід застосовуватиметься до широкого спектру продуктів, зокрема до інтелектуальних лічильників, систем домашньої автоматизації, підключених до мережі побутових приладів, промислових датчиків, носимих пристроїв, медичного обладнання та інших пристроїв з доступом до Інтернету. Оскільки ці технології дедалі ширше інтегруються в побутові приміщення, підприємства, заводи та об'єкти критичної інфраструктури, чиновники вважають, що слабкі або непослідовні стандарти безпеки можуть наражати їх на більші кіберризики...

Тому уряд вивчає питання щодо встановлення мінімальних вимог до кібербезпеки підключених пристроїв перед їх виведенням на індійський ринок, приділяючи особливу увагу тестуванню продукції, оцінці вразливостей, цілісності програмного забезпечення та підвищенню прозорості в ланцюгах постачання. Запропонована система покликана забезпечити, щоб усі підключені продукти, незалежно від місця їх виробництва, відповідали індійським стандартам кібербезпеки перед введенням у експлуатацію...» (**Aabhas Sharma. Government weighs cybersecurity framework for IoT devices // Bennett, Coleman & Co. Ltd. (<https://timesofindia.indiatimes.com/business/india-business/government-weighs-cybersecurity-framework-for-iot-devices/articleshow/132354357.cms>). 13.07.2026).**

«Секретар з питань інформаційних технологій Індії С. Крішнан наголосив, що країна «не має іншого вибору», окрім як швидко розбудовувати власні потужності в галузі штучного інтелекту та кібербезпеки — зокрема в сферах моделей, даних та обчислювальної інфраструктури — для захисту своєї цифрової екосистеми від дедалі витонченіших загроз. Хоча стрімка цифровізація значно підвищила економічну ефективність, вона також піддала підприємства та громадян серйозним кіберризикам. Отже, кібербезпеку слід розглядати як системний ризик для всього підприємства та глибоко інтегрувати її в ширші рамки цифрового управління, захисту приватних даних та операційної стійкості. У цьому мінливому середовищі штучний інтелект діє як двосічний меч: з одного боку, він дає змогу зловмисникам здійснювати більш складні атаки, а з іншого — одночасно надає захисникам передові інструменти для швидшого виявлення загроз та реагування на них...

Щоб вирішити ці проблеми у фінансовому секторі, Міністерство електроніки та інформаційних технологій (MeitY) спільно з CERT-In, CSIRT-Fin та SISA опублікувало «Звіт про цифрові загрози на 2025–26 роки» для банківської сфери, сектору фінансових послуг та страхування (BFSI) і платіжної екосистеми. Основний висновок звіту полягає в тому, що проміжок часу між технологічною інновацією та її практичним застосуванням різко скоротився з кількох років до лічених тижнів. Загрози, які колись вважалися новими або епізодичними — зокрема, соціальна інженерія, крадіжка облікових даних, компрометація ланцюга постачання та зловживання хмарними сервісами — тепер стали стандартними методами атак. Важливо, що найшкідливіші сучасні атаки вже не схожі на традиційні вторгнення; натомість вони маскуються під легітимні сесії користувачів, затверджені платежі або маніпульовані робочі процеси, які практично не відрізняються від справжньої поведінки користувачів, доки шкода вже не завдана...

Ця стрімка еволюція зумовлена «асиметрією III» — явищем, за якого зловмисники з обмеженими ресурсами можуть використовувати III для здійснення складних атак зі швидкістю машини, випереджаючи захисні та регуляторні механізми, призначені для їх стримування. Щоб допомогти організаціям систематично виявляти та визначати пріоритетність цих ризиків, у звіті представлено «Анатомію кіберпровалу» — чотирирівневу архетипну модель прогалин, яка демонструє, що сучасні порушення безпеки рідко є поодинокими помилками, а скоріше ланцюгами взаємопов'язаних слабких місць. Щоб навести галузь на правильний шлях, у звіті наведено 18-місячний план дій, покликаний допомогти фінансовим установам перейти від базових засобів контролю до надзвичайно стійких архітектур безпеки, що працюють у режимі реального часу. Зрештою, у міру того як фінансова екосистема Індії стає дедалі більш взаємопов'язаною та орієнтованою на роботу в режимі реального часу, кіберстійкість має розглядатися як спільна, проактивна відповідальність усіх установ, регуляторних органів та партнерів у цифровому ланцюгу постачання». *(India Must Build Domestic AI " Cybersecurity Capabilities // Rediff.com India Limited* (<https://money.rediff.com/news/market/india-must-build-domestic-ai-cybersecurity-capabilities/50460320260713>). 13.07.2026).

«Національна команда реагування на комп'ютерні надзвичайні ситуації Пакистану (National CERT) опублікувала критичне попередження з питань кібербезпеки, в якому закликає організації державного та приватного секторів — зокрема урядові установи, фінансові установи, телекомунікаційні компанії та операторів критичної інфраструктури — негайно забезпечити захист своїх брандмауерів Fortinet та систем віртуальних приватних мереж (VPN). Це термінове попередження з'явилося на тлі масштабної глобальної кампанії кібервторгнень, в результаті якої було скомпрометовано приблизно 73 932 екземпляри брандмауерів Fortinet FortiGate у 194 країнах. Організовані кіберзлочинні угруповання використовують загальнодоступні інтерфейси управління FortiGate та застарілі механізми зберігання облікових даних для збору адміністративних облікових даних, злому логінів VPN та створення стійких точок

опори для горизонтального переміщення всередині внутрішніх мереж. National CERT попередила, що якщо не усунути цю вразливість, це може призвести до несанкціонованого адміністративного доступу, витоку конфіденційних даних, маніпулювання політиками безпеки брандмауера та серйозних ризиків для ланцюга поставок...

Щоб мінімізувати ці загрози, National CERT Пакистану визначив кілька заходів негайного реагування. Організації повинні надати пріоритет зменшенню вразливості шляхом негайного відключення інтерфейсів управління FortiGate від публічного Інтернету, оновлення до останніх підтримуваних версій FortiOS, зміни всіх паролів адміністраторів та впровадження багатофакторної автентифікації (MFA) як для адміністративних облікових записів, так і для облікових записів VPN. До заходів найвищого пріоритету також належать обмеження доступу до управління лише до надійних мереж, аудит середовищ Active Directory на наявність ознак горизонтального переміщення, а також постійний моніторинг журналів на предмет підозрілих входів адміністраторів, входів у неробочий час або з географічно нетипових локацій. National CERT закликав організації розглядати цей інцидент як активну потенційну загрозу, а не як звичайне оновлення програмного забезпечення, та наказав їм негайно повідомляти агентство про будь-які підозри щодо порушень безпеки або несанкціонованих дій». *(Tahir Amin. Pakistan issues Fortinet cybersecurity warning // Business Recorder (https://www.brecorder.com/news/40429942). 14.07.2026).*

«Відповідно до запропонованої Пакистанської системи інформаційної безпеки (PISF), міністерства, відомства та інші організації державного сектору будуть зобов'язані дотримуватися обов'язкових термінів та стандартизованих процедур щодо повідомлення про підтверджені інциденти у сфері кібербезпеки. Організації, визначені як критична інформаційна інфраструктура (СІІ), повинні негайно повідомляти про підтверджені інциденти відповідним галузевим регуляторним органам, командам реагування на комп'ютерні надзвичайні ситуації (CERT) та національній CERT, а потім протягом 72 годин надати детальний звіт про інцидент. Організації, що не віднесені до категорії СІІ, повинні повідомляти про підтверджені інциденти відповідному галузевому регулятору або CERT протягом 120 годин...

З метою забезпечення дотримання цих вимог ця система передбачає, що кожна організація має розробити комплексну політику управління інцидентами кібербезпеки, яка охоплює підготовку, виявлення, реагування, мінімізацію наслідків, звітування, відновлення, усунення наслідків та аналіз отриманого досвіду. Організації повинні класифікувати інциденти за ступенем серйозності та наслідків, чітко визначити ролі у реагуванні та керувати інцидентами за допомогою затвердженої системи реагування, яка забезпечує розподіл відповідальності та підзвітність. Для підтримання оперативної готовності та виявлення слабких місць у процедурах організації повинні регулярно проводити навчальні тренування та забезпечувати наявність достатніх ресурсів і кваліфікованого персоналу. Крім того, у рамках цієї системи рекомендується оцінювати необхідність створення центрів

оперативної безпеки (SOC), використання платформ управління інформацією та подіями безпеки (SIEM) та інших рішень для моніторингу...

Після будь-якого інциденту організації зобов'язані задокументувати отриманий досвід та вжити коригувальних заходів у встановлені терміни, щоб запобігти повторенню подібних випадків. Нарешті, PISF пов'язує реагування на інциденти з плануванням забезпечення безперервності діяльності та відновлення після надзвичайних ситуацій, вимагаючи від організацій визначати цілі відновлення, проводити щорічні навчання з забезпечення безперервності діяльності та підтримувати задокументовані процедури комунікації, відновлення та реставрації під час кібернадзвичайних ситуацій». (*Govt Sets Strict Deadlines for Reporting Cyberattacks // ProPakistani.PK (<https://propakistani.pk/2026/07/14/govt-sets-strict-deadlines-for-reporting-cyberattacks/>). 14.07.2026*).

Ізраїль, Туреччина та країни Близького сходу

«2026 рік став надзвичайно активним для ізраїльського ринку злиттів і поглинань у сфері технологій: лише за перші шість місяців було оголошено про понад 50 угод з придбання ізраїльських стартапів у таких галузях, як кібербезпека, напівпровідники, фінтех, охорона здоров'я, корпоративне програмне забезпечення та оборона. Активність на ринку — від угод на десятки мільйонів до багатомільярдних транзакцій — значною мірою зумовлена стратегічною цінністю можливостей штучного інтелекту, які покупці розглядають як фундаментальну перевагу, а не як окремий продукт... Провідні міжнародні гравці діють швидко: компанія Apple домовилася про придбання ізраїльського стартапу Q.ai, що спеціалізується на штучному інтелекті, за 1,5 млрд доларів, щоб посилити свої позиції на ринку носимих пристроїв, а Motorola Solutions придбає компанію D-Fend, що спеціалізується на захисті від дронів, за 1,5 млрд доларів, оскільки автономні бойові дії набувають дедалі більшого значення. У сфері напівпровідників компанія Credo планує придбати розробника оптичних мікросхем DustPhotonics за суму до 1,3 млрд доларів, що свідчить про зростання попиту на інфраструктуру штучного інтелекту... Найактивнішим сектором стала кібербезпека: такі компанії, як Cisco (Astrix), Palo Alto Networks (Koi), CrowdStrike (Seraphic) та SailPoint (Entro Security), купують ізраїльські та пов'язані з Ізраїлем фірми, щоб посилити захист у добу штучного інтелекту, зокрема від загроз, що виходять від нелюдських та «машинних» ідентичностей, а також від автономних агентів ШІ. Тенденція до консолідації виходить за межі іноземних покупців: ізраїльські компанії також купують інші стартапи, щоб прискорити розвиток власних платформ безпеки на базі штучного інтелекту, зокрема придбання компанією Cyera компаній Ryft та Genie Security, а також серія покупок на внутрішньому ринку компанією Check Point, тоді як бельгійський кібер-«єдиноріг» Aikido розширив свою діяльність в Ізраїлі через компанію Root... У сфері корпоративного програмного забезпечення та управління доступом також спостерігається консолідація на основі штучного інтелекту, зокрема придбання

компанією 1Password компанії Arpono, купівля компанією Coupa компанії Tonkean та придбання компанією Amdocs компанії Yess, у міру того як компанії розширюють свої можливості в галузі автономних та агентських технологій. Фінтех-сектор також залишається активним: компанія Nuvei домовилася про придбання Payoneer за 2,75 млрд доларів, Western Union купила GMT, а eToro — Zengo, серед інших угод. Серед угод у сфері охорони здоров'я — заплановане придбання компанією Medtronic компанії CathWorks за 585 млн доларів (сума може зрости до 1 млрд доларів) та придбання компанією Guardant Health компанії MetaSight за суму до 150 млн доларів... У різних секторах особливо привертають увагу темпи та терміни виходу з ринку — деякі стартапи купуються вже через кілька місяців або навіть рік — що свідчить про те, що великі покупці дедалі частіше готові придбати інноваційні компанії, що працюють у сфері штучного інтелекту, на ранніх етапах їхнього розвитку, до того, як вони досягнуть зрілості, а також про те, що можливості штучного інтелекту зараз інтегруються в усі технологічні ланцюги — від оборони та кібербезпеки до напівпровідників, фінансів та аналітики в роздрібній торгівлі». *(Cybersecurity, defense and chips: AI reshapes Israel's exit market // CTech (https://www.calcalistech.com/ctechnews/article/bjuwhu7mfg). 02.07.2026).*

«Новий звіт під назвою «Готові до ризиків чи вразливі до них: розрив у кіберстійкості» показує, що вартість кібератаки сьогодні виходить далеко за межі простою в роботі, впливаючи на курси акцій, наражаючи підприємства на судові позови та змушуючи їх йти на серйозні скорочення бюджету на заходи з відновлення. Відповідно, забезпечення безперебійної діяльності та швидке відновлення стали головними пріоритетами, випередивши простий захист систем. Однак звіт виявляє небезпечний «розрив у впевненості» щодо реальної кіберстійкості... Хоча 98% опитаних організацій в ОАЕ заявляють, що мають стратегію кіберстійкості — і майже половина з них дуже впевнена в її ефективності — у глобальному масштабі лише 6% компаній насправді демонструють найвищий рівень зрілості кіберстійкості. Як не дивно, саме менш зрілі організації виявляють найбільшу самовпевненість, тоді як зрілі організації усвідомлюють свої вразливі місця. Така самовпевненість ставить підприємства під серйозний ризик, оскільки їхні плани відновлення даних після атаки часто мають фундаментальні недоліки... Наприклад, хоча більшість організацій в ОАЕ створюють резервні копії конфіденційних даних і використовують інструменти виявлення загроз, менше половини дотримуються базового правила резервного копіювання «3-2-1» або використовують уніфіковану платформу захисту даних, що означає, що їхні резервні копії можуть виявитися неізолюваними або неперевірено чистими після атаки. Крім того, 79% визнають, що не використовують свої можливості з виявлення загроз на повну потужність, а стратегії резервного копіювання часто не відповідають фактичним ризикам для даних, що означає, що критично важливі системи не є пріоритетними для негайного відновлення... Зрештою, для ОАЕ — економічна стратегія яких значною мірою базується на цифровій довірі та операційній стабільності — справжня кіберстійкість вимагає переходу від

фрагментованих, реактивних заходів ІТ-захисту до проактивного, стратегічного підходу, спрямованого на створення ізольованих, безпечних середовищ відновлення, які забезпечують швидке відновлення безперебійної роботи бізнесу в разі неминучих збоїв». (*Johnny Karam. The cyber resilience divide: Will you bounce back or break down? // Gulf Business (<https://gulfbusiness.com/en/2026/opinion/the-cyber-resilience-divide-will-you-bounce-back-or-break-down/>). 08.07.2026*).

Країни Африки

«Щоб адаптуватися до реалій сучасної війни, яка дедалі більше визначається технологіями, Сили протиповітряної оборони Єгипту впроваджують розроблені в країні системи шифрування та спеціалізовані кіберпідрозділи для забезпечення безпеки військового зв'язку. За словами командувача генерал-лейтенанта Яссера Аль-Туді, кібератаки наразі є центральним компонентом сучасних конфліктів, що спонукає Збройні сили Єгипту створювати спеціальні робочі групи з кібербезпеки у всіх видах збройних сил та інтегрувати національні програми шифрування в свої автоматизовані центри управління та контролю для забезпечення найвищих стандартів інформаційної безпеки... Окрім військової сфери, Єгипет суттєво розширив свої загальні можливості у сфері кіберзахисту з метою захисту критичної інфраструктури та державних органів, започаткувавши комплексну Національну стратегію кібербезпеки на період з 2023 по 2027 рік. Підтверджуючи свою прихильність до глобальної співпраці, Каїр також нещодавно взяв участь у діалогах з питань безпеки на високому рівні з ЄС та визначив кібербезпеку як пріоритетний напрям для майбутнього розбудови потенціалу у партнерстві з НАТО». (*Jodesz Gavilan. Egypt Turns to Domestic Encryption to Secure Air Defense Systems // The Defense Post (<https://thedefensepost.com/2026/07/03/egypt-air-defense-cybersecurity/>). 03.07.2026*).

«Південна Африка вже давно є однією з найбільш вразливих до кібератак країн Африки, і ця вразливість стрімко посилюється, оскільки штучний інтелект прискорює темпи, масштаби та реалізацію кіберзагроз. Двоякість цієї технології особливо яскраво ілюструють такі моделі, як Claude Mythos від Anthropic, яка успішно виявила сотні програмних вразливостей, що тривалий час залишалися непоміченими, продемонструвавши, наскільки легко зловмисники можуть використати передові технології ШІ як зброю для експлуатації слабких місць у системі безпеки. Незважаючи на ці ризики, що постійно зростають, південноафриканські організації залишаються в основному недостатньо підготовленими. Дослідження Accenture показує, що лише 44% місцевих лідерів у сфері технологій визнають, що ШІ розвивається швидше, ніж їхні можливості у сфері кібербезпеки, а базові засоби захисту країни мають серйозні прогалини у критично важливих операційних сферах. Зокрема, лише 18% організацій мають повний огляд своїх хмарних конфігурацій, а лише 6% затвердили базові стандарти

безпеки. Управління даними є настільки ж слабким: лише 18% класифікують свої дані за рівнем конфіденційності, а лише 24% встановлюють політики використання штучного інтелекту...

Крім того, безпека ідентифікації значною мірою ігнорується: лише 28% компаній використовують систему постійної верифікації, а лише 8% застосовують принцип «мінімальних привілеїв». Ця невідповідність також очевидна у сфері розробки програмного забезпечення, де лише 8% організацій інтегрують тестування безпеки на всіх етапах життєвого циклу розробки. Як продемонструвала катастрофічна кібератака 2021 року на державну вантажну компанію Південної Африки, яка паралізувала роботу основних портів і порушила роботу загальнонаціональних ланцюгів постачання, кіберінциденти мають прямі та серйозні наслідки для безперервної діяльності підприємств та економічної стабільності. Щоб орієнтуватися в цьому високоавтоматизованому середовищі загроз, південноафриканські підприємства повинні відмовитися від практики, коли безпека розглядається як щось другорядне, про що згадують лише після впровадження. Натомість вони повинні з самого початку інтегрувати надійні засоби контролю хмарних середовищ, даних та ідентифікації в цифрові ініціативи, а також використовувати захисні інструменти штучного інтелекту для проактивного моніторингу, виявлення та нейтралізації загроз у режимі реального часу, щоб забезпечити довгострокову кіберстійкість». (*Kgomotso Lebele. AI Is raising South Africa's cybersecurity stakes // Creamer Media (<https://www.engineeringnews.co.za/article/ai-is-raising-south-africas-cybersecurity-stakes-2026-07-14>). 14.07.2026*).

«Спортивна галузь Південної Африки стає дедалі привабливішою мішенню для кіберзлочинців, які використовують слабкі місця в системі захисту цього сектору, щоб отримати доступ до великих обсягів цінних персональних даних, зокрема ідентифікаційних номерів, медичних карток та платіжних реквізитів. Згідно з Індексом вразливості до кіберзагроз за 2023/24 роки, опублікованим Радою з наукових та промислових досліджень (CSIR) та Міністерством комунікацій та цифрових технологій, 88% південноафриканських організацій повідомили про щонайменше один випадок порушення безпеки, а майже половина з них зазнала від одного до п'яти інцидентів за рік. За оцінками CSIR, кіберзлочинність щорічно завдає економіці країни збитків у розмірі 2,2 млрд рандів... Ця вразливість посилюється тим, що спортивні організації пройшли процес комерційної та цифрової професіоналізації набагато швидше, ніж встигли забезпечити безпеку своїх систем. Більшість клубів мають недостатньо ресурсів і керуються волонтерами, які часто використовують особисті ноутбуки, спільні паролі та незахищений Wi-Fi, а також підтримують застарілі веб-сайти з нерегулярним резервним копіюванням та нерівномірним дотриманням Закону про захист персональних даних (POPIA). Крім того, спорт базується на емоціях, якими активно користуються соціальні інженери — таких як пристрасть, терміновість та довіра — створюючи обстановку сильного тиску, в якій людська здатність до об'єктивної оцінки ситуації легко погіршується...

Кіберзлочинці використовують поєднання автоматизованих сканувань та цілеспрямованих, витончених атак, щоб зламати ці вразливі системи. Компрометація ділової електронної пошти (BEC) є найбільшим глобальним ризиком для спортивних організацій, про що свідчить задокументований випадок, коли клуб англійської Прем'єр-ліги став жертвою цільового фішингу під час переговорів щодо трансферу на суму 1 мільйон фунтів стерлінгів. У міру зростання обізнаності щодо електронної пошти зловмисники також переходять до мобільних шахрайських схем, таких як клонування профілів у WhatsApp та імітація стилю письма для надсилання термінових запитів на оплату тренерам або волонтерам. Крім того, оператори програм-вимагачів часто застосовують тактику «подвійного шантажу»: вони викрадають конфіденційні дані перед шифруванням баз даних і погрожують оприлюднити особисту інформацію членів або вивести системи реєстрації на заходи з ладу, якщо не буде сплачено викуп. Наслідки для репутації можуть виявитися більш згубними, ніж прямі фінансові втрати, оскільки порушення безпеки серйозно підриває довіру, на якій ґрунтуються громадські клуби, що потенційно може відштовхнути членів, спонсорів та учасників...

Згідно з положеннями POPIA, південноафриканські організації можуть бути оштрафовані на суму до 10 мільйонів рандів за порушення безпеки даних, а витрати лише на повідомлення постраждалих осіб можуть перевищити 1 мільйон рандів навіть для клубу, що налічує лише кілька сотень членів. Щоб убезпечити себе, експерти радять спортивним організаціям централізувати дані про членів на захищених хмарних платформах, запровадити багатофакторну автентифікацію та використовувати безпечні процеси оплати. Волонтери повинні пройти навчання з виявлення фішингу та перевірки банківських реквізитів, а клуби повинні регулярно створювати резервні копії даних та розглянути можливість укладення кіберстрахування для забезпечення професійного реагування на інциденти та юридичної підтримки. Зрештою, спортивні організації повинні сформувати культуру перевірки, в якій зупинка для перевірки незвичайних або термінових запитів розглядається як належне управління, а не як недовіра». (*Chris Tredger. SA sports a prime target for cyber criminals // ITWeb Limited (<https://www.itweb.co.za/article/sa-sports-a-prime-target-for-cyber-criminals/GxwQDq1D3W5MIPVo>). 15.07.2026*).

«Південноафриканські організації зазнали різкого сплеску активності кіберзагроз, стикаючись у червні 2026 року в середньому з 2 065 кібератаками на тиждень. Ця тенденція відповідає попереднім сплескам: у січні 2026 року місцеві організації в середньому зазнавали 2 145 атак на тиждень, що на 17% більше, ніж у січні 2025 року. За даними Statista, глобальні витрати, пов'язані з кіберзлочинністю, у 2025 році сягнули 10,29 трлн доларів, а до 2029 року, за прогнозами, зростуть приблизно до 16 трлн доларів, що зумовлено поширенням програм-вимагачів, фішингу та крадіжки облікових даних. Останній звіт Check Point Research «Global Threat Intelligence» показує, що в червні організації по всьому світу зазнавали в середньому 2 270 атак щотижня. Хоча в Південній Африці було зафіксовано менше щотижневих атак, ніж в Анголі (4 890), Нігерії (4 361) та

Кенії (2 646), вона залишається одним із ринків Африки, що найчастіше стають мішенями, оскільки зловмисники продовжують розширювати сферу своєї діяльності. На всьому африканському континенті середня кількість атак на тиждень становила 3 008, причому найбільш уразливими секторами виявилися державні органи, енергетика, комунальні послуги та фінансові послуги. У глобальному масштабі найбільш вразливим сектором залишається освіта, яка щотижня зазнає в середньому 4 816 атак через надзвичайно відкриті мережі та обмежені ресурси безпеки; за нею слідують державні органи та телекомунікації...

У червні також різко зросла активність програм-вимагачів: у всьому світі було зафіксовано 646 публічно повідомлених випадків зараження, що на 33% більше, ніж у червні 2025 року. Найбільшу частку серед цих жертв склали підприємства сфери бізнес-послуг — 31%, за ними йдуть сектори споживчих товарів і послуг (16%), промислового виробництва (14%) та дедалі більша кількість державних організацій. У сфері програм-вимагачів відбулася значна зміна: групою «The Gentlemen» стала найактивнішою у світі, на її частку припадає 17% оприлюднених атак, і вона випередила групу «Qilin» (11%). Група «LockBit», діяльність якої була серйозно порушена міжнародними правоохоронними органами, також відновила свою активність, збільшивши частку атак до 7% і посівши третє місце за активністю. Стрімке зростання групи «The Gentlemen» демонструє, як швидко нові операції за моделлю «вимагальне програмне забезпечення як послуга» (RaaS) можуть залучати партнерів та експлуатувати зламані мережі...

Окрім традиційних загроз, дослідження Check Point підкреслює зростаючі ризики для безпеки даних, пов'язані з корпоративними інструментами генеративної штучної інтелекту (GenAI). Дослідження показало, що 3,9% запитів, надісланих на платформи GenAI з корпоративних мереж, містили високий ризик розкриття конфіденційних даних, а аж 85% організацій, що використовують GenAI, стикалися з такою високоризиковою активністю запитів. Найвищий рівень витоку даних зафіксовано у секторі охорони здоров'я — 5,7%, за ним йдуть телекомунікації та бізнес-послуги — по 5,1% кожна, а також ІТ-сектор — 4,1%. Особиста інформація була найпоширенішим типом конфіденційних даних, що витікали в цих запитах, поряд з деталями мережевої інфраструктури, юридичними документами, фінансовою інформацією та даними про співробітників. Для боротьби з цими зростаючими багатоплановими загрозами експерти з безпеки наголошують, що організації повинні впроваджувати архітектури безпеки на основі штучного інтелекту, орієнтовані на профілактику, щоб захистити свої мережі, користувачів та робочі процеси з використанням штучного інтелекту до того, як атаки зможуть спричинити операційні наслідки». *(SA records over 2 000 weekly cyber attacks // ITWeb Limited (<https://www.itweb.co.za/article/sa-records-over-2-000-weekly-cyber-attacks/WnpNgM21dgm7VrGd>). 14.07.2026).*

«Незважаючи на значне зниження кількості зареєстрованих випадків шахрайства в Нігерії на 46% — з 124 000 у 2021 році до 68 000 у 2025 році — фінансові збитки, спричинені цими злочинами, різко зросли: з ₦17,67 млрд у 2023 році до ₦25,85 млрд (18,7 млн доларів) у 2025 році. Цей парадокс

пояснюється тим, що кіберзлочинці реалізують дедалі більш витончені та прибуткові схеми, використовуючи на свою користь найбільшу цифрову економіку Західної Африки. За даними Check Point Software, у червні 2026 року нігерійські організації стикалися в середньому з 4 361 спробою кібератак на тиждень, що приблизно вдвічі перевищує середній світовий показник і ставить Нігерію на друге місце серед країн Африканського континенту за кількістю атак. Замість використання агресивних методів хакерських атак зловмисники непомітно отримують доступ до облікових даних користувачів, щоб отримати доступ до платіжних платформ, клієнтських рахунків та здійснити банківські перекази. Ця загроза посилюється високим рівнем залучення осіб зсередини, що сприяє виникненню серйозних вразливостей, таких як шахрайство з підміною SIM-карт, компрометація облікових записів та складні фішингові операції...

Вирішення цих системних вразливостей виявилось складним через поширену практику замовчування інцидентів та обмежений регуляторний нагляд. Хоча Закон Нігерії про захист даних 2023 року зобов'язує організації повідомляти про порушення безпеки даних до Комісії з захисту даних Нігерії (NDPC) протягом 72 годин, багато установ мовчки покривають фінансові збитки, щоб захистити свою комерційну репутацію, залишаючи виявлення серйозних інцидентів незалежним дослідникам та ЗМІ. Ця прогалина у дотриманні вимог особливо помітна серед малих та середніх підприємств з обмеженими ресурсами, які зазнають кібератак удвічі частіше, ніж великі корпорації, через брак фінансування заходів безпеки та навчання персоналу з питань інформаційної безпеки...

Щоб подолати розрив між законодавством та його фактичним виконанням, уряд Нігерії надає пріоритет кільком ключовим реформам цифрової інфраструктури. Національне агентство з розвитку інформаційних технологій (NITDA) у співпраці з Федеральним міністерством комунікацій, інновацій та цифрової економіки завершує розробку комплексної концепції кібербезпеки та суверенітету хмарних технологій. Ця ініціатива, запуск якої очікується пізніше цього року, передбачатиме встановлення мінімальних обсягів інвестицій у кібербезпеку, запровадження суворих термінів повідомлення про порушення та сприяння глибокому обміну інформацією про загрози між державним і приватним секторами. Хоча на даний момент Нігерія посідає третє місце з п'яти у Глобальному індексі кібербезпеки Міжнародного союзу електрозв'язку, експерти наголошують, що для забезпечення зростання цифрової економіки країни необхідно перетворити ці політичні пропозиції на суворі та дієві правові норми». *(Robert Lemos. Nigeria Deepens Cybersecurity Efforts as Cybercriminals See More Profits // TechTarget, Inc. (<https://www.darkreading.com/cyber-risk/nigeria-cybersecurity-efforts-cybercriminals-profits>). 15.07.2026).*

«У червні 2026 року Сомалі запровадила комплексну Національну систему управління ризиками у сфері кібербезпеки, покликану зміцнити кіберстійкість країни та захистити її критичну інформаційну інфраструктуру (КІІ) в умовах триваючої цифрової трансформації. Ця система, розроблена Міністерством комунікацій та технологій (MoCT) за ініціативою міністра

Мохамеда Адама Моаліма, визначає базові вимоги до кібербезпеки, принципи управління та механізми контролю ризиків як спільну відповідальність державних і приватних зацікавлених сторін. Головний регулятор у сфері кібербезпеки Сомалі — Національне управління з питань комунікацій (NCA) на чолі з генеральним директором Мустафою Ясіном Шейхом — використовуватиме цю структуровану систему для покращення регуляторного нагляду, інституційної стійкості та прийняття рішень на основі оцінки ризиків як у державному, так і в приватному секторах...

У рамках цієї системи та відповідно до Закону Сомалі про кібербезпеку всі державні та приватні організації, що експлуатують критично важливі інформаційні інфраструктури (СІІ), повинні виявляти та визначати пріоритетність кіберризиків, що впливають на конфіденційність, цілісність та доступність їхніх активів, проводити регулярні оцінки та подавати щорічні звіти про ризики до Національного центру з кібербезпеки (NCA). Для забезпечення управління кібербезпекою ця концепція базується на міжнародно визнаних стандартах ISO/IEC 27000 та ISO/IEC 27005, використовуючи структурований процес ідентифікації активів, аналізу загроз, оцінки ризиків та заходів щодо їх усунення. Організації повинні класифікувати свої критичні процеси, інформаційні активи, апаратне та програмне забезпечення, мережі та інфраструктуру за сферами безпеки, щоб забезпечити послідовний захист. Крім того, ця система включає галузеві моделі впливу на бізнес для секторів оборони, громадської безпеки, критичної інфраструктури та фінансових послуг, а також рекомендації щодо національної моделі зрілості кібербезпеки, ризиків, пов'язаних із новими технологіями, та управління змінами». (*Joyce Onyeagoro. Somalia Launches National Cybersecurity Risk Management Framework // Tech Africa News (https://techafricanews.com/2026/07/21/somalia-launches-national-cybersecurity-risk-management-framework/). 21.07.2026*).

Кібервійни та протидія зовнішній кібернетичній агресії

«НАТО стикається зі значними викликами у кіберпросторі, оскільки кібератаки як з боку державних, так і злочинних суб'єктів продовжують набирати масштабів і ставати дедалі витонченішими, що змушує альянс посилювати свою кіберзахисну позицію ще з початку 2000-х років. Хоча НАТО відіграє важливу роль у формуванні політики, координації та встановленні стандартів, більшість кіберпотужностей залишаються у віданні окремих держав-членів, що призводить до нерівномірного рівня готовності в межах альянсу. Більші країни мають розвинені кібервійська, тоді як менші або менш розвинені члени можуть не мати достатніх можливостей, що створює одну з головних вразливостей НАТО...

Підхід НАТО зосереджений на захисті власних мереж, наданні підтримки союзникам у зміцненні національної стійкості та забезпеченні механізмів колективного реагування, зокрема можливості розглядати масштабні кібератаки як

підстави для застосування колективної оборони відповідно до статті 5. Альянс також створив такі структури, як групи швидкого реагування на кібератаки, навчальні програми та спеціалізовані центри, а також оновив свою «Декларацію про кіберзахист», включивши до неї більш суворі вимоги щодо повідомлення про інциденти, захисту інфраструктури та співпраці...

Загалом кіберстратегія НАТО ґрунтується на координації, спільних стандартах та інтеграції національних можливостей, а не на централізованому контролі. Хоча альянс досяг прогресу в питаннях управління, підготовки кадрів та співпраці з такими партнерами, як ЄС, постійні загрози та розбіжності між державами-членами означають, що зміцнення кіберпотенціалу залишається незмінним пріоритетом». **(G. Alexander Crowther. How NATO is facing mounting cybersecurity challenges // Atlantic Council (<https://www.atlanticcouncil.org/in-depth-research-reports/report/how-nato-is-facing-mounting-cybersecurity-challenges/>). 01.07.2026).**

«З травня група зломисників, яка, як підозрюється, пов'язана з Китаєм і відстежується компанією Proofpoint під назвою «UNK_MassTraction», здійснює атаки на університети США та Канади, зосереджуючись, зокрема, на дослідниках у галузі фізики, інженерії та національної безпеки. Шпигунська кампанія розпочинається з типових шкідливих електронних листів, які при відкритті у вразливому веб-клієнті Roundcube активують уразливість міжсайтового скриптингу (CVE-2024-42009)... Це запускає JavaScript для завантаження «IceCube» — спеціального шкідливого програмного забезпечення, призначеного для викрадення облікових даних, файлів cookie та даних двофакторної автентифікації. Потім IceCube намагається скористатися другорядною уразливістю десеріалізації (CVE-2025-49113) для встановлення «SquareShell» — веб-шелу на РНР, що дозволяє виконувати код віддалено на поштовому сервері. Якщо це не вдається, шкідливе програмне забезпечення замість цього розгортає «VShell» — стандартний бекдор на мові Go, що працює безпосередньо в пам'яті... Дослідники Proofpoint приписують цю кампанію суб'єкту, пов'язаному з Китаєм, спираючись на спільну інфраструктуру, артефакти китайською мовою та характерну тактику атак на поштові сервери, підключені до Інтернету, хоча вони зазначають, що ця оцінка не є цілком достовірною. Оскільки зломисники, судячи з усього, провели попередню розвідку, щоб цілеспрямовано атакувати системи без встановлених оновлень, адміністраторам настійно рекомендується встановити останні оновлення безпеки Roundcube та забезпечити захист своїх поштових серверів з такою ж ретельністю, як і інших критично важливих вузлів віддаленого доступу». **(Bill Toulas. Hackers exploit Roundcube flaw to spy on academic researchers // Bleeping Computer® LLC (<https://www.bleepingcomputer.com/news/security/hackers-exploit-roundcube-flaw-to-spy-on-academic-researchers/>). 08.07.2026).**

«Оскільки такі супротивники, як Росія, дедалі частіше вдаються до кібервійни та диверсій у «сірій зоні», національна безпека Європи стикається з серйозними викликами, що вимагають оборони за участю «всього

суспільства». Хоча гучні атаки на великі корпорації та критичну інфраструктуру потрапляють на перші шпальти газет, переважна більшість вразливостей припадає саме на малі підприємства та окремих громадян. Малі підприємства, яким часто бракує елементарних засобів кібербезпеки і які не дотримуються чіткого розмежування між особистими та робочими пристроями, часто покладаються на незахищені хмарні сервіси споживчого рівня... Аналогічно, домашні мережі переповнені пристроями «Інтернету речей» (IoT) — такими як смарт-телевізори та камери відеоспостереження — які часто мають серйозні недоліки в безпеці або навіть містять попередньо встановлене шкідливе програмне забезпечення. Крім того, ворожі суб'єкти, що діють за підтримки держав, часто контролюють шкідливі споживчі додатки та розширення для браузерів. Як наслідок, ці скомпрометовані пристрої можуть бути масово використані супротивниками як зброя для здійснення масштабних атак типу «розподілена відмова в обслуговуванні» (DDoS), поширення дезінформації, порушення зв'язку або непрямого нападу на електромережі шляхом створення потужних стрибків напруги...

Хоча Національний центр кібербезпеки Великої Британії (NCSC) надає чудові поради з питань безпеки, він покладає нереалістичне навантаження на пересічних громадян та зайнятих власників малого бізнесу, очікуючи від них проведення власних складних технічних перевірок. Щоб ефективно залучити громадськість до національної оборони, NCSC має перейти від надання абстрактних порад до надання прямих, практичних рекомендацій. Автори пропонують, щоб NCSC створив і активно оновлював національний реєстр затвердженого обладнання, програмного забезпечення та хмарних сервісів, що забезпечують безпеку вже на етапі проектування... Цей реєстр буде вести спеціальна урядова група експертів, яка оцінюватиме комерційні рішення з огляду на юрисдикцію, прозорість власності та політику безпеки, автоматично виключаючи з нього будь-яких постачальників із ворожих країн. Поєднавши цей зручний у користуванні та постійно оновлюваний реєстр із масштабною загальнонаціональною рекламною кампанією з питань громадської безпеки, уряд зможе розібратися в цифровій плутанині та надати громадянам можливість швидко впровадити конкретні засоби кібербезпеки, необхідні для захисту країни від катастрофічних кібератак, що охоплюють усе суспільство». (*Mark Philpott, Ed Hare. National defence requires much better cybersecurity advice for citizens // Resilience Media (<https://resiliencemedia.co/national-defence-requires-much-better-cybersecurity-advice-for-citizens/>). 06.07.2026*).

«Російські хакери здійснили серйозний злом, що загрожує національній безпеці, проникнувши в електронні поштові акаунти урядовців Великої Британії та співробітників Міністерства закордонних справ, які працюють за кордоном. У ході цієї атаки, що отримала назву «FortiBleed», зловмисники скористалися вразливістю у понад 80 000 брандмауерів, наданих компанією з кібербезпеки Fortinet, що дозволило їм викрасти облікові дані. Ця викрадена інформація, що включає адреси електронної пошти та паролі співробітників британських посольств і місцевих органів влади, зараз продається в даркнеті за

ціною до 60 000 доларів, що створює значний ризик подальшого проникнення в конфіденційні системи урядового комплексу Вайтхолл... В результаті злом також були викрадені облікові дані операторів критичної інфраструктури, зокрема організацій Національної служби охорони здоров'я (NHS) та енергопостачальників, що змусило експертів попередити про можливий «катастрофічний» інцидент, який може загрожувати безпеці пацієнтів. Національний центр кібербезпеки Великої Британії (NCSC) опублікував термінове попередження, в якому підтвердив факт атаки методом «грубої сили» та наказав постраждалим організаціям провести перевірку своїх мереж і негайно змінити паролі. Хоча прямих доказів причетності російської держави немає, цей інцидент підтверджує зростаючі побоювання щодо того, що Кремль підтримує та керує хакерськими угрупованнями-посередниками, які націлені на британські інтереси...» (*Richard Holmes. Russian hackers steal government logins // Telegraph Media Group Holdings Limited (<https://www.telegraph.co.uk/news/2026/07/05/russian-hackers-steal-government-logins/>). 07.07.2026*).

«Глобальна компанія з кібербезпеки Forescout Technologies оголосила, що вона виконала суворі вимоги НАТО щодо забезпечення інформаційної безпеки та була включена до Каталогу продуктів забезпечення інформаційної безпеки НАТО (NIAPC). Цей централізований ресурс, який веде Агентство зв'язку та інформації НАТО (NCIA), допомагає НАТО та організаціям-союзникам визначати надійні рішення з кібербезпеки, що відповідають суворим оперативним стандартам. Включення до NIAPC підтверджує, що платформа Forescout сертифікована для розгортання в середовищах, критично важливих для виконання місій, та забезпечує захист секретних мереж і оперативну готовність. У міру зростання кіберзагроз у 32 країнах-членах НАТО, що впливають на ІТ, операційні технології (ОТ) та системи виконання місій, організації потребують рішень, які забезпечують комплексний огляд, швидке розгортання та автоматизоване реагування... Forescout задовольняє ці потреби за допомогою платформи, яка безперервно виявляє та класифікує підключені пристрої, забезпечує дотримання принципу «Універсального доступу до мережі за принципом нульової довіри» (UZTNA) та використовує динамічну сегментацію для локалізації загроз у режимі реального часу й запобігання побічному переміщенню. Її можливості були перевірені в реальних оборонних сценаріях, зокрема під час навчань НАТО «Locked Shields» — найбільших у світі навчань з кіберзахисту з використанням реальних атак, — де захисники покладаються на видимість у режимі реального часу та скоординовані заходи реагування. Генеральний директор Forescout Баррі Майнц назвав включення компанії до NIAPC важливою віхою, яка підкріплює її здатність підтримувати вимогливі оборонні середовища по всьому світу. Платформа забезпечує єдиний огляд у режимі реального часу всіх пристроїв у ІТ- та ОТ-середовищах, що дозволяє швидше приймати рішення, автоматично реагувати на аномалії та забезпечувати безпеку операцій... Вона забезпечує безперервне виявлення та класифікацію ІТ-, ОТ-, IoT-ресурсів та ресурсів, пов'язаних із виконанням місій, підтримує автоматизоване локалізування загроз без необхідності використання

програмних агентів або перепроєктування мережі, а також дозволяє здійснювати розгортання у великих масштабах. Розроблена як для оперативного, так і для тактичного використання, платформа забезпечує безпечне управління складними розподіленими середовищами, включаючи несекретні, обмежені та секретні мережі, поширюючи захист у сфері кібербезпеки на системи, пов'язані з виконанням місій, розгорнуті команди та критичну інфраструктуру». ***(Forescout added to NATO cybersecurity catalogue for defense and critical infrastructure deployments // Industrial Cyber (<https://industrialcyber.co/news/forescout-added-to-nato-cybersecurity-catalogue-for-defense-and-critical-infrastructure-deployments/>). 08.07.2026).***

«Очікується, що світовий ринок кібервійни демонструватиме стійке зростання протягом наступного десятиліття, оскільки уряди країн посилюють національну кіберстійкість, модернізують оборонні можливості та збільшують інвестиції в інфраструктуру цифрової безпеки. Оцінюваний у 39,12 млрд доларів США у 2025 році, ринок, за прогнозами, досягне 66,84 млрд доларів США до 2035 року, при цьому середньорічний темп зростання (CAGR) у період з 2026 по 2035 рік становитиме 5,54%. Швидкі досягнення у сфері кібербезпеки вивели кіберпростір у ранг критично важливого компонента національної безпеки, нарівні з сушею, водою, повітрям та космосом. Зростання кількості випадків кібершпигунства, атак із використанням програм-вимагачів та атак на урядові структури й об'єкти критичної інфраструктури стимулювало попит на передові технології кібербезпеки. Оскільки організації дедалі більше покладаються на хмарні обчислення, підключені пристрої та штучний інтелект, кібербезпека стала стратегічною необхідністю, а співпраця між державним і приватним секторами та посилення регуляторних вимог ще більше сприяють зростанню ринку...

Державні видатки на програми кібербезпеки продовжують зростати, що спонукає збройні сили по всьому світу розвивати все більш потужні наступальні та оборонні кіберможливості. Впровадження архітектури «нульової довіри» підвищує стійкість організацій до атак, забезпечуючи швидше виявлення вразливостей та реагування на них. Міжнародна співпраця, інвестиції в персонал та захист інфраструктури також створюють нові можливості для постачальників рішень у сфері кібербезпеки. Що стосується сегментів ринку, то у 2025 році на програмне забезпечення припадало 41,37% доходу, що зумовлено попитом на системи виявлення загроз на основі штучного інтелекту, платформи кіберрозвідки та рішення для автоматизованого реагування на інциденти. Очікується, що програмне забезпечення залишатиметься найдинамічнішим сегментом ринку аж до 2035 року.

У 2025 році на ринку домінувала оборонна кібервійна, на яку припадало 81,63% доходу, що відображає інвестиції в захист урядових та військових систем. Однак прогнозується, що наступальна кібервійна зростатиме із середньорічним темпом зростання (CAGR) 6,82%, оскільки країни розширюють свої стратегічні кіберможливості. На частку урядових та оборонних організацій припадало 36,72% ринкового доходу, що зумовлено триваючою військовою модернізацією та національними ініціативами з кібербезпеки. Очікується, що найдинамічнішим

сегментом застосування стане захист критичної інфраструктури, зосереджений на забезпеченні безпеки систем енергетики, транспорту, телекомунікацій та водопостачання. Оборонні та військові організації очолили сегмент кінцевих користувачів із часткою 34,62% доходу, тоді як найшвидше зростання очікується у секторах банківських, фінансових та страхових послуг (BFSI) та корпоративному секторі, оскільки кібербезпека стає пріоритетом на рівні правління компаній...» **(Cyber Warfare Market Size To Exceed \$66.84 Billion By 2035 | SNS Insider // S&S Insider Pvt Ltd (<https://www.snsinsider.com/press-release/global-cyber-warfare-market>). 02.07.2026).**

«ФБР спільно з міжнародними партнерами у сфері безпеки попередило, що Федеральна служба безпеки Росії (ФСБ), а саме її кіберпідрозділ, відомий як «Центр 16», активно використовує неправильно налаштовані та вразливі маршрутизатори для атак на мережі в західних країнах. Згідно з повідомленням, «Центр 16» — також відомий під кількома назвами груп зловмисників, зокрема Berserk Bear, Energetic Bear та Ghost Blizzard — підтримує операції російської зовнішньої розвідки та має тривалий досвід атак на сектори критичної інфраструктури, такі як енергетика, охорона здоров'я, фінанси, освіта та державні органи...

Ця група, насамперед, сканує Інтернет у пошуках маршрутизаторів зі слабкими налаштуваннями або налаштуваннями за замовчуванням протоколу SNMP (Simple Network Management Protocol), використовуючи ці базові слабкі місця в системі безпеки для отримання початкового доступу. Експерти з безпеки зазначають, що ці атаки й надалі є успішними, оскільки багато організацій, особливо тих, що використовують застарілі системи операційних технологій, не дотримуються основних практик мережевої безпеки. ФБР рекомендує посилити налаштування маршрутизаторів шляхом впровадження протоколу SNMPv3 із надійною автентифікацією та шифруванням, безпечного зберігання паролів та поліпшення загальної гігієни мережевих налаштувань...

У цьому попередженні наголошується, що зловмисники використовують недооцінені та усунві вразливості, а не складні експлойти, що підкреслює важливість ставлення до мережевої інфраструктури як до критичного пріоритету в галузі безпеки, а не як до компонента, про який можна «встановити й забути». **(Davey Winder. FBI Issues Warning As Russia's FSB Center 16 Hackers Target Routers // Forbes Media LLC (<https://www.forbes.com/sites/daveywinder/2026/07/14/fbi-issues-warning-as-russias-fsb-center-16-hackers-target-routers/>). 14.07.2026).**

«Згідно з даними, оприлюдненими Міністерством оборони та наведеними депутатом Ю Йон-веоном, у 2025 році кількість спроб кібератак на збройні сили Південної Кореї зроста майже до 19 000, що є найвищим показником за останні п'ять років і свідчить про значне збільшення порівняно з попередніми роками. Переважна більшість із цих 18 951 інцидентів полягала у спробах зламати

військові веб-сайти шляхом захоплення прав адміністратора... Хоча Командування кібероперацій визнало, що ідентифікувати зловмисників складно через приховані сліди, південнокорейські власті мають серйозні підозри щодо причетності північнокорейської розвідувальної служби — Головного управління розвідки та збору інформації. Ця оцінка узгоджується зі спостереженнями щодо зростання кіберпотенціалу Північної Кореї та нещодавнім повідомленням державних ЗМІ, в якому підтверджується, що лідер Кім Чен Ин закликав розширити функції та завдання цієї служби». (*Yonhap. Military targeted in nearly 19,000 cyberattack attempts in 2025: lawmaker // The Korea Times* (<https://www.koreatimes.co.kr/southkorea/defense/20260712/military-targeted-in-nearly-19000-cyberattack-attempts-in-2025-lawmaker>). 12.07.2026).

«Згідно з доповіддю компанії Recorded Future, зловмисники, пов'язані з Іраном, активно використовують генеративний штучний інтелект та великі мовні моделі (LLM) для посилення своїх операцій у сфері кібер- та інформаційної війни, що підвищує ризик асиметричних атак проти Сполучених Штатів та їхніх союзників. Хоча немає ознак того, що Іран розробив повністю автономні моделі штучного інтелекту, ця технологія скоротила відстань між наміром і дією, прискоривши реалізацію існуючих можливостей країни. Злочинні угруповання використовують великі мовні моделі для картографування промислових систем управління, дослідження вразливостей програмного забезпечення, створення шкідливого програмного забезпечення та ведення фішингових діалогів мовами, якими оператори-люди не володіють вільно...

Цю зростаючу тенденцію ілюструють кілька задокументованих кампаній. У січневій кампанії, відомій як «Operation Olalampro», група зловмисників MuddyWater використала штучний інтелект для розробки чотирьох варіантів шкідливого програмного забезпечення, вбудованого в шкідливі документи Office, спрямованих проти країн Близького Сходу та Північної Африки. У квітні інша група, пов'язана з Іраном, — «Ababil of Minab», яка також взяла на себе відповідальність за атаку на систему громадського транспорту Лос-Анджелеса, — використала ChatGPT для вдосконалення скриптів, призначених для переліку та розміщення баз даних під час атаки на Vynco, американську компанію, що займається відстеженням транспортних засобів за допомогою GPS. Крім того, раніше OpenAI заблокувала акаунти, пов'язані з іранськими суб'єктами, пов'язаними з державою, зокрема Charming Kitten та CyberAv3ngers, після того, як виявила, що CyberAv3ngers використовувала ChatGPT для розвідки програмованих контролерів PLC...

Хоча розвиток штучного інтелекту в Ірані стримується руйнуванням інфраструктури, країна тісно співпрацює з Росією та Китаєм з метою розширення своїх технологічних можливостей. Аналітики з питань безпеки припускають, що Іран може звернутися до Китаю за додатковою допомогою, щоб використовувати його передові моделі штучного інтелекту. Крім того, очікується, що іранські кібероператори наслідуватимуть приклад китайських суб'єктів, впроваджуючи розроблені в Китаї моделі у провідні програмні комплекси, такі як Claude Code, з

метою подальшої оптимізації своїх наступальних кіберможливостей». (*David Jones. Iran-nexus actors using AI to enhance cyber playbook // TechTarget, Inc. (<https://www.cybersecuritydive.com/news/iran-nexus-actors-ai-cyber-ChatGPT-malware/825415/>). 16.07.2026*).

Кіберзахист критичної інфраструктури

«На тлі дедалі тіснішої інтеграції операційних технологій (ОТ) з корпоративними ІТ-системами кіберзагрози у глобальних ланцюгах створення вартості в енергетиці та нафтохімічній галузі стрімко зростають. Останні дані розвідки свідчать про приголомшливий 935-відсотковий сплеск атак з використанням програм-вимагачів на нафтогазову галузь за останній рік, а також про зростання кількості спеціалізованих угруповань зловмисників, які активно складають карти промислових контурів управління. Ці зловмисники — від хакерів, що діють за підтримки держави, до недосвідчених зловмисників, які використовують методи грубої сили, — успішно експлуатують недотримання правил кібергігієни, стандартні облікові дані та неправильно налаштовані периферійні пристрої, підключені до Інтернету. Яскравим прикладом цього стала скоординована атака з використанням шкідливого програмного забезпечення типу «wiper», яка вразила понад 30 об'єктів відновлюваної енергетики в Польщі, серйозно порушивши роботу їхніх інтерфейсів «людина-машина» та віддалених термінальних пристроїв...

Щоб мінімізувати ці серйозні економічні, екологічні та безпекові ризики, оператори повинні перейти від реактивного реагування на інциденти до проактивного, комплексного забезпечення кіберстійкості. Справжня операційна обережність вимагає від операторів досягнення повної видимості мережі та проведення всебічного аналізу небезпек процесів для встановлення базового рівня їхнього стану ризику. Покладатися виключно на периметрові засоби захисту недостатньо; натомість організації повинні впровадити інтегровану стратегію глибокого захисту, розроблену за зразком таких рамок, як Рамка кібербезпеки NIST та ISA/IEC 62443. Цей багаторівневий підхід вимагає суворої сегментації мережі, зміцнення каналів віддаленого доступу, надійного виявлення аномалій та критично важливого захисту систем інструментальної безпеки (SIS). Формування такого рівня стійкості — це багаторічна робота, яка вимагає незалежних оцінок ризиків, що проводяться сторонніми організаціями, постійних інвестицій та активної співпраці з галузевими органами для обміну інформацією про загрози та проактивного захисту критичної енергетичної інфраструктури світу». (*Ellie Brosnan. Defence-in-depth cybersecurity // Palladian Publications Ltd. (<https://www.hydrocarbonengineering.com/special-reports/06072026/defence-in-depth-cybersecurity/>). 06.07.2026*).

«У той час як уряди та приватні компанії вкладають мільярди в супутники, орбітальні системи зв'язку, системи спостереження за Землею і навіть проекти створення космічних центрів обробки даних, експерти з кібербезпеки попереджають, що на орбіті з'являється нова поверхня атаки. Оскільки орбітальні системи не можна легко оновити, фізично перевірити чи відремонтувати технічним персоналом на Землі, захист інфраструктури, що функціонує на висоті сотень кілометрів над Землею, вимагає іншого підходу до безпеки — такого, що зосереджений на профілактиці та автономності, а не на швидкому реагуванні на інциденти... Нещодавнє випробування, проведене компанією OPSWAT, ілюструє, як галузь починає вирішувати цю проблему: компанія за допомогою метеорологічного аеростата підняла свій пристрій MetaDefender Kiosk Mini в умови, близькі до космічних, де він продовжував сканувати та очищати файли, працюючи повністю в автономному режимі, незважаючи на мінусові температури, низький атмосферний тиск, високий рівень ультрафіолетового випромінювання та вільне падіння. Це випробування не лише демонструє технічну стійкість, а й підкреслює більш загальну тезу про те, що космічна інфраструктура дедалі частіше розглядається як частина екосистеми критичної інфраструктури світу... Космічні об'єкти забезпечують функціонування таких повсякденних процесів, як визначення місцезнаходження, прогнозування погоди, телекомунікації, фінансові системи, військові операції та підключення до Інтернету, тому їхня вразливість — від радіоелектронного придушення та підробки сигналів до атак на наземні станції та кібератак, спрямованих на порушення зв'язку — стає дедалі більшою проблемою. Геополітична напруга посилила ці побоювання, оскільки уряди багатьох країн розглядають космос як стратегічну сферу нарівні з сушею, морем, повітрям та кіберпростором, що ще більше стимулює зусилля щодо захисту орбітальних об'єктів як від загроз з боку держав, так і від злочинних угруповань... Генеральний директор OPSWAT стверджує, що традиційні припущення щодо кібербезпеки — такі як уявлення про те, що на Землі завжди знайдеться хтось, хто зможе вирішити проблеми, — не діють у космосі, що відповідає принципам «нульової довіри» та «передусім профілактики». Використовуючи технологію «Content Disarm and Reconstruction» (CDR), система MetaDefender розглядає вхідні файли як потенційно шкідливі, видаляючи з них ризикований вміст і відтворюючи чисті версії ще до того, як вони потраплять у захищені середовища. Ця стратегія є особливо актуальною для високоізольованих середовищ, таких як військові системи або космічні апарати... З огляду на майбутнє, перспектива створення орбітальних центрів обробки даних додає актуальності, оскільки майбутнім космічним обчислювальним системам може бракувати доступу до безперервного моніторингу та хмарних даних про загрози, що робить автономне прийняття рішень щодо безпеки надзвичайно важливим. Загрози, окрім шкідливого програмного забезпечення, також включають підробку сигналів GPS, перехоплення команд, перехоплення комунікацій, витік даних, компрометацію ланцюга поставок та більш широкі сценарії електронної війни. Тим часом очікується, що генеративна штучна інтелектуальна система зробить наступальні можливості — такі як швидше виявлення вразливостей та більш переконливий фішинг — більш масштабованими, що підкріплює аргументи на

користь архітектур, які мінімізують вразливість, а не покладаються переважно на виявлення. Вважається, що Канада має особливий інтерес у цьому питанні завдяки своїй багаторічній історії розвитку космічних технологій та постійним інвестиціям у супутниковий зв'язок та широкосмугові мережі на низькій навколоземній орбіті... У міру розвитку космічного сектору Канади канадські органи влади та науковці все більше приділяють увагу кіберстійкості, особливо з огляду на те, що штучний інтелект, кібербезпека та космічні операції стають дедалі тісніше пов'язаними між собою, а супутникові групи розширюються у сферу, де протидіяти складним і тривалим кібератакам з землі може ставати дедалі складніше». (*Tim Sandle. Cybersecurity in space: Protecting the next frontier of critical infrastructure // Digital Journal Inc. (<https://www.digitaljournal.com/article/cybersecurity-in-space-protecting-the-next-frontier-of-critical-infrastructure/>). 03.07.2026*).

«Німецький технологічний концерн Siemens та манчестерська компанія з кібербезпеки NCC Group підписали Меморандум про взаєморозуміння щодо співпраці у сфері захисту критичної національної інфраструктури та промислових секторів Великої Британії від кіберзагроз, що стрімко розвиваються. Партнерство спрямовано на забезпечення безпеки операційних технологій (OT) у промисловості, енергетиці та оборонному секторі, зокрема на усунення вразливостей, що виникають внаслідок інтеграції IT-систем обробки даних із реальними фізичними операціями... Поєднуючи великий досвід компанії Siemens у галузі промислової автоматизації та систем управління з глибокими компетенціями NCC Group у сфері кібербезпеки, обидві компанії прагнуть надати власникам та операторам активів комплексний підхід до забезпечення кіберстійкості, що дозволить їм безпечно прискорити процес модернізації та автоматизації. Ця стратегічна співпраця, яка відображає масштаб та актуальність сучасних загроз, була офіційно обговорена як ключовий тренд на конференції «Transform 2026» — дводенному заході в Манчестері, організованому компанією Siemens». (*Neil Hodgson. NCC Group and Siemens work to improve industry, energy and defence cyber security // Regional Media Services Ltd. (<https://www.thebusinessdesk.com/northwest/news/2175899-ncc-group-and-siemens-work-to-improve-industry-energy-and-defence-cyber-security>). 15.07.2026*).

«Білий дім запустив «Gold Eagle» — новий інформаційний центр на базі штучного інтелекту, призначений для оперативного збору, класифікації та координації заходів з усунення вразливостей програмного забезпечення в критичній інфраструктурі США. Ця ініціатива, спрямована на протидію загрозі з боку шкідливого програмного забезпечення, створеного штучним інтелектом зі швидкістю роботи комп'ютера, об'єднує Міністерство фінансів, Міністерство внутрішньої безпеки через CISA та нещодавно перейменоване Міністерство війни, а також неназвані групи з відкритим кодом та компанії, що забезпечують функціонування критичної інфраструктури (серед яких, ймовірно, є й Anthropic)... Ініціатива «Gold Eagle», яку міністр оборони Піт Хегсет охарактеризував як таку,

що забезпечує «військовий режим» у сфері кіберзахисту, впливає з указу від 2 червня, який зобов'язав провідних розробників штучного інтелекту надати уряду ранній доступ до своїх систем, фактично використовуючи ті самі моделі штучного інтелекту, що прискорюють кібератаки, для проактивного захисту від них. Однак в оголошенні про цю ініціативу відсутні важливі деталі: не вказано, яке відомство керуватиме повсякденною діяльністю, як забезпечуватиметься захист конфіденційних даних про вразливості та які приватні компанії беруть участь у програмі... Крім того, Gold Eagle виходить на ринок, де вже існує чимало федеральних програм з розкриття інформації, таких як система CVE та Національна база даних вразливостей NIST. Що особливо важливо, програма, судячи з усього, є лише координаційним механізмом, який не має повноважень змушувати компанії фактично усувати виявлені нею вразливості, через що експерти ставлять під сумнів, чи зможе цей амбітний інформаційний центр справді випередити швидко розвиваються кіберзагрози на основі штучного інтелекту, для боротьби з якими він і був створений». (*Ana-Maria Stanciu. The White House's Gold Eagle wants to patch cyber flaws at machine speed // Cogneve, INC. (<https://thenextweb.com/news/gold-eagle-white-house-ai-cyber-clearinghouse>). 15.07.2026*).

Кіберзахист промислових об'єктів та об'єктів будівництва

П'ятий рік поспіль виробнича галузь залишається найбільш вразливою до атак у світі, на її частку припадає 27,7% інцидентів, за даними Індексом загроз IBM X-Force за 2026 рік. Останні дані про загрози підтверджують різке зростання кількості окремих фішингових атак, спрямованих проти виробників, що зумовлено не однією кампанією, а розширенням спектру загроз. Зловмисники активно націлюються на цей сектор через великий обсяг постійного руху рахунків-фактур, розгалужені та постійно мінливі мережі постачальників, а також через безперервний тиск виробничих процесів, що вимагають швидких рішень — все це підвищує ймовірність успіху шкідливого електронного листа...

Наразі трьома найбільш руйнівними типами атак є викрадення облікових даних, видавання себе за постачальника та шахрайство з рахунками-фактурами. Приманки для викрадення облікових даних часто імітують важливе програмне забезпечення, таке як платформи електронного підпису та ERP-системи, використовуючи цілком точні цільові сторінки та ланцюжки перенаправлень через легітимну інфраструктуру для викрадення даних для входу, що становить 41% випадків порушень безпеки у виробничій галузі. Злом електронної пошти постачальників (VEC) та видавання себе за постачальника експлуатують довіру в рамках розгалужених мереж постачальників; зловмисники використовують зламані або підроблені облікові записи постачальників для видачі шахрайських інструкцій щодо зміни банківських реквізитів або підроблених рахунків-фактур, що є надзвичайно ефективним, оскільки такі повідомлення часто проходять стандартні протоколи автентифікації, такі як SPF, DKIM та DMARC...

Поширеною та надзвичайно ефективною технікою доставки в таких атаках є зловживання функцією «Direct Send» у Microsoft 365. Ця функція спочатку була розроблена для того, щоб пристрої, такі як принтери, могли надсилати внутрішні електронні листи без авторизації, проте зловмисники використовують «Direct Send» для доставки підроблених листів без шкідливого вмісту, які начебто надходять із власного домену компанії, безперешкодно обходячи традиційні шлюзи та сканери вмісту.

Щоб захиститися від цих витончених атак, виробники повинні впровадити три ключові заходи: вимкнути або обмежити доступ до вразливої функції Direct Send за допомогою нового параметра Microsoft «RejectDirectSend»; забезпечити дотримання суворих політик DMARC на своїх доменах та спонукати ключових постачальників робити те саме; а також модернізувати системи виявлення, щоб використовувати адаптивний штучний інтелект, здатний виявляти аномалії в поведінці автентифікованих електронних листів без корисного навантаження». *(Audian Paxson. Why Attackers Target Manufacturers, and What the Attacks Look Like // Techstrong Group Inc. (<https://securityboulevard.com/2026/07/why-attackers-target-manufacturers-and-what-the-attacks-look-like/>). 03.07.2026).*

Кіберзахист закладів охорони здоров'я

«Між кібербезпекою медичних пристроїв та дотриманням нормативних вимог FDA (Управління з контролю за продуктами харчування та ліками США) існує фундаментальна суперечність. Хоча FDA, що цілком зрозуміло, вимагає від виробників постійно контролювати, виправляти та оновлювати підключені пристрої для забезпечення безпеки, саме ці оновлення можуть зумовити необхідність подання нової заявки 510(k) перед виведенням на ринок, якщо вони суттєво змінюють програмне забезпечення, архітектуру або клінічний робочий процес пристрою. Неоднозначність виникає через те, що, хоча вузькоспрямовані виправлення відомих вразливостей можуть не вимагати подання нової заявки, більш надійні заходи безпеки — такі як додавання багатофакторної автентифікації або шифрування даних — можуть вплинути на продуктивність або сумісність пристрою, що потенційно може позначитися на безпеці пацієнтів та ефективності лікування... Ця нормативно-правова неоднозначність створює хибний стимул для виробників застосовувати вузькі, недостатні обхідні рішення або взагалі уникати подання заявки 510(k) через побоювання привернути увагу FDA або затримати впровадження критично важливих виправлень з безпеки. Хоча FDA намагалася роз'яснити, що не всі зміни в програмному забезпеченні вимагають подання нових заяв і що нещодавні законодавчі вимоги згідно з розділом 524В Закону про харчові продукти, ліки та косметичні засоби (FD&C Act) не мають зворотної сили, виробники все ще не мають чітких рекомендацій... Щоб вирішити цю проблему, FDA має навести практичні приклади на основі конкретних сценаріїв, коли оновлення з кібербезпеки перевищують поріг 510(k), а також заохочувати використання заздалегідь розроблених планів контролю змін.

Кінцевою метою політики має бути забезпечення того, щоб регуляторна невизначеність не перешкоджала та не затримувала впровадження необхідних виправлень з кібербезпеки, тоді як компанії, у свою чергу, повинні інтегрувати регуляторні вимоги у свої процедури оновлення програмного забезпечення, щоб безпечно орієнтуватися в цьому складному середовищі». ***(Cybersecurity Updates and 510(k) Anxiety: How Good Updates Create Regulatory Risk // Blank Rome LLP (<https://www.blankrome.com/news-and-events/cybersecurity-updates-and-510k-anxiety-how-good-updates-create-regulatory-risk/>). 01.07.2026).***

«3 січня 2023 року в медичних радах NHS Scotland було зафіксовано понад 5 000 випадків витоку даних, що призвело до застосування дисциплінарних заходів щонайменше до 182 співробітників, шести звільнень та шести звернень до поліції Шотландії, як свідчить розслідування, проведене виданням The Ferret на підставі Закону про свободу інформації (FOI). Зареєстровані інциденти — від помилкового надсилання електронних листів до несанкціонованого доступу до надзвичайно конфіденційних медичних записів пацієнтів — свідчать про значні вразливості в системі управління інформацією у 14 територіальних радах охорони здоров'я країни, причому найбільшу кількість порушень зафіксовано в NHS Greater Glasgow and Clyde та NHS Lanarkshire. Справжня кількість, ймовірно, є вищою через неповноту даних та обмеження щодо витрат на оприлюднення інформації відповідно до Закону про свободу інформації...»

Хоча уряд Шотландії та Управління комісара з питань інформації (ICO) наголошують на надзвичайній важливості конфіденційності даних пацієнтів і вимагають надійних технічних заходів контролю та підзвітності, експерти критикують реакцію Національної служби охорони здоров'я (NHS) як недостатню. Експерт з кібербезпеки Саїф Абед зазначив, що необхідність звертатися із запитами на отримання інформації (FOI) для з'ясування цих цифр свідчить про відсутність прозорості та «загальну недбалість на керівних рівнях» щодо конфіденційності даних та кібербезпеки, стверджуючи, що ані ради з питань охорони здоров'я, ані ICO не вживають суттєвих покаральних заходів для запобігання такій поведінці. Ці постійні внутрішні порушення ще більше ускладнюються значними зовнішніми кіберзагрозами, такими як кібератака 2024 року на NHS Думфріс і Галлоуей, в результаті якої було викрадено величезні обсяги даних про пацієнтів та персонал». ***(Jordan Sollof. More than 5,000 NHS Scotland data breaches since 2023 // Digital Health (<https://www.digitalhealth.net/2026/07/more-than-5000-nhs-scotland-data-breaches-since-2023/>). 13.07.2026).***

«Австралійська медична організація «Partnered Health» зазнала масштабної кібератаки, яка зачепила 21 її амбулаторію в штатах Новий Південний Уельс, Вікторія, Квінсленд, Західна Австралія та в Австралійській столичній території. В результаті інциденту, виявленого 23 червня, було викрадено надзвичайно конфіденційну особисту та медичну інформацію, зокрема записи про консультації, результати діагностики, дані про програму Medicare,

імена, адреси та інформацію про приватне медичне страхування... Компанія Partnered Health повідомила про цей інцидент у поліцію, до Австралійського центру кібербезпеки та до Управління комісара з питань інформації Австралії, продовжуючи при цьому розслідувати повний масштаб викрадення даних та підтримуючи зв'язок із пацієнтами, яких це торкнулося. Компанія щиро вибачилася за цей інцидент, порадила пацієнтам зберігати пильність щодо переконливих цілеспрямованих шахрайських схем та успішно домоглася від Верховного суду Нового Південного Уельсу винесення тимчасового судового заборони, щоб запобігти використанню або оприлюдненню викрадених даних». (*Zoe Phillips. Australian healthcare provider hit by major cyberattack with medical records compromised across 21 clinics // Australian News Channel Pty (<https://www.skynews.com.au/business/tech-and-innovation/australian-healthcare-provider-hit-by-major-cyberattack-with-medical-records-compromised-across-21-clinics/news-story/d27e1a5a68f9533c540d6bbfb6e7bdd8>). 15.07.2026*).

«Компанія Craneware, що котирується на біржі AIM і спеціалізується на рішеннях для управління фінансовими показниками у сфері охорони здоров'я, реагує на інцидент у сфері кібербезпеки, пов'язаний із несанкціонованим доступом до частини її інформаційного середовища. Після запуску плану реагування на інциденти компанія залучила зовнішніх фахівців з кібербезпеки та цифрової криміналістики для проведення розслідування спільно зі своєю внутрішньою ІТ-командою та залученими постачальниками послуг з безпеки. Наразі інцидент успішно локалізовано без жодних перебоїв у роботі Craneware чи наданні послуг клієнтам, а слідчі не виявили у системах жодних залишкових ознак компрометації... Компанія Craneware повідомила про інцидент відповідні органи, зокрема Управління комісара з питань інформації Великої Британії та Федеральне бюро розслідувань США. Хоча в ході розслідування, яке триває, було встановлено, що значна кількість імен файлів була переглянута та викрадена, поточна оцінка свідчить про те, що, хоча більша частина скомпрометованих даних не є конфіденційною або є публічною нормативною інформацією, зловмисники також отримали доступ до певної частки даних про співробітників та частини записів про клієнтів і партнерів». (*Craneware plc hit by cyber security breach // BusinessCloud (<https://businesscloud.co.uk/news/craneware-plc-hit-by-cyber-security-breach/>). 20.07.2026*).

Масштабні витоки персональних даних

«Управління земельних ресурсів Сінгапуру (SLA) повідомило, що в результаті інциденту з кібербезпекою, пов'язаного з хмарним середовищем, яке перебуває під управлінням IBM, стався витік персональних даних приблизно 70 000 осіб. Порухення сталося внаслідок несанкціонованого доступу до набору даних, який використовувався виключно для розробки та тестування постачальниками Сінгапурської системи автоматизованої реєстрації прав власності (STARS) та системи eLodgment. Хоча цей набір даних, який використовується з 1998 року, мав містити лише фіктивні та анонімізовані записи, до нього помилково потрапили справжні імена, номери національних реєстраційних посвідчень та адреси... SLA наголосила, що це тестове середовище повністю ізольоване від її діючих операційних систем, що гарантує безпеку та цілісність записів про право власності на нерухомість та їх реєстрацію. Наразі органи влади повідомляють про інцидент постраждалих осіб та розпочали спільне розслідування разом з IBM, Агентством з кібербезпеки Сінгапуру та Урядовим агентством з технологій, щоб з'ясувати, чому дані не були знеособлені. Також подано заяву до поліції та повідомлено Комісію з захисту персональних даних». *(Personal data of 70,000 people in Singapore breached in IBM-managed cloud environment // Anadolu Ajansı (<https://www.aa.com.tr/en/science-technology/personal-data-of-70-000-people-in-singapore-breached-in-ibm-managed-cloud-environment/3985540>). 03.07.2026).*

«Нещодавно Університет Ноттінгема зазнав серйозної кібератаки з боку злочинного угруповання, в результаті якої було скомпрометовано приблизно 455 000 записів про студентів, що містять конфіденційну інформацію, таку як номери соціального страхування, поштові адреси та фінансові дані. У відповідь університет розпочав кримінальне розслідування та активно співпрацює з правоохоронними органами, адміністраторами сторонніх платформ та регуляторними органами, такими як Управління комісара з питань інформації, а також надав спеціальну гарячу лінію для підтримки постраждалих осіб. Однак Ноттінгем — це лише останній у дедалі довшому списку університетів «Russell Group», які в останні роки стали мішенями кіберзлочинців...

Прямі витоки даних торкнулися й низки інших престижних навчальних закладів. У 2026 році хакери зламали сайт CareerConnect Оксфордського університету, оприлюднивши контактні дані студентів та зашифровані паролі. Аналогічно, інцидент 2023 року в Імперському коледжі Лондона дозволив злочинцям отримати доступ до імен студентів та даних про заборгованість університету. Серед попередніх випадків — атака програм-вимагачів на Ньюкаслський університет у 2020 році, в результаті якої дані студентів і співробітників були опубліковані в даркнеті після того, як навчальний заклад

відмовився сплатити викуп. Крім того, у 2020 році суперкомп'ютер Единбурзького університету було виведено з ладу через шкідливе програмне забезпечення для майнінгу криптовалют, а у 2019 році Університет Варвіка зазнав витоку даних, про який співробітникам і студентам не повідомляли понад шість місяців...

Не всі атаки призвели до викрадення даних; деякі були спрямовані на порушення роботи. У лютому 2024 року як Кембриджський університет, так і Манчестерський університет зазнали тимчасових перебоїв у роботі ІТ-сервісів через DDoS-атаки, відповідальність за які взяла на себе хактивістська група «Anonymous Sudan», яка вказала як мотив зовнішню політику уряду Великої Британії. Крім того, університети також вразливі до непрямих порушень безпеки з боку третіх осіб. У 2020 році масштабна кібератака була спрямована проти компанії Blackbaud, що розробляє програмне забезпечення для збору коштів та управління випускниками, в результаті чого були скомпрометовані дані кількох інших університетів «Russell Group», зокрема Бірмінгемського, Ексетерського, Глазгоського, Лідського, Ліверпульського, Редінгського, Стратклайдського та Йоркського». *(Maia Traverse. Revealed: The eight Russell Group unis hit by cyber attacks since 2020 – Nottingham the most recent // Digitalbox Publishing Ltd (<https://thetab.com/2026/07/10/revealed-the-eight-russell-group-unis-hit-by-cyber-attacks-since-2020-nottingham-the-most-recent>). 10.07.2026).*

Кібербезпека Інтернету речей. Штучний інтелект

«Нещодавній звіт Bitdefender свідчить про зростання занепокоєння тим, що штучний інтелект надає більшу перевагу кібератакувальникам, ніж захисникам: понад половина фахівців з кібербезпеки вважають, що ШІ дає перевагу зловмисникам. Респонденти визначили такі ключові загрози, як вдосконалене шкідливе програмне забезпечення, більш витончені методи соціальної інженерії та автоматизовані моделі атак. У звіті також висвітлюються тривожні тенденції всередині організацій, зокрема зростання випадків приховування інцидентів: понад половина працівників заявили, що їм було наказано не розголошувати про інциденти, що свідчить про те, що культурні уявлення щодо прозорості відстають від нормативних вимог...

Опитування, в якому взяли участь фахівці з різних країн, показало, що випадки витоку даних залишаються поширеним явищем, а серед найпоширеніших інцидентів — несанкціонований доступ до хмарних сервісів, компрометація корпоративної електронної пошти та атаки програм-вимагачів. Воно також виявило такі проблеми, як використання «тіньового ШІ» та значний розрив у рівні впевненості між керівництвом та рядовими співробітниками, причому менеджери часто переоцінюють рівень готовності своїх організацій до забезпечення безпеки. Загалом, отримані дані вказують на зростання тиску на команди з кібербезпеки у міру розвитку загроз, пов'язаних зі штучним інтелектом, а також на внутрішні виклики, пов'язані з прозорістю, видимістю та узгодженістю дій». *(Eric Geller.*

Most cybersecurity workers have been told to conceal a breach, report finds // TechTarget, Inc. (<https://www.cybersecuritydive.com/news/data-breach-coverups-ai-bitdefender/824331/>). 02.07.2026).

«Нове дослідження Університету Вашингтона попереджає, що нові веб-браузери на базі штучного інтелекту з автономними «агентськими» можливостями становлять значну загрозу для кібербезпеки, зокрема через ослаблення таких фундаментальних засобів захисту, як політика «одного походження», яка запобігає доступу веб-сайтів до даних один одного. Під час тестування кількох популярних браузерів з агентами дослідники виявили, що деякі з них дозволяли зловмисним сайтам експлуатувати ці агенти за допомогою таких методів, як «введення підказок» (вбудовування прихованих інструкцій, що змушують ШІ розкривати конфіденційну інформацію) та «отруєння пам'яті», коли скомпрометовані дані впливають на подальші дії...

Оскільки ці агенти можуть отримувати доступ до численних веб-сайтів і взаємодіяти з ними з більшою автономністю, ніж люди, вони можуть бути більш вразливими до маніпуляцій, особливо якщо їм надано широкі повноваження. Хоча більш функціональні браузери забезпечують зручність, вони також підвищують ризик, а безпечніші конструкції, як правило, обмежують функціональність. У дослідженні зроблено висновок, що сучасні браузерні агенти на основі штучного інтелекту ще не є достатньо безпечними для широкого використання, при цьому підкреслюється компроміс між високим рівнем автоматизації та захистом даних користувачів у міру подальшого розвитку технології. *(Stefan Milne. Some agentic AI browsers may come with major cybersecurity risks // Tech Xplore (<https://techxplore.com/news/2026-06-agentic-ai-browsers-major-cybersecurity.html>). 03.07.2026).*

«Штучний інтелект дедалі сильніше впливає на обидві сторони сфери кібербезпеки: організації впроваджують ШІ для покращення виявлення загроз, тоді як кіберзлочинці використовують цю ж технологію для розширення масштабів та посилення атак. Дослідження показують, що багато організацій вважають, що зловмисники отримують перевагу завдяки ШІ, використовуючи його для автоматизації фішингу, створення шкідливого програмного забезпечення та проведення розвідки більш ефективно й переконливо. Це призвело до появи швидших і витонченіших атак, які зменшують перевагу в часі реагування, якою традиційно володіли захисники...

У відповідь на це постачальники послуг з кібербезпеки впроваджують штучний інтелект у системи виявлення та реагування для аналізу поведінки, визначення пріоритетності ризиків та оптимізації розслідувань, допомагаючи командам з безпеки справлятися зі зростаючим обсягом роботи. Однак ефективне впровадження штучного інтелекту пов'язане з певними викликами, зокрема з проблемами якості даних, складністю інтеграції, нестачею кваліфікованих кадрів та необхідністю створення механізмів управління. Експерти наголошують, що для

успішного впровадження штучного інтелекту потрібні уніфіковані платформи, інтегровані робочі процеси та ретельне планування, а не окремі інструменти...

Загалом «гонка озброєнь» у сфері кібербезпеки дедалі більше визначається штучним інтелектом, і організації повинні стратегічно інтегрувати штучний інтелект у свою інфраструктуру безпеки, щоб залишатися стійкими до нових загроз». (*Simon Tung. Harnessing AI in cybersecurity: Ways companies can stay ahead of AI-driven threats // TNGlobal (<https://technode.global/2026/07/06/harnessing-ai-in-cybersecurity-ways-companies-can-stay-ahead-of-ai-driven-threats/>). 06.07.2026*).

«Автономні агенти штучного інтелекту все частіше виконують практичні завдання у сфері кібербезпеки, такі як пошук вразливостей у програмному забезпеченні, проведення тестів на проникнення та організація багатостадійних атак без постійного контролю з боку людини. Натомість дослідження в галузі кібербезпеки з використанням ШІ відстають, оскільки досі обмежуються нестачею фахівців та значною мірою ручними, розробленими вручну експериментами. Щоб усунути цю прогалину, команда з Китайської академії наук пропонує «Cybersecurity AI Scientist» — дослідницьку систему на базі ШІ, яка може самостійно переходити від постановки питання до розробки експерименту, створення інструментів, контрольованого виконання, оцінки та, зрештою, оформлення письмових результатів дослідження... Вони представляють Nephastus як один із способів реалізації цієї ідеї за допомогою модульної мультиагентної системи, в якій спеціалізовані агенти займаються формулюванням проблем, моделюванням загроз, створенням інструментів та підготовкою звітів. Однак автори стверджують, що пряме перенесення методологій вчених у галузі штучного інтелекту з інших галузей не працює в кібербезпеці, оскільки об'єкт дослідження адаптується в процесі його вивчення: платформи моделювання, обмежувальні механізми та доступні інструменти змінюються швидше, ніж може пройти один дослідницький цикл, і може навіть бути незрозуміло, чи залежать результати від окремих елементів методу, таких як кіберполігони, цифрові двійники або ланцюги доказів, вбудовані в саму оцінку... Щоб впоратися з цими труднощами, автори описують «модель чотирьох нулів», зосереджену на чотирьох режимах збою, які система повинна передбачати та мінімізувати: ризик (приховані дефекти в програмному забезпеченні), довіра (допомога, яка залишається відкаліброваною, щоб люди могли й надалі здійснювати нагляд), інцидент (операційні помилки та необхідність тестових середовищ) та енергія (довгострокові організаційні та етичні наслідки). У статті вказується на нещодавнє підвищення можливостей у вимірі ризику, наводяться приклади таких тестових платформ, як CyberGym, які перевіряють агентів на наявність реальних вразливостей і демонструють відносно високі показники успішності для передових моделей, а також здатність виявляти нові вразливості «нульового дня». Також підкреслюється перехід до оборонної стратегії, яку автори називають «легіонами стійких агентів»: припущення про те, що периметр залишається надійним, а ремонт відбувається з людською швидкістю, замінюються ідеєю надлишкової популяції оборонних агентів, розподілених по

всьому периметру мережі... У цій моделі безпека стає «безпекою агентів», а не безпекою кінцевих точок: система керує популяціями агентів, які координують свої дії навколо категоризованих подій та забезпечують відновлення за допомогою пакетних «капсул подій та захисту». Для оцінки автори пропонують проводити позовжнє, зважене за наслідками порівняння результатів у динаміці, вимірюючи наукову віддачу, якість доказів, навантаження на калібрування, стійкість до змін моделей та інструментів, відповідність вимогам управління, а також те, наскільки добре система справляється з подіями, що швидко поширюються та спричиняють значні втрати, а не лише з дрібними проблемами... Вони також наголошують на необхідності обмеження подвійного використання шляхом розділення процедур авторизації для наступальних досліджень, оборонного аналізу, оцінки та прийняття рішень про розгортання, а також шляхом утримання конфіденційної роботи в ізольованих цифрових двійниках та кіберполігонах, причому ключовим питанням є те, хто що авторизував, з якою метою, на підставі яких повноважень та де отримані можливості можуть бути розгорнуті. Ця робота не досягає рівня повністю побудованої системи, натомість пропонуючи рамки з відкритими дослідницькими завданнями, такими як робота з гетерогенними цілями та запобігання перепрофілюванню тих самих можливостей для наступальних цілей — при цьому стверджуючи, що успіх слід оцінювати не лише за швидкістю досліджень, а й за покращеною стратегічною виваженістю, чіткішим визначенням пріоритетів та більш стійким оборонним дизайном». (*Mirko Zorz. Researchers make the case for a cybersecurity AI scientist // Help Net Security (https://www.helpnetsecurity.com/2026/07/07/cybersecurity-ai-scientist-research/). 07.07.2026*).

«У міру того як робочі навантаження штучного інтелекту (ШІ) дедалі частіше переміщуються в середовища публічних хмар, підприємства та регуляторні органи дедалі частіше ставлять питання щодо кібербезпеки нового типу: не просто чи забезпечують хмарні провайдери захист даних під час зберігання та передачі, а як клієнти можуть самостійно перевірити, що базова інфраструктура дійсно обробляє конфіденційну інформацію надійним чином, без жодних порушень безпеки. Ця стурбованість посилюється, оскільки критично важливі робочі навантаження — такі як моделі штучного інтелекту, фінансові системи, додатки для охорони здоров'я та конфіденційна аналітика — працюють на спільних хмарних платформах, а клієнти хочуть бачити докази, а не лише запевнення від провайдерів... Ця проблема стає ще гострішою у випадку генеративного ШІ, де великі мовні моделі обробляють величезні обсяги власних даних, тому надзвичайно важливо мати впевненість, що дані залишаються в безпечних, перевірених середовищах виконання. Компанія DigiCert у співпраці з Google Cloud вирішує цю проблему за допомогою незалежної криптографічної атестації для середовищ конфіденційного обчислення, яка використовує апаратне надійне виконання для ізоляції робочих навантажень під час обробки; додаткова атестація надає незалежне криптографічне підтвердження того, що саме середовище є надійним і немодифікованим, ефективно поширюючи модель довіри

типу РКІ на хмарну інфраструктуру, а не покладаючись лише на внутрішні перевірки провайдера... Загальна тема полягає у переході до «перевірюваної довіри», коли твердження щодо інфраструктури підкріплюються криптографічною верифікацією — що відповідає тенденціям у сферах «нульової довіри», безпеки ланцюга постачання програмного забезпечення та перевірки цифрової ідентичності. У Канаді це питання, ймовірно, набуватиме все більшої актуальності з огляду на потужну інноваційну екосистему країни в галузі штучного інтелекту та зростаюче впровадження хмарних технологій і штучного інтелекту в таких секторах, як фінанси та охорона здоров'я, а також на тлі суворих вимог щодо конфіденційності та зростаючого інтересу до управління даними та відповідального впровадження штучного інтелекту». (*Tim Sandle. Cloud trust is becoming the next cybersecurity battleground for AI // Digital Journal Inc. (<https://www.digitaljournal.com/article/cloud-trust-is-becoming-the-next-cybersecurity-battleground-for-ai/>). 03.07.2026*).

«...Поява передових моделей штучного інтелекту з агентною поведінкою — які в цьому тексті називаються можливостями «Mythos» — знаменує собою постійний структурний зсув у динаміці кібербезпеки, що робить традиційне, поступове формування ІТ-бюджету застарілим. Історично склалося так, що виявлення вразливостей зі швидкістю, властивою людині, дозволяло фінансовим директорам управляти кібербюджетами за допомогою фіксованих відсотків, надаючи інженерним командам достатньо часу для виправлення систем. Сьогодні ж автономні агенти ШІ промислово масштабують виявлення та експлуатацію існуючого технічного боргу зі швидкістю машин, здатні виявляти вразливості в сім разів швидше, ніж люди можуть їх усунути. Як наслідок, високооплачувані інженерні команди страждають від «втоми від сортування», витрачаючи капітал, тоді як критичні загрози залишаються непоміченими...

Щоб вирішити проблему цієї серйозної асиметрії, не обмежуючись лише збільшенням ІТ-бюджету, керівники підприємств повинні терміново перерозподілити капітал, відмовившись від застарілих засобів захисту на основі периметра, і спрямувати його на п'ять критично важливих напрямків. По-перше, операційні витрати слід переорієнтувати на архітектуру «Zero Trust» та мікросегментацію, щоб обмежити масштаби наслідків порушення безпеки та запобігти поперечному переміщенню агентів штучного інтелекту. По-друге, стратегічний капітал необхідно інвестувати в модернізацію інфраструктури та переписання коду на безпечних мовах, щоб назавжди усунути технічний борг. По-третє, організації повинні фінансувати засоби внутрішнього контролю — такі як система запобігання втраті даних (DLP) на рівні запитів та безпечні приватні анклавні штучного інтелекту — щоб запобігти ненавмисному витоку конфіденційних даних співробітниками до загальнодоступних моделей штучного інтелекту... По-четверте, необхідні інвестиції в платформи управління станом безпеки, побудовані на базі штучного інтелекту, щоб миттєво оцінювати ризики в контексті та відфільтровувати нерелевантні сповіщення, гарантуючи, що інженери усувають лише ті вразливості, які несуть істотний фінансовий ризик. Нарешті,

підприємства повинні впроваджувати автономні операції, що використовують агентів штучного інтелекту для автоматизованого управління виправленнями та робочих процесів самовідновлення, тим самим усуваючи затримки, пов'язані з людським фактором, під час усунення вразливостей. Зрештою, таке структурне перерозподілення капіталу вже не є добровільним; це фундаментальна фідучіарна відповідальність, необхідна для захисту бізнесу, збереження страхової придатності та забезпечення довгострокової стійкості підприємства до загроз, що поширюються зі швидкістю машин». (*Kris Lovejoy. Reallocating cybersecurity capital in the Mythos era // FoundryCo, Inc. (<https://www.cio.com/article/4193990/reallocating-cybersecurity-capital-in-the-mythos-era.html>). 08.06.2026*).

«...Звіт про загрози в сфері кібербезпеки став причиною федерального судового позову в Південній Каліфорнії після того, як американський медіа-стартап MeetingTV заявив, що його бізнес був зруйнований через «галюцинацію» штучного інтелекту. У грудні 2025 року компанія Koi Security — яку у квітні 2026 року за сотні мільйонів доларів придбав гігант у сфері кібербезпеки Palo Alto Networks — опублікувала звіт про шпигунську мережу, пов'язану з Китаєм. У звіті помилково було включено домен MeetingTV до переліку «індикаторів компрометації» (Indicators of Compromise). MeetingTV стверджує, що ця класифікація не була результатом традиційного криміналістичного розслідування, а скоріше — неперевіреною, помилковим результатом, згенерованим власною системою штучного інтелекту Koi під назвою «Wings»...

Згідно з позовом проти компанії Koi, її ізраїльських засновників та компанії Palo Alto Networks, оприлюднення цього звіту завдало негайної та катастрофічної шкоди. Постачальники засобів безпеки та корпоративні брандмауери по всьому світу почали автоматично блокувати трафік до MeetingTV, що призвело до серйозних операційних збоїв та обвалу доходів і репутації компанії. Хоча компанія Koi Security згодом оновила звіт, щоб уточнити, що не було доказів, які б пов'язували MeetingTV зі зловмисною діяльністю, стартап стверджує, що шкода вже була незворотною. У відповідь компанія Palo Alto Networks подала клопотання про відхилення позову, стверджуючи, що звіт було опубліковано з добросовісними намірами як дослідження з питань безпеки, що становлять життєво важливий суспільний інтерес, і що в ньому не містилося прямих звинувачень MeetingTV у злочинній діяльності. Сторона захисту наголошує, що дослідники у сфері кібербезпеки повинні бути захищені від позовів про дифамацію під час проведення аналізу критичної інтернет-інфраструктури». (*Meir Orbach. Palo Alto Networks and Koi Security sued over alleged AI error in cyber threat report // CTech (<https://www.calcalistech.com/ctechnews/article/bjkvcpxzl>). 05.07.2026*).

«Агентство з кібербезпеки та безпеки інфраструктури США (CISA) почало використовувати модель штучного інтелекту «Mythos» від компанії Anthropic для аудиту урядового програмного забезпечення на наявність

вразливостей, якими могли б скористатися іноземні розвідувальні служби або кіберзлочинці. Ця ініціатива свідчить про все ширше застосування штучного інтелекту в урядовій кібербезпеці: команда CISA з оцінки площі атаки вже виявила численні слабкі місця в системі безпеки, хоча подробиці щодо цих результатів не оприлюднювалися. Впровадження відбувається попри попередні напруження між компанією Anthropic та урядом США, коли заходи безпеки штучного інтелекту, запроваджені компанією, змусили Пентагон розглядати її як ризик для ланцюга поставок. З того часу відносини покращилися, особливо після того, як Агентство національної безпеки (NSA) почало використовувати Mythos, хоча дискусія щодо заходів безпеки моделі та їхнього оперативного впливу триває». (*Mythos: A New Era in Cyber Defense Amidst Government Struggles // Devdiscourse* (<https://www.devdiscourse.com/article/technology/3946113-mythos-a-new-era-in-cyber-defense-amidst-government-struggles>). 07.07.2026).

«Штучний інтелект стрімко змінює ландшафт кібербезпеки, скорочуючи тривалість складних операцій з безпеки — таких як «червона команда», виявлення вразливостей та розробка засобів виявлення — з місяців до хвилин. У провідних організаціях, таких як Amazon Web Services (AWS), ШІ вже автоматизує створення засобів захисту на основі висновків «червоної команди» всього за п'ятнадцять хвилин, що ілюструє майбутнє високоавтономної безпеки, керованої агентами. Однак цей значний стрибок у можливостях викликає серйозну стурбованість щодо давнього класового розриву в сфері кібербезпеки. Хоча адміністрація Трампа доручила федеральним агентствам розширити доступ до штучного інтелекту для організацій з обмеженими ресурсами, таких як сільські лікарні та місцеві комунальні підприємства, експерти стверджують, що «межа бідності в галузі безпеки» існує вже понад десятиліття. Організації з обмеженими ресурсами, такі як невеликі місцеві органи влади з мінімальним ІТ-персоналом, часто надто перевантажені вирішенням щоденних нагальних проблем, щоб інвестувати час і капітал, необхідні для впровадження або освоєння цих нових технологій...

Крім того, впровадження штучного інтелекту створює унікальні фінансові та операційні ризики, які непропорційно сильно впливають на організації з обмеженим фінансуванням. Наприклад, ті, хто не може дозволити собі дорогі ліцензії корпоративного рівня, можуть бути змушені поступитися конфіденційністю даних, використовуючи загальнодоступні моделі, що створює небезпечний компроміс. Непередбачуване ціноутворення на токени, засноване на обсязі використання, також значно ускладнює складання бюджету для невеликих компаній з низькою рентабельністю. Хоча вартість моделей з часом може знизитися, вартість висококваліфікованих фахівців, здатних безпечно керувати цими інструментами ШІ, залишається стійкою перешкодою. Це свідчить про те, що розрив визначається не лише доступом до моделей, а й операційною глибиною, необхідною для запуску циклів безпеки виробничого рівня. Справжня безпека залежить від зберігання конфіденційних корпоративних даних у контрольованих, централізованих середовищах, а не від експериментів на особистих ноутбуках...

І навпаки, деякі керівники у сфері безпеки вважають, що ШІ в кінцевому підсумку стане чудовим вирівнювачем, а не чинником розколу. Оптимістично налаштовані аналітики стверджують, що нинішній розрив у доступі до передових моделей, таких як обмежена у доступі Claude Mythos, є лише тимчасовим. Архітектури з відкритою вагою, квантизація та стрімкий розвиток систем другого рівня означають, що високопродуктивні інструменти ШІ незабаром стануть недорогими й легко працюватимуть на стандартному обладнанні, що дозволить захисникам використовувати ті самі складні інструменти, що й зловмисники... З цієї точки зору ШІ демократизує елітні можливості — дозволяючи навіть найменшим організаціям використовувати автоматизовані тестування «червоної команди», виявлення внутрішніх загроз та моніторинг дотримання нормативних вимог, які раніше були фінансово недоступними. Зрештою, новий розрив у кібербезпеці, пов'язаний із ШІ, визначатиметься не самою технологією, а тим, чи зможе галузь успішно використовувати ці автоматизовані інструменти, щоб допомогти тим, хто перебуває за межею бідності, наздогнати лідерів, чи це просто послужить мультиплікатором сили для організацій, які вже мають найкращі можливості для самозахисту». (*Cynthia Brumfield. Can AI narrow cybersecurity's class divide? // FoundryCo, Inc. (<https://www.csoononline.com/article/4195787/can-ai-narrow-cybersecuritys-class-divide.html>). 13.07.2026*).

«...Штучний інтелект стає основною інфраструктурою 21 століття, стрімко перетворюючись із вузькоспеціалізованих інструментів обробки даних на автономні системи, здатні до логічного мислення, які переосмислять людський потенціал у всіх галузях. У міру того, як ми вступаємо в «Еру прискорення», конвергенція ШІ з квантовими обчисленнями, робототехнікою та біотехнологіями відкриває безпрецедентні можливості — такі як трансформація сфери охорони здоров'я, оптимізація глобальних ланцюгів постачання та розширення когнітивних здібностей — але водночас створює безпрецедентні вразливості. Ця парадигма подвійного призначення робить ШІ як найпотужнішим оборонним активом у сфері кібербезпеки, так і потужним інструментом для зловмисників, які використовують генеративний ШІ для розгортання просунутих фішингових атак, поліморфного шкідливого програмного забезпечення та дїпфейків...

Отже, традиційна кібербезпека, заснована на периметрі, на сьогодні є застарілою. Щоб безпечно використовувати трансформаційний потенціал ШІ, зацікавлені сторони повинні інтегрувати підхід «Security by Design» та надійні принципи «Zero Trust» упродовж усього життєвого циклу ШІ. Це включає впровадження систем виявлення загроз, вдосконалених за допомогою ШІ, конфіденційного обчислення для захисту даних та постквантової криптографії. Крім того, у міру того як ШІ еволюціонує у складний «стек інтелекту» — модульну архітектуру, що поєднує дані, моделі, оркестрування, агенти та управління, — він потребує комплексних регуляторних рамок та державно-приватних партнерств. Нещодавній указ Білого дому підкреслює цю реальність: кібербезпека більше не є допоміжною функцією, а є необхідною основою для безпечних інновацій у сфері

III. Зрештою, узгодження цього стрімкого технологічного прогресу з етичним наглядом, стійкою інфраструктурою та кваліфікованим людським контролем є необхідною умовою для забезпечення нашого гіперпідключеного майбутнього...» (*Chuck Brooks. Tracking The AI Revolution: Innovation And Cyber Risks // Forbes Media LLC* (<https://www.forbes.com/sites/chuckbrooks/2026/07/13/tracking-the-ai-revolution-innovation-and-cyber-risks/>). 13.07.2026).

«Компанія OpenAI розробила GPT-Red — передову модель штучного інтелекту, призначену виключно для внутрішнього використання, яка спеціально створена для автоматизації процесу «ред-тімінгу», що дозволяє виявляти та усувати вразливості в системах III до того, як зловмисники зможуть ними скористатися. У міру того, як системи штучного інтелекту все більше інтегруються із зовнішніми інструментами, такими як браузері та електронна пошта, вони стають дедалі вразливішими до маніпуляцій, зокрема до атак типу «prompt injection». Оскільки тестування безпеки силами людей є трудомістким і важко масштабується, OpenAI навчила GPT-Red за допомогою методу підкріплювального навчання з самограми, в рамках якого модель постійно змагалася з моделями захисників у реалістичних імітованих середовищах... Ці масштабні інвестиції в безпеку штучного інтелекту дали вражаючі результати: GPT-Red успішно зламав майже всі протестовані моделі аж до GPT-5.5, виявив нові вектори атак, такі як ін'єкції «Fake Chain-of-Thought», і значно перевершив людських хакерів у відтвореному випробуванні (рівень успішності 84% порівняно з 13% у людей). Крім того, GPT-Red успішно зламав діючий агент-автомат зі штучним інтелектом стороннього розробника, продемонструвавши свою ефективність у реальних умовах... Важливо, що атаки, згенеровані GPT-Red, згодом були використані для навчання флагманської моделі OpenAI — GPT-5.6, що зробило її значно стійкішою до прямих вторгнень у промпти. Хоча GPT-Red не буде оприлюднено, щоб запобігти його зловживанню як інструменту для атак, ця модель знаменує значний прогрес у сфері безпеки III, створюючи безперервний цикл зворотного зв'язку, в якому сучасні моделі III активно забезпечують безпеку майбутніх поколінь». (*Bhaswati Guha Majumder. OpenAI Unveils GPT-Red: AI 'Super-Hacker' Built to Hunt Vulnerabilities Before Cybercriminals Can Exploit Them // IBTimes Co., Ltd.* (<https://www.ibtimes.sg/openai-unveils-gpt-red-ai-super-hacker-built-hunt-vulnerabilities-before-cybercriminals-can-89863>). 16.07.2026).

«22 червня розвідувальний альянс «Five Eyes» — до складу якого входять США, Велика Британія, Канада, Австралія та Нова Зеландія — опублікував спільну заяву, в якій попередив, що стрімкий розвиток передових технологій штучного інтелекту (ШІ) змінює характер кіберризиків та різко скорочує терміни здійснення кібератак. Прикладом такого переходу є такі передові системи, як модель Claude Mythos від компанії Anthropic, яка розроблена для забезпечення кібербезпеки, автономного кодування та роботи довготривалих агентів... Під час контрольованих випробувань, за якими спостерігали фахівці

Агентства національної безпеки США, модель Mythos виявила 271 уразливість у браузері Mozilla Firefox і успішно створила діючі експлойти для 181 з них. Окрім цього конкретного інструменту, сучасні системи штучного інтелекту здатні швидко й безперервно сканувати складні кодові бази з метою виявлення раніше невідомих уразливостей типу «нульового дня», а також об'єднувати численні слабкі місця низького та середнього рівня серйозності у складні, взаємопов'язані ланцюжки атак... Таке безперервне автоматичне виявлення різко скорочує традиційний часовий запас, на який покладаються захисники для встановлення виправлень до програмного забезпечення до того, як відбудеться зловживання вразливістю, що призводить до швидкого поширення оновлень можливостей у ширшій екосистемі штучного інтелекту...

Сектор фінансових послуг є особливо вразливим до цих загроз, що набирають обертів, через свою складну та тісно взаємопов'язану цифрову інфраструктуру. Багато фінансових установ поєднують застарілі архітектури з сучасними хмарними системами, що вимагає ретельного тестування та отримання дозволів від регуляторних органів перед тим, як можна буде розгорнути оновлення безпеки. Це створює небезпечні затримки у встановленні оновлень, якими легко можуть скористатися автоматизовані системи, що працюють зі швидкістю машин. Оскільки фінансові платформи значною мірою залежать від спільних постачальників та стандартизованого програмного забезпечення, навіть одна вразливість може спровокувати системні, взаємопов'язані кібершоки, що охоплюють одразу кілька установ, а не окремі інциденти... Згідно з доповіддю Міжнародного валютного фонду від 7 травня, така динаміка надає зловмисникам очевидну перевагу в швидкості над захисниками в умовах екосистеми з високим рівнем взаємозалежності. Ці проблеми ускладнюються оперативними труднощами, такими як збільшення часу простою систем через частіші оновлення та нерівномірний доступ до обчислювальних ресурсів, що створює розрив у захисних можливостях між великими та малими фінансовими установами... Відповідно, фінансові органи зараз розглядають кіберризики як пряму загрозу загальній фінансовій стабільності, попереджаючи, що взаємопов'язані збої можуть поширюватися через платіжні, розрахункові та ліквідні мережі. Зрештою, ситуація у сфері кібербезпеки структурно перетворилася на середовище постійної вразливості, що вимагає від організацій відмовитися від механізмів захисту, що працюють зі швидкістю людського реагування, на користь безперервної, високочастотної операційної стійкості». *(Alexander Jones. AI, Mythos and the New Era of Global Cybersecurity Risk // International Banker (<https://internationalbanker.com/technology/ai-mythos-and-the-new-era-of-global-cybersecurity-risk/>). 17.07.2026).*

«Хоча організаціям часто обіцяють, що штучний інтелект та передові механізми управління допоможуть вирішити сучасні виклики у сфері кібербезпеки, ці інструменти в кінцевому підсумку виявляються неефективними, якщо у відносинах між директором з інформаційних технологій (CIO) та директором з інформаційної безпеки (CISO) відсутні взаємна довіра та узгодженість дій. Технології та автоматизація не можуть

замінити міцне партнерство між людьми, яке є фундаментальною інфраструктурою, що забезпечує цілісність програми безпеки підприємства. Реальні приклади успіху, такі як партнерство між колишнім СІО штату Вашингтон Біллом Кехо та CISO Ральфом Джонсоном, демонструють, що послідовна щоденна комунікація робить ці високонапружені керівні посади стійкими. Коли безпека з самого початку інтегрується безпосередньо в основні технологічні рішення, а не розглядається як щось другорядне, керівництво створює необхідні умови для співпраці, завдяки яким технічні засоби контролю та системи управління можуть дійсно досягти успіху...

Така узгодженість є особливо важливою в умовах, коли цифрові операції прискорюються до швидкості роботи машин. Оскільки платформи на базі штучного інтелекту та автоматизовані програмні агенти виконують робочі процеси за лічені секунди, організації не можуть дозволити собі обговорювати розподіл ролей або налагоджувати довіру під час активного кіберінциденту; ланцюжок ескалації через людей та взаємна довіра повинні бути вже міцно встановлені. Окрім управління безпосередніми технічними кризами, тісні співпраці є найефективнішим засобом боротьби з серйозним вигоранням, яке наразі вражає посаду CISO, яка історично несе величезну відповідальність без відповідних повноважень в організації. Ізольований CISO є значною вразливістю, тоді як CISO, якого підтримує узгоджений з ним СІО, розділяє оперативне та репутаційне навантаження місії, створюючи надійну систему захисту, коли критичні інциденти загрожують довірі громадськості та інституцій...

Досягнення такого рівня узгодженості вимагає цілеспрямованого лідерства, а не пасивної залежності від електронного листування, нормативних документів чи технологічних платформ. Щоб сприяти справжній співпраці, організації можуть створити структуровані, нейтральні майданчики — такі як ради з питань штучного інтелекту — щоб виносити на обговорення складні технічні та етичні питання ще до виникнення кризи. Щоб цілеспрямовано налагодити цей зв'язок, СІО та CISO повинні встановити постійний, майже щоденний ритм взаємодії, чітко визначити повноваження щодо прийняття рішень та рамки відповідальності в спокійні періоди, а також спільно перетворювати складні показники безпеки на конкретні бізнес-результати. Зрештою, організації, які надають пріоритет такому партнерству між людьми, а не суто технологічним скороченням шляхів, зможуть безпечніше впроваджувати стратегії штучного інтелекту, завоювати довіру своїх правлінь завдяки єдиній позиції керівництва та набагато швидше, ніж їхні конкуренти, долати сучасні цифрові ризики». (*Steve Tout. The last human relationship in cybersecurity // FoundryCo, Inc. (<https://www.cio.com/article/4197971/the-last-human-relationship-in-cybersecurity.html>). 17.07.2026*).

«У відповідь на стрімкий темп технологічних інновацій, прикладом яких є випуск моделі Claude Mythos від компанії Anthropic, уряд Японії переглянув свої керівні принципи щодо штучного інтелекту, спочатку сформовані в грудні минулого року. Затверджені Кабінетом міністрів, переглянуті керівні принципи стосуються серйозних ризиків кібератак, пов'язаних із передовими

генеративними моделями, та передбачають суттєве посилення потенціалу Японського інституту безпеки штучного інтелекту шляхом активної співпраці з іноземними урядовими установами та приватними розробниками штучного інтелекту. З метою захисту національних інтересів у цих принципах наголошується на важливості уникнення надмірної залежності від конкретних іноземних держав або корпорацій, а також висловлюється намір уряду розробляти власні моделі штучного інтелекту, адаптовані до унікальних суспільних викликів Японії... Крім того, в оновлених рекомендаціях наголошується на необхідності просування «вертикального» ШІ для спеціалізованих галузей та «фізичного» ШІ для управління робототехнікою, а також закликаються організації реструктурувати свою діяльність з метою кращої інтеграції цих технологій. Нарешті, з метою управління довгостроковими суспільними змінами політика передбачає проведення постійних досліджень щодо розподілу праці між людьми та машинами, а також розробку освітніх середовищ, покликаних запобігти зниженню когнітивних та фізичних здібностей людини, що може бути наслідком надмірної залежності від систем штучного інтелекту». (*Japan revises AI policy guidelines to bolster cybersecurity* // *THE JAPAN TIMES LTD.* (<https://www.japantimes.co.jp/news/2026/07/16/japan/japan-ai-policy-revision-cybersecurity/>). 16.07.2026).

«Штучний інтелект докорінно змінює сферу кібербезпеки, прискорюючи перетворення загроз із технічної проблеми на критичний бізнес-ризик, що вимагає нової, інтегрованої моделі реагування. ШІ виступає як захисним інструментом, так і потужним прискорювачем для зловмисників, які зараз використовують великі мовні моделі для автоматизації цілих атак — від розвідки цілей до викрадення даних — та створюють надзвичайно переконливі дідфейки й кампанії соціальної інженерії. Ці інциденти, пов'язані з використанням ШІ, до яких також належать ризики, пов'язані з власним середовищем ШІ організації, створюють загальну бізнес-проблему, ускладнюючи визначення того, що є реальним, і, таким чином, спричиняють швидкі правові, репутаційні та фінансові наслідки, з якими не може впоратися лише команда з безпеки...

Отже, керівники підприємств та ради директорів повинні перенести акцент з самої технології на її вплив на бізнес, зосередившись на тому, як ці швидкі та більш адаптивні атаки впливають на ризики підприємства, породжують юридичну відповідальність та можуть зашкодити репутації з тією ж швидкістю, з якою формується громадська думка. Вирішенням є перетворення готовності до кризових ситуацій, пов'язаних зі штучним інтелектом, на міжфункціональну ініціативу, оновлення посібників з реагування на інциденти з урахуванням реалістичних сценаріїв використання ШІ, таких як «дідфейки» та кампанії з поширення дезінформації. Для цього необхідно об'єднати зусилля фахівців з кібербезпеки, юристів, фахівців з комунікацій, ризиків та керівництва, щоб перевірити процес прийняття рішень на міцність за допомогою настільних навчань та повномасштабних симуляцій. Заздалегідь підготувавши шаблони реагування, визначивши зовнішніх експертів та встановивши чітку політику використання ШІ,

організації зможуть створити необхідні процеси для ефективного реагування, зменшення плутанини та збереження довіри у разі виникнення кризи, спричиненої ШІ». (*Brandy Wityak. Why Business Leaders Need a New Response Model to AI-Enabled Incidents // Cybersecurity Insiders* (<https://www.cybersecurity-insiders.com/why-business-leaders-need-a-new-response-model-to-ai-enabled-incidents/>). 20.07.2026).

Штучний інтелект, як інструмент боротьби із кіберзлочинністю

«Згідно з новим звітом ISC2 «Переосмислення впливу штучного інтелекту на ролі у сфері кібербезпеки», штучний інтелект кардинально змінює обов'язки, робочі процеси та рівень стресу фахівців з кібербезпеки, що в кінцевому підсумку підвищує попит на перевірку результатів людиною та управління процесами. Штучний інтелект не замінює працівників, а переорієнтовує їхні ролі на виконання завдань з вищою доданою вартістю: 65% опитаних фахівців витрачають більше часу на прийняття рішень щодо того, коли довіряти рекомендаціям ШІ, а 63% приділяють більше часу перевірці та підтвердженню результатів роботи ШІ. Такий людський контроль залишається критично важливим, оскільки майже 90% респондентів стикалися з некоректними рекомендаціями, згенерованими ШІ, а половина всіх організацій покладає остаточну відповідальність на людей, які приймають рішення, коли ці автоматизовані дії призводять до неправильних результатів...

Операційний та психологічний вплив ШІ на команди з безпеки є дуже багатограним. Хоча 48% фахівців зазначають, що ШІ зменшив їхній загальний рівень стресу на робочому місці, майже третина відчула зростання стресу, що тісно пов'язано з інтенсивним тиском, пов'язаним із перевіркою результатів роботи ШІ та прийняттям рішень щодо того, коли слід діяти відповідно до автоматизованих рекомендацій. Крім того, 48% респондентів повідомляють, що витрачають менше часу на завдання, які не пов'язані з ШІ, що свідчить про значний перехід до робочих процесів із використанням ШІ. Незважаючи на цю інтеграцію, 62% фахівців стверджують, що базові навички у сфері кібербезпеки залишаються необхідними, відкидаючи думку про те, що автоматизація зменшила потребу в основних технічних знаннях. ШІ також активно переосмислює шляхи розвитку на початку кар'єри: хоча 56% респондентів вважають, що ШІ зменшив потребу в традиційних посадах початкового рівня, 53% бачать у ньому створення цілком нових можливостей для початківців, а 48% відчують більший оптимізм щодо своїх довгострокових кар'єрних перспектив...

Зрештою, успішна інтеграція ШІ в операції з кібербезпеки залежить від надійних організаційних запобіжних заходів. Приблизно 80% фахівців наголошують на критичній важливості створення чітких механізмів управління, визначення, коли можна довіряти результатам ШІ, та точного розуміння, коли слід ігнорувати автоматизовані рішення. Як підкреслює генеральний директор ISC2 Скотт Біл, ШІ не замінює фахівців з кібербезпеки, а навпаки — змінює вимоги, які

ця професія ставить перед ними. У міру того як машини беруть на себе повторювані та швидкі аналітичні завдання, роль людей зміщується в бік стратегічної перевірки та критичного аналізу, що робить необхідними постійні інвестиції організації в управління, наставництво та розвиток навичок на всіх рівнях...» (*ISC2 Research Finds AI Is Reshaping Cybersecurity Roles and Increasing Human Oversight* // *Yahoo! Finance*. (<https://finance.yahoo.com/technology/ai/articles/isc2-research-finds-ai-reshaping-100000750.html>). 14.07.2026).

«Опитування SANS щодо штучного інтелекту за 2026 рік, в якому взяли участь 536 фахівців у галузі кібербезпеки та ІТ з усього світу, а також 57 керівників вищого рівня у сфері безпеки, показує, що у 2026 році команди з безпеки впроваджували штучний інтелект швидше, ніж у будь-якому попередньому році, хоча структури управління та кадрові ресурси, необхідні для підтримки цієї інтеграції, не встигали за цими темпами. Хоча ШІ активно використовується в повсякденних операціях, таких як розслідування, реагування та забезпечення безпеки додатків, лише 27% фахівців описують свої впровадження ШІ як зрілі виробничі рішення, тоді як більшість із них все ще перебуває на пілотній або допоміжній стадії. Незважаючи на це, «червоні команди» з використанням ШІ стали переважною практикою: у 2026 році їх використовували 61% фахівців, порівняно з лише 33% у 2025 році. Крім того, 76% команд з безпеки взяли на себе функції управління корпоративним ШІ, проте більше половини з них не мають офіційних систем аудиту для забезпечення виконання цих обов'язків. Ця відсутність структурної підтримки супроводжується зростанням незадоволеності результатами роботи: 63% фахівців повідомили про значні недоліки ШІ у виявленні загроз та реагуванні на них, що є зростанням порівняно з 45% у 2025 році...

Ця затримка в регулюванні є вкрай критичною, оскільки зловмисники активно інтегрують ШІ майже на кожному етапі життєвого циклу атаки, використовуючи його для розвідки, експлуатації вразливостей та соціальної інженерії на основі «дідфейків». Загалом 95% респондентів вважають, що зловмисники використовують ШІ, а 78% організацій повідомили про підтверджені або ймовірні атаки з використанням ШІ протягом останнього року. Для протидії цим загрозам людська експертиза залишається основною опорою захисту. Майже половина опитаних фахівців вважають виявлення поведінкових аномалій найефективнішим засобом контролю, за ним слідує навчання користувачів з підвищення обізнаності (45%) та перевірка людськими аналітиками (39%)... Оскільки для виявлення того, що пропускають автоматизовані інструменти, необхідна перевірка людиною, 73% фахівців повідомили, що у 2026 році штучний інтелект змінив вимоги до підготовки їхніх команд, тоді як у 2025 році таких було лише 51%. Щоб подолати існуючий розрив у рівні готовності, у звіті окреслено три необхідні зміни: створення інфраструктури перевірки ШІ, яка вимірює точність, повноту виявлення та забезпечує постійне порівняння, а не лише обсяг впровадження; перенесення управління з політичних документів у сферу щоденного оперативного контролю, що забезпечує безпечний доступ до конфіденційних даних; а також розгляд

негайного підвищення кваліфікації персоналу як нагального оперативного пріоритету, а не як майбутньої мети з найму». *(AI Use in Cybersecurity Jumped From 50% to 78% in a Year. AI-Related Failures Rose Sharply Too. New SANS Institute Survey Reveals a Governance Gap // The Manila Times (<https://www.manilatimes.net/2026/07/14/tmt-newswire/globenewswire/ai-use-in-cybersecurity-jumped-from-50-to-78-in-a-year-ai-related-failures-rose-sharply-too-new-sans-institute-survey-reveals-a-governance-gap/2383643>). 14.07.2026).*

Штучний інтелект, як зброя кіберзлочинців

«Дослідники виявили, на їхню думку, першу задокументовану операцію з використанням програм-вимагачів під назвою «JadePuffer», яка була повністю здійснена автономним агентом на основі великої мовної моделі (LLM). За даними Sysdig, агент на базі штучного інтелекту виконав повний ланцюжок атак — розвідку, викрадення облікових даних, горизонтальне переміщення, встановлення стійкого доступу, підвищення привілеїв і, зрештою, шифрування даних — і міг адаптуватися в режимі реального часу у разі невдачі окремих етапів, наприклад, повторюючи спроби з уточненими параметрами та виправляючи невдалий вхід у систему протягом 31 секунди... Операція розпочалася з експлуатації раніше виправленої уразливості, що дозволяла віддалено виконати код без аутентифікації (CVE-2025-3248) у Langflow — фреймворку з відкритим кодом для створення додатків на основі великих мовних моделей (LLM), яку CISA також позначила як таку, що експлуатувалася під час атак на кінцеві точки, підключені до Інтернету. Отримавши можливість виконання коду, агент зробив дамп бази даних PostgreSQL Langflow, зібрав інформацію про хост та середовище, здійснив пошук конфіденційних файлів та облікових даних, просканував сховище об'єктів MinIO за допомогою адаптивної логіки API та забезпечив свою стійкість за допомогою серверного завдання cron, яке кожні 30 хвилин надсиало сигнал до інфраструктури зловмисника... Потім зловмисник перейшов з Langflow на виробничий сервер MySQL, на якому працювала система Alibaba Nacos, використовуючи облікові дані користувача root невідомого походження, скористався вразливістю, що дозволяла обійти аутентифікацію (CVE-2021-29441), щоб отримати несанкціонований адміністративний доступ, вивчила можливості виходу з контейнера та розгорнула корисне навантаження програми-вимагача, зашифрувавши 1 342 елементи конфігурації Nacos — за допомогою функцій MySQL, видаливши оригінальні таблиці та створивши записку з вимогою викупу, що містила адресу для оплати та контактні дані. Sysdig зазначає, що, хоча у записці з вимогою викупу йдеться про шифрування AES-256, дослідники підозрюють використання слабшого алгоритму AES-128-ECB; вони також вказують на підозрілі артефакти, такі як, ймовірно, тимчасовий біткойн-адресу та код, що містить коментарі з оперативними міркуваннями, написані природною мовою... Загалом, компанія Sysdig стверджує, що цей випадок свідчить про появу «агентних зловмисників», що потенційно знижує поріг кваліфікації для

використання складних програм-вимагачів, водночас створюючи нові можливості для їх виявлення, оскільки корисні навантаження, згенеровані штучним інтелектом, можуть бути ідентифіковані сучасними засобами безпеки». (*Bill Toulas. JadePuffer ransomware used AI agent to automate entire attack // Bleeping Computer® LLC (<https://www.bleepingcomputer.com/news/security/jadepuffer-ransomware-used-ai-agent-to-automate-entire-attack/>). 04.07.2026*).

Кіберзлочинність та кібертероризм

«Атаки типу ClickFix, які базуються на соціальному інжинірингу, що спонукає жертв самостійно виконувати шкідливі команди, постійно еволюціонують і використовують підроблені сторінки верифікації Google та Cloudflare для розповсюдження широкого спектру шкідливого програмного забезпечення. Ці кампанії, що діють з кінця 2025 року, використовують переконливі приманки — такі як підроблені тести reCAPTCHA, «виправлення» аудіо в Google Meet та генератори QR-кодів — щоб змусити користувачів скопіювати та вставити шкідливі команди PowerShell у свої термінали...

Діючи з спільної інфраструктури, яка активно використовує контейнери Cloudflare R2 та IP-адреси, розміщені компанією Dedik Services Limited, зловмисники використовують каталог C:\ProgramData\Zooms для розпакування корисних навантажень. Ці навантаження доставляють різні програми для викрадення даних та трояни віддаленого доступу, зокрема HijackLoader, NetSupport, CastleLoader та StealC. В одному з найпомітніших ланцюгів зараження команда PowerShell завантажує троянізовану версію додатка для обміну повідомленнями з відкритим кодом «Franz», який виступає завантажувачем для нещодавно виявленого завантажувача .NET під назвою «ResiLoader». ResiLoader запускається шляхом перехоплення DLL, обходить антивірусне програмне забезпечення, розміщуючи вразливий драйвер для припинення роботи процесів безпеки, обходить UAC, забезпечує стійкість у системі та, зрештою, розгортає інфостілер StealC за допомогою порожнечності процесу...

Щоб захиститися від цих атак, експерти з кібербезпеки настійно рекомендують користувачам ніколи не виконувати несподівані команди в терміналі — особливо на сторінках підтвердження — бути обережними щодо тактик, спрямованих на створення тиску, а також регулярно оновлювати програмне забезпечення для забезпечення безпеки, щоб блокувати шкідливі домени ще до початку ланцюжка зараження. (*Gabriele Orini. Fake Google and Cloudflare verification pages spread multiple malware families // Malwarebytes (<https://www.malwarebytes.com/blog/threat-intel/2026/07/fake-google-and-cloudflare-verification-pages-spread-multiple-malware-families>). 02.07.2026*).

«Дослідники з безпеки компанії JFrog виявили кампанію кібершпигунства, пов'язану з Північною Кореєю, яку, ймовірно, організувала

група «Lazarus». У її рамках було використано шість шкідливих пакетів npm, призначених для імітації легітимних інструментів polyfill для Rollup. Ці пакети, зокрема «rollup-packages-polyfill-core», точно імітували метадані та структуру справжніх проєктів, щоб ввести розробників в оману. Використовуючи багаторівневий, прихований ланцюжок доставки, розроблений для обходу пісочниць, шкідливе програмне забезпечення завантажувало приховані залежності другого рівня, які виконували вбудовані корисні навантаження... Після розгортання шкідливе ПЗ надавало зловмисникам широкі можливості віддаленого керування ураженими комп'ютерами під управлінням Windows та активно збирало облікові дані розробників, ключі SSH, криптовалютні гаманці та налаштування з таких основних інструментів, як VS Code та AWS. Цей інцидент є частиною ширшої, тривалої хвилі атак на ланцюг постачання, спрямованих на репозиторії з відкритим кодом, такі як npm та PyPI, що підкреслює критичну вразливість робочих станцій розробників та конвеєрів безперервної інтеграції (CI) до витончених кампаній з крадіжки облікових даних та отримання віддаленого доступу. З того часу всі шість шкідливих пакетів було видалено з реєстру npm». *(Ana Maria Constantin. North Korea-linked npm packages impersonate Rollup polyfill tools to steal developer secrets // Cogneve, INC (<https://thenextweb.com/news/north-korea-npm-rollup-polyfill-developer-secrets>). 03.07.2026).*

«Кіберзлочинне угруповання TeamPCP, відоме численними атаками на ланцюги постачання, що полягають у зараженні репозиторіїв програмного забезпечення з відкритим кодом, таких як npm та PyPI, уклало партнерство з операцією «вимагальне програмне забезпечення як послуга» (RaaS) Vect, щоб ефективніше монетизувати свої вторгнення. TeamPCP, до складу якої, ймовірно, входять колишні члени підліткового кіберзлочинного угруповання «The Com», використовує конвеєри безперервної інтеграції для швидкого поширення шкідливого коду. Нещодавно група взяла на приціл такі інструменти, як KICS і Trivy, щоб розповсюдити троянізовані бібліотеки Python, які були завантажені десятки тисяч разів, перш ніж їх було виявлено... Хоча TeamPCP демонструє високу ефективність у отриманні початкового доступу — зламавши такі організації, як Cisco, Trellix, Checkmarx та GitHub — їй історично не вдавалося перетворити цей доступ на грошовий прибуток. Щоб вирішити цю проблему, група уклала союз як із угрупованням Lapsus\$, що спеціалізується на витоках даних, для продажу викрадених даних, так і з нещодавно створеною групою Vect для розповсюдження програм-вимагачів у зламаних мережах... Однак це партнерство зіткнулося зі значними труднощами: дослідники у сфері кібербезпеки виявили серйозні недоліки в коді шифрувального модуля Vect, через які великі файли стають остаточно втраченими, навіть у разі сплати викупу. Як наслідок, TeamPCP заявила, що використовує виключно власний шифрувальний модуль «CipherForce», а не недосконалі інструменти Vect, що змусило експертів застерігати жертв від сплати викупу цим угрупованням, оскільки відновлення даних залишається вкрай сумнівним». *(Mathew J. Schwartz. Vect and TeamPCP Cybercrime Groups Link for Ransomware Hits // Information Security Media Group, Corp.*

(<https://www.inforisktoday.com/vect-teampcp-cybercrime-groups-link-for-ransomware-hits-a-32159>). 06.07.2026).

«Китайські хакери, відомі під назвою «UAT-7810», активно розширюють мережу Operational Relay Box (ORB), зламуючи незахищені мережеві пристрої, підключені до Інтернету — переважно маршрутизатори Ruckus та ASUS — з використанням відомих вразливостей. Ця мережа ORB використовується іншими просунутими постійними загрозами, пов'язаними з Китаєм, для проксі-передачі свого трафіку через регіональні пристрої, що створює враження локального походження трафіку та значно ускладнює його виявлення та атрибуцію. Дослідники Cisco Talos виявили кілька нових і постійно вдосконалюваних шкідливих програм, які сприяють цьому розширенню... Центральне місце в цій кампанії займає LONGLEASH — надзвичайно вдосконалена версія раніше відомого бекдору SHORTLEASH, що має широкі можливості проксі-сервера, зворотні шели, функціонал проміжного сервера C2 та протоколи самовидалення. Хакери також використовують DOGLEASH — полегшений бекдор для Linux, призначений для виконання команд оболонки та довільного коду безпосередньо в пам'яті; JARLEASH — адміністративний інструмент на базі Java для веб-управління файлами; а також LEASHTEST — утиліту, призначену для перевірки, чи підтримують пристрої IoT на базі архітектури MIPS роботу шкідливого програмного забезпечення... Цей набір інструментів, що постійно розвивається, свідчить про те, що UAT-7810 активно модернізує свою інфраструктуру з метою створення більш надійної та функціональної мережі ретрансляторів для кібершпигунства в інтересах держави». (*Bill Toulas. Chinese hackers develop LONGLEASH malware to expand ORB network // Bleeping Computer® LLC* (<https://www.bleepingcomputer.com/news/security/chinese-hackers-develop-longleash-malware-to-expand-orb-network/>). 07.07.2026).

У червні 2026 року в зоні відповідальності Центру об'єднання інформації (IFC) було зареєстровано загалом 40 інцидентів у сфері кібербезпеки, усі з яких були пов'язані з суднами, що передавали неправдиву інформацію через сигнали системи автоматичної ідентифікації (AIS). Вважається, що така діяльність, яка включає передачу оманливих даних, таких як неправдиві назви або типи суден, є спробою ввести в оману морських спостерігачів щодо ідентичності або призначення судна. IFC зазначає, що цей вид обману з використанням AIS є поширеною проблемою в регіоні, яка набуває все більшого масштабу, і очікується, що кількість зареєстрованих інцидентів буде й надалі зростати у міру вдосконалення механізмів виявлення. Це зростання кількості зареєстрованих випадків також пов'язане зі зміною методології звітності IFC, яка перейшла до підходу, орієнтованого на конкретні цілі, з метою кращого аналізу та розуміння регіональних загроз кібербезпеці». (*IFC: AIS deception drives surge in maritime cyber security incidents // SAFETY4SEA* (<https://safety4sea.com/ifc-ais-deception-drives-surge-in-maritime-cyber-security-incidents/>). 07.07.2026).

«Морський та офшорний енергетичні сектори стикаються із серйозною загрозою кібербезпеці через інцидент «FortiBleed», в результаті якого стався витік понад 86 000 облікових даних адміністраторів для брендмауерів та VPN-мереж Fortinet. За даними компанії з кібербезпеки Cudome, цей витік даних зачіпає приблизно 50% усіх пристроїв FortiGate, доступних через Інтернет, у тому числі понад 700 пристроїв, пов'язаних із морським супутниковим зв'язком, що робить понад 250 компаній у цих секторах вкрай вразливими до кібератак... Корінь проблеми полягає не в новій уразливості програмного забезпечення, а в неналежній практиці використання паролів: багато організацій не оновлюють застарілі облікові дані, не змінюють облікові записи адміністраторів за замовчуванням і не забезпечують належного захисту інтерфейсів управління, що мають вихід в Інтернет. Це дозволяє зловмисникам використовувати старі, дійсні облікові дані навіть після встановлення програмних виправлень. З огляду на те, що у 2026 році кількість кіберінцидентів зростає, а Берегова охорона США повідомляє про 71-відсоткове збільшення атак на основі облікових даних у 2025 році, такі органи, як NCSC, закликають постраждалі організації негайно ізолювати скомпрометовані пристрої, скинути налаштування систем та запровадити сувору політику ротації облікових даних і багатофакторну автентифікацію, щоб запобігти подальшому проникненню в мережу». *(Martyn Wingrove. Firewall hacks, password leaks threaten major maritime, offshore energy companies // Riviera Maritime Media Ltd. (<https://www.rivieramm.com/news-content-hub/firewall-hacks-password-leaks-threaten-major-maritime-offshore-energy-companies-89274>). 06.07.2026).*

«Перша половина 2026 року ознаменувалася серією руйнівних і дедалі зухваліших кібератак, які пронизували ниткою цифрових зривів основні світові події. Від державних суб'єктів, що націлюються на критичну інфраструктуру, до угруповань-вимагачів, які беруть у заручники великі корпорації, — ці інциденти підкреслюють ситуацію, в якій цифровий і фізичний світи небезпечно переплітаються...

Однією з найбільш тривожних подій став масштабний витік даних в Адміністрації соціального забезпечення США, який, як стверджується, був організований політично мотивованим Департаментом урядової ефективності (DOGE) і, ймовірно, поставив під загрозу особисті дані більшості живих американців. Одночасно хвиля кібератак, які здебільшого приписують Росії, була спрямована проти цивільних енергетичних та водопостачальних систем по всій Європі, що свідчить про явний намір завдати реальної шкоди. Критична інфраструктура США також стала мішенню: з'явилися попередження про те, що іранські хакери націлюються на «м'які цілі», такі як підприємства водопостачання, — про цю загрозу наочно свідчить руйнівна атака типу «wiper» на компанію Stryker, що спеціалізується на медичних технологіях.

Корпоративний світ зазнав серйозного удару як від програм-вимагачів, так і від атак на ланцюги постачання. Компанія з ринкових досліджень Klue зазнала масштабного витоку даних, що торкнувся майже 200 її клієнтів, серед яких були

гіганти сфери кібербезпеки, після того, як хакери скористалися обліковими даними, отриманими ще кілька років тому. Зробивши крок, що викликав суперечки, Klue, судячи з усього, заплатила банді вимагачів. Гігант у сфері освітніх технологій Instructure також став жертвою угруповання ShinyHunters, яке за допомогою простого голосового фішингу проникло в її системи, викрало дані понад 30 мільйонів студентів і зірвало проведення випускних іспитів після того, як компанія спочатку відмовилася платити викуп...

Під ударом опинилися й основоположні стовпи технологічної екосистеми. Серія витончених атак на проекти з відкритим кодом призвела до подальшого компрометації таких великих компаній, як OpenAI, а ФБР було змушене оголосити про «серйозний кіберінцидент» після того, як його власні системи спостереження були зламані, ймовірно, китайськими шпигунами. У результаті гучного провалу системи безпеки штучного інтелекту тисячі акаунтів в Instagram було захоплено, просто попросивши чат-бота Meta, що працює на базі штучного інтелекту, скинути паролі, що підкреслило ризики впровадження нових технологій без належних заходів безпеки. Виробник іграшок Hasbro також зазнав серйозного інциденту з безпекою, через який компанія була практично відключена від мережі протягом кількох тижнів, що продемонструвало руйнівний вплив на операційну діяльність, який може мати злом навіть без підтвердженого викрадення даних. Нарешті, серія легко уникнутих прогалин у безпеці призвела до витоку мільйонів конфіденційних документів, що посвідчують особу, виданих урядом, підриваючи ефективність систем «знай свого клієнта» та перевірки віку саме тоді, коли вони стають дедалі поширенішими». *(Zack Whittaker. Hacked, leaked, and held for ransom: The worst breaches of 2026 so far // TechCrunch Media LLC. (<https://techcrunch.com/2026/07/07/the-worst-hacks-and-breaches-of-2026-so-far/>). 07.07.2026).*

«Міністерство внутрішньої безпеки (DHS) проводить розслідування нещодавнього інциденту в сфері кібербезпеки, пов'язаного з його Мережею інформації з питань внутрішньої безпеки (HSIN) — ключовою платформою для обміну конфіденційною, але несекретною інформацією між федеральними, штатними, місцевими органами влади та партнерами з промисловості. Як повідомляється, злом, який, як вважається, стався в період з кінця травня до початку червня, був спрямований проти серверів HSIN та системи SharePoint, що, ймовірно, призвело до несанкціонованого доступу до конфіденційних даних... Хоча особистість зловмисника та масштаби витоку даних залишаються невідомими, Міністерство внутрішньої безпеки (DHS) ізолювало уражені системи та проводить криміналістичне розслідування. Речник відомства підтвердив, що інцидент стосувався несекретної застарілої системи, та зазначив, що немає жодних ознак того, що це вплинуло на секретні мережі. Цей випадок стався на тлі того, як адміністрація продовжує активізувати зусилля з посилення кібербезпеки країни у відповідь на нові загрози, зокрема ті, що пов'язані зі штучним інтелектом». *(Jane Edwards. DHS Launches Probe Into HSIN Cyber Incident // Executive Mosaic*

(<https://www.executivegov.com/articles/dhs-hsin-cyber-incident-investigation>). 07.07.2026).

«Протягом останніх двох тижнів кілька великих японських компаній, серед яких страхова компанія Aflac Japan, гігант у галузі напоїв Sapporo, промисловий виробник Nides та телекомунікаційний оператор KDDI, повідомили про серйозні кіберінциденти. Найбільший випадок порушення безпеки стався в компанії Aflac Japan, де хакери зламали клієнтський портал і оприлюднили особисті дані приблизно 4,38 мільйона страхувальників, зокрема реквізити платіжних рахунків близько 230 000 клієнтів... У ході окремих, на перший погляд, не пов'язаних між собою атак, закордонні дочірні компанії Sapporo в Сінгапурі та Канаді зазнали, ймовірно, несанкціонованого доступу, тоді як група хакерів, що використовує програмне забезпечення для вимагання викупу, взяла на себе відповідальність за злам у тайванській дочірній компанії Nides, вимагаючи викуп у розмірі 2 мільйонів доларів. Тим часом компанія KDDI повідомила, що зловмисники скористалися вразливістю стороннього програмного забезпечення, щоб отримати несанкціонований доступ до системи електронної пошти, яку вона обслуговує для п'яти японських інтернет-провайдерів, що потенційно може призвести до витоку електронних адрес та паролів клієнтів... Ці інциденти підкреслюють постійну та різноманітну ситуацію з кіберзагрозами, з якою стикаються великі корпорації в Японії». (*Daryna Antoniuk. Japanese insurer, brewer, manufacturer and telecom disclose cyber breaches // Recorded Future News* (<https://therecord.media/japan-cyber-breaches-aflac-sapporo-nides-kddi>). 01.07.2026).

«Кіберінцидент у Литві в 2026 році може спричинити серйозні наслідки, що виходять далеко за межі технічних збоїв, переростаючи у суперечки з клієнтами, розслідування з боку регуляторних органів та значні фінансові санкції відповідно до оновленого Закону Литви про кібербезпеку та рамок директиви ЄС NIS2. Незважаючи на повідомлення про 25-відсоткове зниження кількості зареєстрованих кіберінцидентів у 2025 році — які, як і раніше, переважно спричинені людською помилкою та соціальною інженерією, а не складними порушеннями — регуляторний нагляд посилився. Реєстр суб'єктів кібербезпеки Литви наразі налічує 1 443 організації з критично важливих секторів, які підпадають під дію нових суворих організаційних та технічних вимог, виконання яких контролює Національний центр кібербезпеки. Відповідно, вартість кіберінциденту тепер включає не лише безпосередні операційні простоти та потенційні позови про відповідальність перед третіми особами, а й загрозу суворих регуляторних санкцій; суб'єкти, що мають критичне значення, можуть зіткнутися зі штрафами до 10 млн євро або 2% від їхнього глобального обороту, тоді як суб'єкти, що мають важливе значення, — зі штрафами до 7 млн євро або 1,4% від обороту...» (*Cyber incidents can expose Lithuanian companies to lawsuits // infoerdve.lt* (<https://infoerdve.lt/en/cyber-incidents-can-expose-lithuanian-companies-to-lawsuits/>). 07.07.2026).

«У першій половині 2026 року вже сталася низка значних інцидентів у сфері кібербезпеки, які підкреслюють зростаючий масштаб, витонченість та різноманітність цифрових загроз... Серед найпомітніших — шахрайські схеми, спрямовані на очікування майбутнього виходу гри Grand Theft Auto VI: для викрадення інформації у шанувальників використовувалися фальшиві сайти попереднього замовлення, шахрайські мобільні додатки та підроблені платформи для завантаження, тоді як сама компанія Rockstar Games зазнала витоку даних через стороннього постачальника, відповідальність за який взяла на себе хакерська група ShinyHunters. ShinyHunters також здійснила одну з найбільших цьогорічних атак на освітній сектор, зламавши компанію Instructure — розробника системи управління навчанням Canvas, якою користуються приблизно 275 мільйонів людей по всьому світу. В результаті злому були оприлюднені особисті дані та приватні повідомлення, а друга атака, що сталася незабаром після цього, спричинила перебої в роботі навчальних закладів через пошкодження сторінок входу в систему, що призвело до перенесення іспитів та виконання завдань...

Ще один серйозний інцидент стався у компанії Conduent, що спеціалізується на управлінні даними та обслуговує медичних постачальників і державні установи: внаслідок злому було викрадено надзвичайно конфіденційну особисту, медичну та страхову інформацію щонайменше 25 мільйонів людей у штатах Техас та Орегон. Штучний інтелект також виявився новим джерелом вразливості, коли хакери скористалися чат-ботом служби підтримки Instagram від Meta, що працює на базі ШІ, переконавши його перенаправляти посилання для скидання пароля на електронні адреси, контрольовані зловмисниками, що дозволило викрасти та перепродати популярні акаунти до того, як цю вразливість було усунуто...

Безпека мобільних пристроїв опинилася під загрозою через появу шпигунського ПЗ DarkSword, яке використовувало вразливості iPhone для викрадення великого обсягу особистих даних, просто заманюючи жертв на шкідливі веб-сайти. Це шпигунське ПЗ, яке, за повідомленнями, використовували російські хакерські угруповання, продемонструвало ризики, пов'язані з атаками типу «zero-click» або «near-zero-click», і потенційно зачепило сотні мільйонів пристроїв, доки не було випущено оновлення безпеки. Нарешті, дослідники звернули увагу на зростаючу доступність кіберзлочинності завдяки WeedHack — недорогій платформі «шкідливе програмне забезпечення як послуга», замаскованій під модифікацію гри Minecraft. За невелику щомісячну плату користувачі могли отримати розширені можливості спостереження та дистанційного керування пристроями жертв. Особливе занепокоєння викликали докази того, що цей інструмент широко використовувався підлітками для домагань та кібербулінгу, що ілюструє, як кіберзлочинність стає дедалі доступнішою для недосвідчених зловмисників...

У сукупності ці інциденти свідчать про те, що кіберзагрози у 2026 році виходять далеко за межі традиційних витоків даних, охоплюючи зловживання штучним інтелектом, складне шпигунське програмне забезпечення, компрометацію ланцюгів постачання та шахрайські схеми, спрямовані на споживачів, що підкреслює необхідність посилення заходів безпеки як в організаціях, так і серед

окремих користувачів». (*Matt Binder. The 6 biggest cybersecurity breaches of 2026 so far // Ziff Davis company (<https://mashable.com/tech/biggest-cybersecurity-data-breaches-2026>). 11.07.2026*).

«Дослідники з ASSET Research Group виявили новий вид атаки на ланцюг постачання під назвою «Ghostcommit», який успішно обходить системи перевірки коду на основі штучного інтелекту та змушує агентів-кодувальників розкривати конфіденційні дані репозиторію, такі як файли .env. Оскільки сучасні системи перевірки на основі великих мовних моделей (LLM), такі як Cursor Bugbot і CodeRabbit, легко виявляють явні шкідливі інструкції у вигляді простого тексту, Ghostcommit розділяє своє корисне навантаження. Він використовує файл AGENTS.md, що виглядає нешкідливим, щоб дати агенту-програмісту вказівку вивести «константу збірки» з певного зображення у форматі PNG. Фактична шкідлива інструкція — прочитати файл .env і закодувати його у вигляді цілих чисел у форматі ASCII — прихована у вигляді тексту всередині самого зображення. Оскільки текстові системи перевірки ігнорують непрозорі бінарні блоби, такі як файли PNG, запит на злиття (pull request) об'єднується без будь-яких попереджень...

Пастка спрацьовує пізніше, коли розробник просить агента з кодування виконати рутинне завдання. Агент зчитує файл AGENTS.md, слідує вказівкам щодо образу і, як наслідок, вбудовує конфіденційні дані з файлу .env (включно з ключами API та обліковими даними хмарних сервісів) у новий код у вигляді, на перший погляд, нешкідливого кортежу цілих чисел. Це дозволяє успішно обійти звичайні сканери секретних даних, які шукають лише шаблони рядків, а не числові послідовності... Хоча тестування показало, що вразливість значною мірою залежала від конкретного набору інструментів для кодування — Cursor та Antigravity розкривали секретні дані, тоді як Claude Code відхиляв запит у всіх моделях — атака успішно використовує суттєві слабкі місця в сучасних інструментах розробки, що базуються на штучному інтелекті. У відповідь на це дослідники розробили прототип мультимодального додатка для рецензування, який успішно виявляє ці приховані варіанти каналу зображень, та опублікували свою концептуальну демонстрацію для подальшого вивчення». (*Guru Baran. New Ghostcommit Attack Hides Malicious Prompts in Images to Exploit AI Agents // Cyber Security News (<https://cybersecuritynews.com/ghostcommit-attack-hides-prompts/>). 11.07.2026*).

«Аргентинська федерація футболу (AFA) розпочала розслідування щодо несанкціонованого доступу до одного зі своїх офіційних електронних акаунтів після того, як його використали для розсилки масових листів із вимогою «справедливості» для Єгипту після скандального матчу 1/8 фіналу чемпіонату світу. Листи під назвою «СИСТЕМА ЗЛАМАНА: НЕСПРАВЕДЛИВЕ РІШЕННЯ» були надіслані журналістам після того, як Аргентина перемогла Єгипет з рахунком 3:2 у матчі, під час якого вирішальний гол єгиптян був скасований після перегляду

VAR, що викликало суперечки... У повідомленнях, підписаних «Усіма єгипетськими кібервоїнами», стверджувалося, що матч не був чесним, висувалися звинувачення, що тренер Єгипту став мішенню через свою пропалестинську позицію, а також містилися погрози щодо подальших зривів роботи мереж AFA. AFA негайно закликала одержувачів ігнорувати ці несанкціоновані електронні листи та не переходити за жодними посиланнями й не відкривати вкладення, поки її команда IT-фахівців розслідує цей випадок порушення безпеки... Хоча, згідно з повідомленнями, хакери, ймовірно, отримали доступ до частини бази даних AFA, зокрема до адрес електронної пошти та паролів, речник AFA незабаром після цього заявив, що ситуація була «вирішена», і не надав жодних додаткових подробиць щодо масштабів інциденту». (*Anna Zhadan. Hackers hijack Argentina football federation to demand "justice" for Egypt // Cybernews (https://cybernews.com/news/hackers-hijack-argentina-football-federation-fifa-world-cup/). 12.07.2026*).

«Японська компанія Nichirei Corp., що спеціалізується на харчових продуктах та логістиці холодового ланцюга, підтвердила, що кібератака, яка розпочалася 13 липня 2026 року, призвела до порушення безпеки її серверів та спричинила системні збої, що порушили роботу всієї групи компаній. У відповідь на це Nichirei створила штаб з реагування на надзвичайні ситуації та відключила свої системи з метою захисту даних клієнтів і партнерів. Це тимчасово зупинило операції з прийому та відвантаження на холодильних складах Nichirei Logistics Group, а також операції з відвантаження заморожених продуктів у компанії Nichirei Foods Inc... Хоча на деяких зламаних серверах містилася персональна інформація — що стало приводом для подання попереднього звіту до Комісії з захисту персональних даних Японії — витоку даних підтверджено не було. Спільно з зовнішнім фахівцем з кібербезпеки компанія Nichirei планує поступово відновити порушені операції 17 липня та дотримується графіка оприлюднення фінансових результатів за перший квартал 7 серпня 2026 року. Коментуючи інцидент, Філ Вайлі з Suzu Labs та Дональд Макфарлейн з Xcare, Inc. наголосили, що ця атака наочно демонструє, як кіберризики можуть легко поширюватися від одного логістичного провайдера до тисяч ресторанів, роздрібних торговців та виробників, що знаходяться нижче за ланцюгом постачання, підкреслюючи нагальну необхідність для організацій проактивно оцінювати залежність від сторонніх постачальників та зміцнювати операційну стійкість...

Водночас на вразливість критичної інфраструктури вказали повідомлення про те, що група викрадачів-вимагачів World Leaks заявила про оприлюднення в даркнеті документів, пов'язаних з індійською атомною електростанцією «Куданкулам». Серед оприлюднених файлів, як стверджується, були креслення об'єкта та інформація про постачальників, що походила від підрядника — компанії Reliance Group. «Reliance Group» підтвердила, що на сторонньому сервері, розміщеному в індійському центрі обробки даних «Yotta», стався частковий злом, хоча конкретні дані, що потрапили в руки зловмисників, не розкривалися, а «Nuclear Power Corporation of India» заявила, що жодна конфіденційна інформація

щодо ядерної безпеки не була оприлюднена... Брайан Проктор, засновник і генеральний директор компанії Frenos, зазначив, що цей інцидент свідчить про стратегічну зміну в тактиці зловмисників, які атакують операційні технології: замість спроб безпосереднього проникнення в реактор зловмисники все частіше отримують карти об'єктів, схеми вентиляції та списки постачальників, щоб вивчити фізичні процеси на станції, операційні взаємозалежності та наслідки для подальших етапів роботи. Проктор порадив, що для протидії цим новим тактикам розвідки захисники повинні впровадити методику перевірки без реальних наслідків, щоб безпечно моделювати потенційні дії зловмисників і готуватися до них». (*Anna Ribeiro. Nichirei cyberattack disrupts food and cold chain operations as Kudankulam data leak flags rising infrastructure threats // Industrial Cyber* (<https://industrialcyber.co/critical-infrastructure/nichirei-cyberattack-disrupts-food-and-cold-chain-operations-as-kudankulam-data-leak-flags-rising-infrastructure-threats/>). 17.07.2026).

«Fairlife — чиказька дочірня компанія Coca-Cola, що спеціалізується на виробництві молочних продуктів і відома своїм ультрафільтрованим молоком та протеїновими коктейлями, — тимчасово призупинила виробничу діяльність у США внаслідок кібератаки. Coca-Cola повідомила, що сторонні особи отримали несанкціонований доступ до окремих частин мережі Fairlife, що призвело до порушення безпеки бізнес-систем, пов'язаних із виробничою діяльністю компанії. Виявивши злом, компанія негайно задіяла свої плани реагування на інциденти та забезпечення безперебійної роботи, залучила зовнішніх експертів з кібербезпеки для проведення розслідування та повідомила про це правоохоронні органи... Хоча повний масштаб інциденту та його можливі фінансові наслідки поки що невідомі, компанія Coca-Cola підтвердила, що якість та безпека продукції не постраждали, а виробництво Fairlife в Канаді продовжується без змін. Наразі компанія працює над завершенням розслідування, з'ясуванням, чи не стався витік конфіденційних даних споживачів або співробітників, а також над безпечним відновленням уражених систем та виробничих ліній». (*Erin Keller. Coca-Cola pauses production of Fairlife milk and other drinks after cyber attack // The Independent* (<https://www.independent.co.uk/news/world/americas/fairlife-milk-stop-production-cyberattack-b3016943.html>). 17.07.2026).

«Національне агентство Румунії з кадастру та реєстрації землі (ANCPPI) працює над відновленням своїх послуг після серйозної кібератаки з фінансовою мотивацією, яка вивела з ладу його центральну ІТ-інфраструктуру, зокрема загальнонаціональну платформу e-Terra. Хоча атака призвела до повного зупинення роботи повністю цифрових систем реєстрації операцій з нерухомістю та іпотеки в країні, ANCPPI підтвердило, що його основні технічні та юридичні бази даних — які містять межі земельних ділянок, карти, записи про право власності та іпотеки — залишаються в безпеці та не зазнали пошкоджень. Для вирішення цієї проблеми агентство переносить свої додатки до

хмарного середовища уряду Румунії, ізолюючи уражені системи до усунення всіх вразливостей у системі безпеки...

Ця інцидента сталася в надзвичайно чутливий період, що призвело до затримки важливих операцій з купівлі житла та угод з девелоперами всього за кілька тижнів до запланованого підвищення в Румунії податку на додану вартість на нове житло з 9% до 21%. За словами Дана Чимпеана, директора Національного управління з кібербезпеки Румунії (DNSC), вторгнення було відносно простим: зловмисники скористалися відомими, не виправленими вразливостями програмного забезпечення та раніше викраденими обліковими даними, щоб викрасти вихідний код додатків та дані для входу користувачів, а не особисті дані громадян. Зловмисник, що діє під ніком «ByteToBreach» — якого влада вважає брокером початкового доступу, що базується в Алжирі, і якого компанія з кібербезпеки Kela пов'язує з кіберзлочинцем Закарією Махджубом з Орана — взяв на себе відповідальність за атаку та виставив на продаж викрадений вихідний код e-Terra та внутрішні бази даних на підпільному форумі». (*Daryna Antoniuk. Romania races to restore land registry after cyberattack disrupts property market // Recorded Future News (<https://therecord.media/romania-cyberattack-land-registry>). 20.07.2026*).

«Для боротьби з широко поширеною глобальною проблемою кіберзлочинності необхідна тісна співпраця між державним і приватним секторами — саме ця філософія лежить в основі «Партнерства проти кіберзлочинності» та «Атласу кіберзлочинності» Світового економічного форуму. «Атлас кіберзлочинності», що діє в рамках Форуму, — це ретельно відібрана спільнота експертів із компаній у сфері кібербезпеки, фінансових установ, наукових кіл та некомерційних організацій, які використовують відкриті джерела інформації для картографування злочинних мереж, виявлення інфраструктури та грошових потоків, а також розробки спільних заходів реагування. Ця модель співпраці була втілена в життя під час операції «CyberProtect III» — спільної ініціативи, координованої Інтерполом та Організацією з безпеки та співробітництва в Європі (ОБСЄ) у травні 2026 року. Ця операція була спрямована проти мереж організованої злочинності, які використовували платформи з контентом за передплатою та кодованою мовою для вербування та експлуатації жінок, неповнолітніх та вразливих дорослих. Цей метод, що полягає у видаванні себе за модельні агентства з метою контролю над акаунтами та доходами жертв, раніше був висвітлений у «фіолетовому повідомленні» Інтерполу...

Щоб подолати перешкоди, пов'язані з обміном даними та захистом приватних даних, які часто гальмують міжнародні розслідування, «Атлас кіберзлочинності» використовує розвіддані з відкритих джерел, якими можна вільно обмінюватися через національні кордони для створення вичерпних профілів злочинців. Ця здатність ґрунтується на успішному досвіді організації, яка раніше виступала оперативним партнером у рамках операцій Інтерполу «Серенгеті» та «Серенгеті 2.0» — масштабної операції у 18 африканських країнах та Великій Британії, що

призвела до понад тисячі арештів та вилучення злочинних активів на суму 140 мільйонів доларів, — а також на її співпраці в середині 2025 року з некомерційною організацією «STOP THE TRAFFIK», що бореться з торгівлею людьми. Під час операції «CyberProtect III», яка проходила у форматі спеціалізованого «хакатону» з цифрового правоохоронного забезпечення, 14 співробітників правоохоронних органів протягом чотирьох днів працювали разом із дослідниками «Atlas», щоб отримати десятки корисних зачіпок, що в результаті дозволило виявити 34 підозрілі випадки, 18 профілів підозрюваних та 27 потенційних жертв.

Ця операція також висвітлила критично важливі тенденції в сучасній злочинній діяльності, зокрема використання криптовалют для переміщення коштів, онлайн-платформ «коучингу» для розширення масштабів операцій та штучного інтелекту для створення надзвичайно переконливих фейкових профілів. Як підкреслює Дерек Манкі, головний стратег з питань безпеки та глобальний віцепрезидент з аналізу загроз у компанії Fortinet, кіберзлочинність є складною економічною системою з власними ланцюгами постачання та постачальниками послуг; для її знешкодження потрібні скоординовані дії в масштабах усієї екосистеми. Поєднуючи технічну експертизу приватного сектору з оперативними можливостями державного сектору щодо зриву діяльності злочинних мереж, «Атлас кіберзлочинності» допомагає перетворити розрізнені дані на спільну, придатну для практичного використання розвідінформацію. Як зазначає Стівен Масада, глобальний керівник підрозділу з боротьби з цифровими злочинами компанії Microsoft, такий системний підхід до захисту — детальніше описаний у нещодавно опублікованій білій книзі Форуму «Боротьба з шахрайством, що здійснюється за допомогою кібертехнологій» — створює суттєві перешкоди для злочинних мереж, прокладаючи шлях до масштабованої та адаптивної співпраці з метою захисту вразливих груп населення в Інтернеті». (*Natalia Umansky. How shared intelligence protects against and disrupts online exploitation and cybercrime // World Economic Forum (<https://www.weforum.org/stories/cybersecurity/shared-intelligence-disrupting-online-exploitation-cybercrime/>). 21.07.2026*).

Діяльність хакерів та хакерські угруповування

«Відома група хакерів-вимагачів World Leaks опублікувала в даркнеті величезний масив викрадених документів, що містить приблизно 19 000 конфіденційних файлів загальним обсягом 14,3 гігабайта, пов'язаних із найбільшим ядерним об'єктом Індії — Куданкуламською атомною електростанцією (KKNPP). Серед викрадених документів, датованих періодом з 2016 року до середини 2025 року, є нібито креслення систем вентиляції та охолодження об'єкта, план розміщення «загальної диспетчерської», протоколи нарад та інспекцій, огляди обладнання, пропозиції постачальників та страхові поліси. Хоча, як видається, ці документи не стосуються основних систем ядерних реакторів — які постачає російська компанія «Росатом» — експерти з кібербезпеки та ядерної безпеки, такі як Ніколас Рот з організації «Nuclear Threat Initiative»,

попереджають, що цей витік становить серйозну загрозу безпеці. Зловмисники можуть використати ці файли для складання карти допоміжних систем станції, виявлення постачальників та визначення критичних слабких місць у її системі безпеки...

Дані були викрадені з компанії Reliance Infrastructure — дочірньої компанії групи Reliance та одного з головних підрядників, якому доручено проектування та будівництво інфраструктури для блоків № 3 та № 4 АЕС, що наразі перебувають на стадії будівництва і мають бути введені в експлуатацію до 2027 року. Reliance Group підтвердила «частковий витік» своїх даних із сервера, розміщеного у стороннього постачальника послуг дата-центру Yotta, який 29 травня 2026 року повідомив про виявлення підозрілої активності. Хоча компанія Yotta заявила, що припинила цю активність і запобігла запуску програми-вимагача, компанія Reliance Infrastructure згодом зіткнулася з претензіями щодо витоку даних з боку World Leaks, що спричинило початок розслідування Індійською командою реагування на комп'ютерні надзвичайні ситуації (CERT-In) та налагодження зв'язку з Індійською корпорацією атомної енергетики. Організація World Leaks, яка традиційно оприлюднює викрадені корпоративні дані після ігнорування вимог про викуп — як от нещодавня вимога на суму 1,5 мільйона доларів до Tata Group — не прокоментувала цей витік...» (*Munsif Vengattil and Aditya Kalra. Files relating to India's largest nuclear power plant Kudankulam exposed in data breach // Reuters (<https://www.reuters.com/world/india/files-relating-indias-largest-nuclear-power-plant-kudankulam-exposed-data-breach-2026-07-15/>). 15.07.2026*).

«Компанія Accenture нещодавно підтвердила, що стала жертвою інциденту в сфері кібербезпеки після того, як хакер під псевдонімом «888» заявив, що в липні 2026 року викрав 35 гігабайтів внутрішніх даних компанії та виставив їх на продаж на форумі кіберзлочинців. Хакер стверджував, що серед викрадених даних містяться критично важливі компоненти програмного забезпечення та хмарних систем компанії, а саме: вихідний код, ключі RSA, ключі SSH, токени особистого доступу до Azure, ключі доступу до Azure Storage та файли конфігурації. На підтвердження цих тверджень зловмисник опублікував скріншот проєкту Azure DevOps, пов'язаного з доменом Accenture, що містив репозиторій під назвою «121123_AtriasTalentAcademy». Хоча ці докази додали вірогідності загрозі, незалежні дослідники та експерти з безпеки ще не перевірили, чи справді було викрадено всі 35 ГБ даних...

У відповідь компанія Accenture визнала, що інцидент дійсно мав місце, але запевнила громадськість, що джерело проблеми було швидко усунуто, її системи та бізнес-операції продовжують працювати в звичайному режимі, а на наданні послуг це ніяк не позначилося. Однак компанія відмовилася надати конкретні деталі щодо того, як зловмиснику вдалося проникнути в її системи, точного обсягу викрадених даних або того, чи постраждала інформація про клієнтів. Цей інцидент підкреслює постійний ризик того, що конфіденційний код та облікові дані хмарних сервісів можуть потрапити до рук кіберзлочинців, які можуть використовувати їх для виявлення вразливостей у системах. Це не перший випадок, коли Accenture стала

мішенню; у 2021 році компанія зазнала атаки програм-вимагачів LockBit, а той самий хакер під ніком «888» раніше заявляв, що отримав доступ до даних співробітників Accenture внаслідок злому сторонньої системи у 2024 році. Незважаючи на ці минулі та поточні атаки, повний масштаб інциденту, що стався в липні 2026 року, залишається непідтвердженим; компанія Accenture лише підтвердила, що локальна проблема була усунена без перебоїв у роботі». **(Akshita Pidiha. Accenture Confirms Data Breach After Hacker Claims Theft of 35GB Internal Data // Analytics Insight (<https://www.analyticsinsight.net/news/accenture-confirms-data-breach-after-hacker-claims-theft-of-35gb-internal-data>). 10.07.2026).**

«Невідомі хакери зламали онлайн-платформу дистанційного навчання Корейської національної дипломатичної академії в період з квітня 2025 року по лютий 2026 року, викравши імена, ідентифікаційні номери, адреси електронної пошти та зашифровані паролі нинішніх і колишніх співробітників Міністерства закордонних справ Південної Кореї (МЗС). Отримавши повідомлення про нестандартний доступ до мережі, міністерство негайно відключило платформу, яка залишається недоступною, поки слідчі працюють над встановленням повного обсягу викрадених даних. Зловмисники здійснили злом, скориставшись раніше невідомою уразливістю «нульового дня» у програмному забезпеченні сервера, що поєдналася з неправильно налаштованими параметрами безпеки. Хоча південнокорейські власті офіційно не пов'язали цю атаку з конкретним зловмисником, Національна розвідувальна служба зазначає, що на північнокорейських хакерів історично припадає приблизно 80% кібератак, спрямованих проти державних установ країни...

Оскільки академія готує діючих дипломатів, кандидатів на дипломатичні посади та високопосадовців уряду, цей витік даних викликав серйозні побоювання щодо національної безпеки. Цей інцидент є останнім у серії серйозних провалів у сфері безпеки в Південній Кореї, серед яких — масштабний витік даних у 2025 році в гіганта електронної комерції Coupang, що призвів до витоку інформації про 33,7 мільйона клієнтських облікових записів і спричинив рекордний штраф від регуляторних органів у розмірі 409 мільйонів доларів. У відповідь на цю хвилю все більш витончених цифрових загроз Південна Корея готується у вересні впровадити історичну реформу Закону про захист персональних даних. Внесений до закону поправки значно посилять вимоги щодо дотримання безпеки даних, дозволивши регуляторним органам накладати на організації-порушників штрафи у розмірі до 10% їхнього річного обороту та чітко визначивши генерального директора компанії як особу, яка несе кінцеву відповідальність за порушення у сфері захисту даних». **(Alexander Martin. Hackers were inside South Korea's diplomat training system for 9 months // Recorded Future News (<https://therecord.media/south-korea-cyberattack-foreign-ministry>). 20.07.2026).**

«Дослідники з кібербезпеки компанії Jamf виявили нове, надзвичайно приховане шкідливе ПЗ для macOS під назвою «PamStealer», яке використовує незвичайні методи для зараження комп'ютерів Mac та викрадення облікових даних користувачів. Шкідливе ПЗ поширюється у два етапи, починаючи з образу диска, замаскованого під легітимний менеджер буфера обміну для Mac «Масу». На першому етапі використовується скомпільований скрипт AppleScript, який при запуску за допомогою певної комбінації клавіш (Command-R) обходить попередження macOS про завантаження з Інтернету (com.apple.quarantine) і непомітно завантажує корисне навантаження за допомогою автономного завантажувача на базі JavaScript for Automation (JXA) та вбудованих API Objective-C, уникаючи типових, більш помітних команд оболонки...

Другий етап — це компактний інфостілер, написаний на Rust (що є нетиповим вибором мови для шкідливого ПЗ для macOS), який маскується під вбудовані компоненти macOS, такі як Finder або Software Update, і працює у прихованому режимі. Найхарактернішою особливістю PamStealer є його алгоритм перехоплення паролів. Він показує користувачам підроблене системне вікно авторизації та перевіряє введений пароль локально за допомогою інтерфейсу Pluggable Authentication Modules (PAM) macOS. Перевіряючи пароль виключно через PAM без запуску зовнішніх процесів, шкідливе ПЗ діє набагато непомітніше, ніж типові програми для викрадення даних. Після введення правильного пароля шкідливе ПЗ відображає фальшиве повідомлення про помилку, в якому стверджується, що файл пошкоджено, водночас таємно запитуючи повний доступ до диска та націлюючись на криптовалютні рахунки. Ці витончені тактики ухилення підкреслюють стрімку еволюцію шкідливого ПЗ для macOS у бік більш непомітних, вбудованих реалізацій, які легко обходять традиційні засоби виявлення загроз». *(Dan Goodin. Newly discovered PamStealer isn't your typical macOS malware // Condé Nast (https://arstechnica.com/security/2026/07/new-pamstealer-macos-malware-uses-clever-tradecraft-to-remain-stealthy/). 02.07.2026).*

«Дослідники з кібербезпеки компанії Blackpoint Cyber виявили «Avalon» — раніше не задокументовану модульну платформу шкідливого програмного забезпечення, яка об'єднує функції збору облікових даних, горизонтального переміщення, віддаленого доступу, блокування відновлення системи та запуску програм-вимагачів. Атака, що здійснюється в рамках багатоетапної фішингової кампанії з використанням підробленого юридичного документа, збереженого у вигляді ISO-образу на Proton Drive, запускає поетапну послідовність дій шкідливого програмного забезпечення, яке маніпулює системою Event Tracing for Windows з метою уникнення виявлення під час криміналістичного аналізу. «Avalon» має надзвичайно витончену підсистему обходу засобів захисту, здатну оминати основні засоби безпеки від Microsoft, CrowdStrike та SentinelOne. Після розгортання ця платформа активно збирає облікові дані з браузерів, менеджерів паролів та криптовалютних гаманців; викрадає дані на віддалений сервер; шифрує

критично важливі бізнес-файли за допомогою свого компонента-вимагача «CrownX»; а також активно знищує засоби відновлення системи, такі як тіньові копії...

Примітно, що Avalon демонструє явні ознаки розробки за допомогою штучного інтелекту, що свідчить про те, як штучний інтелект суттєво знижує бар'єр для створення шкідливого програмного забезпечення та дозволяє зловмисникам із меншими технічними навичками швидко створювати складні багатофункціональні загрози. Це відкриття відповідає тривожній тенденції до інтеграції штучного інтелекту в кібератаки. Одночасно дослідники з Sysdig повідомили про «JADEPUFFER» — перше публічно задокументоване зараження агентною програмою-вимагачем, що повністю керується великою мовною моделлю (LLM), яка адаптивно виконувала завдання в режимі реального часу з метою вимагання викупу за виробничу базу даних. Крім того, підрозділ Unit 42 компанії Palo Alto Networks виявив нове «безкодове» шкідливе ПЗ на основі ШІ, яке використовує LLM для автоматичного перекладу повідомлень Telegram у вигляді звичайного тексту, надісланих зловмисником, у виконуваних команди оболонки на комп'ютері жертви. У сукупності ці події підкреслюють, як ШІ докорінно змінює ландшафт кіберзагроз, роблячи традиційні показники рівня кваліфікації зловмисників застарілими». *(Ravie Lakshmanan. New Avalon Malware Framework Packs CrownX Ransomware Capabilities // The Hacker News (<https://thehackernews.com/2026/07/new-avalon-malware-framework-packs.html>). 03.07.2026).*

«Новий клас шкідливого програмного забезпечення успішно обходить сканери безпеки, призначені для захисту популярних помічників з кодування на основі штучного інтелекту, таких як Claude Code та OpenAI Codex. Дослідники виявили, що шкідливе програмне забезпечення, приховане всередині «навичок агентів» — додаткових пакетів, які надають агентам ШІ нові функціональні можливості, — може бути майстерно замасковане, зберігаючи при цьому свої шкідливі можливості. Оскільки ці навички працюють з тими самими правами доступу, що й сам агент ШІ, зловмисники дедалі частіше використовують їх для викрадення конфіденційних даних, таких як облікові дані браузера, ключі SSH та гаманці криптовалют. Розробивши інструмент під назвою SkillCloak, дослідники протестували понад 1 600 реальних шкідливих навичок на восьми широко використовуваних сканерах і виявили, що замасковане шкідливе програмне забезпечення проникало майже повністю непоміченим... Зловмисники досягають такого ухилення за допомогою двох основних технік: «структурного заплутування», яке переписує підозрілі команди у форми, що здаються сканерам нешкідливими, та «саморозпаковувального пакування скілів», яке приховує корисне навантаження в ігнорованих папках або зашифрованих блоках даних, відновлюючи його лише під час активного виконання скілу. Це виявляє фундаментальний недолік сучасних засобів безпеки, які покладаються на статичний аналіз, а не на оцінку поведінки скілу під час його активної роботи. Щоб протидіяти цій зростаючій реальній загрозі — прикладом якої є такі кампанії, як

ClawHavoc, що розмістили сотні заражених пакетів на публічних маркетплейсах — дослідники розробили «SkillDetonate», інструмент, який аналізує поведінку в пісочниці для відстеження доступу до файлів та мережових викликів у реальному часі. Зрештою, експерти з кібербезпеки закликають розробників ніколи не дозволяти агентам автоматично виконувати кроки налаштування без перевірки, тестувати незнайомі скіли в ізольованих середовищах та суворо обмежувати права доступу, надані інструментам кодування III». (*Tushar Subhra Dutta. Agent Skill Malware Targets Claude Code and OpenAI Codex With Scanner-Evasion Techniques // Cyber Security News (<https://cybersecuritynews.com/agent-skill-malware-targets-claude-code-and-openai-codex/>). 06.09.2026*).

«Дослідники з кібербезпеки компанії Jamf Threat Labs виявили нове складне шкідливе ПЗ для macOS, призначене для викрадення інформації, яке отримало назву «CrashStealer» і яке швидко еволюціонувало від експериментального зразка в травні до активного розповсюдження в липні. Написане на мові C++, «CrashStealer» обходить систему безпеки Apple Gatekeeper, поширюючись через підписаний та нотаріально завірений інсталятор під назвою «Werkbit Setup», розміщений на підробленому сайті програмного забезпечення, що вимагає введення певного PIN-коду. Після запуску шкідливе програмне забезпечення маскується під легітимну програму Apple «CrashReporter.app» і використовує оманливе повідомлення, щоб спонукати користувачів ввести свій пароль адміністратора macOS, який воно перевіряє локально... Отримавши правильний пароль, CrashStealer збирає надзвичайно конфіденційні дані, зокрема вміст «Ключового ланцюга», облікові дані браузерів, файли cookie, файли з каталогів користувачів, а також дані з понад 80 криптовалютних гаманців та 14 основних менеджерів паролів. Щоб зберегти прихованість, шкідливе ПЗ стискає та шифрує викрадену інформацію за допомогою алгоритму AES-256-GCM перед її передачею на віддалений сервер, а також забезпечує свою стійкість, створюючи підроблений LaunchAgent та неодноразово перепідписуючи свій корисний вантаж для зміни хешу файлу». (*Bhaswati Guha Majumder. New CrashStealer Malware Targets macOS Users, Disguises Itself as Apple's Crash Reporter to Steal Passwords and Crypto Wallets // IBTimes Co., Ltd. (<https://www.ibtimes.sg/new-crashstealer-malware-targets-macos-users-disguises-itself-apples-crash-reporter-steal-89687>). 14.07.2026*).

«Зловмисник, який діє з фінансових мотивів і, ймовірно, є російськомовним, розпочав широкомасштабну кампанію з використанням 292 підроблених репозиторіїв GitHub для розповсюдження варіанту програми-викрадача даних BoryptGrab. Ця кампанія, виявлена 26 червня компанією з кібербезпеки Arctic Wolf, маскується під легітимне програмне забезпечення — зокрема, продукти для безпеки, криптосервіси та ігрові інструменти — щоб заманити користувачів із результатів пошуку. Підроблені репозиторії перенаправляють жертв на шаблонну шкідливу цільову сторінку, яка надає

постійно змінюваний ZIP-архів, що містить легітимний, підписаний оновлювач WinGUP та троянізований файл libcurl.dll... Під час виконання програма-оновлювач завантажує DLL-файл у пам'ять, запускаючи програму для викрадення даних повністю в пам'яті, не створюючи персистентності та не застосовуючи заходів проти аналізу. Шкідливе ПЗ активно збирає конфіденційні дані — такі як паролі, файли cookie та платіжну інформацію з 19 браузерів, дані з 32 криптовалютних гаманців, а також токени з месенджерів, таких як Discord і Telegram, — після чого стискає їх і передає на командно-контрольний сервер, розташований у Росії... Варто зазначити, що цей варіант BoryptGrab має нову функцію, яка дозволяє обійти систему «App-Bound Encryption» у Chrome шляхом введення коду безпосередньо в браузер. Хоча GitHub видалив багато підроблених репозиторіїв, деякі редиректори залишаються активними, що змусило дослідників попередити користувачів про небезпеку завантаження нібито безкоштовного преміум-програмного забезпечення з неофіційних джерел». **(Bill Toulas. Nearly 300 GitHub repos pose as legit software to push malware // Bleeping Computer® LLC (<https://www.bleepingcomputer.com/news/security/nearly-300-github-repos-pose-as-legit-software-to-push-malware/>). 14.07.2026).**

Програми-вимагачі

«Атака програм-вимагачів на підприємства компанії MacKay Sugar у Північному Квінсленді на початку червня на короткий час паралізувала роботу двох цукрових заводів, але ситуація була вирішена протягом кількох днів, що дозволило уникнути катастрофічних економічних наслідків, характерних для подібних масштабних промислових кіберінцидентів — таких як атака на компанію Jaguar Land Rover, яка потребувала фінансової допомоги від уряду Великої Британії у розмірі 1,5 млрд фунтів стерлінгів. Цей випадок підкреслює стійку вразливість критичної інфраструктури Австралії: хоча організації вкладають значні кошти в корпоративну ІТ-безпеку, системи операційних технологій (ОТ), які фактично генерують дохід, часто базуються на застарілому обладнанні та застарілих конструкціях, що не були розроблені для протистояння сучасним кіберзагрозам... За словами Джейсона Пірса з компанії Claroty, ця невідповідність залишає важливі виробничі об'єкти вразливими, незважаючи на значний загальнонаціональний прогрес у підвищенні обізнаності з питань кібербезпеки в цілому. Для регіональних підприємств, таких як MacKay Sugar — яке, будучи другим за величиною виробником цукру в Австралії, також забезпечує приблизно третину електроенергії навколишнього регіону завдяки своїй теплоелектростанції — наслідки збою виходять далеко за межі самої компанії, впливаючи на місцеві підприємства, ланцюги постачання та цілі громади, які значною мірою залежать від обмежених життєво важливих послуг... Регіональні оператори стикаються з додатковими викликами через географічну розрізненість, інфраструктуру, що розвивалася протягом десятиліть, та невеликі місцеві команди, здатні реагувати на інциденти. Експерти стверджують, що для забезпечення

справжньої стійкості необхідно розширити інвестиції та планування у сфері кібербезпеки за межі традиційних ІТ-мереж і охопити весь спектр операційних середовищ, ланцюгів постачання сторонніх постачальників та стратегій забезпечення безперервності бізнесу, щоб захистити економічну та соціальну структуру, на якій ґрунтуються регіональні галузі». **(David Hollingworth. The operational challenge: What the Mackay Sugar cyber attack reveals about Australia's cyber readiness // MOMENTUMMEDIA (<https://www.cyberdaily.au/security/13858-the-operational-challenge-what-the-mackay-sugar-cyber-attack-reveals-about-australias-cyber-readiness>). 06.07.2026).**

«Один із провідних європейських оборонних підрядників — іспанська транснаціональна група «Indra Group» — наразі перебуває під значним тиском після атаки з використанням програм-вимагачів, здійсненої кіберзлочинним угрупованням «Gentlemen», яке поставило компанію в ситуацію, коли час на відлік: угруповання погрожує оприлюднити нібито викрадені дані, якщо не буде сплачено викуп. 30 червня угруповання опублікувало повідомлення про злам на своєму сайті в даркнеті, використовуючи загрозу публічного оприлюднення даних як засіб тиску на компанію, яка є важливим постачальником для НАТО та глобальних секторів критичної інфраструктури, зокрема управління повітряним рухом, супутникового зв'язку та інтелектуальних транспортних систем. Компанія Indra підтвердила інцидент, але охарактеризувала його як «інцидент у сфері кібербезпеки з мінімальними наслідками», який було швидко локалізовано в некритичному середовищі однієї з її дочірніх компаній, що дозволило продовжити безперебійну ділову діяльність, поки триває розслідування джерела зломи. З більш ніж 62 000 співробітників, річним доходом майже 5 млрд євро та діяльністю, що охоплює понад 140 країн, роль Indra як головної мішені підкреслює ризики, з якими стикаються навіть найдосконаліші організації в сучасному середовищі загроз...

Зловмисники, відомі як угруповання «Gentlemen», діють за моделлю «вимагальне програмне забезпечення як послуга» (RaaS), ділячи доходи з партнерами, які надають шкідливу інфраструктуру. За даними дослідників у сфері безпеки, група виникла в результаті навмисного відокремлення від програми-вимагача «Qilin» у середині 2025 року через суперечку щодо невикладених комісій на суму приблизно 48 000 доларів. Відтоді «Gentlemen» проявляє особливу активність, обираючи Таїланд своєю найчастішою ціллю, за яким слідує США, Франція та Бразилія. Здатність таких угруповань атакувати такі великі організації, як «Indra», підкреслює еволюційний характер загроз, пов'язаних із програмним забезпеченням для вимагання викупу, де оперативна стійкість та швидке локалізування залишаються ключовими засобами захисту проти витончених злочинних угруповань». **(Paulina Okunytė. NATO contractor Indra suffers data breach // Cybernews (<https://cybernews.com/security/indra-group-ransomware-attack-data-leak/>). 01.07.2026).**

«Згідно з аналізом компанії Aon, до четвертого кварталу 2025 року частота глобальних атак із використанням програм-вимагачів зросла на 650 відсотків порівняно з 2019 роком, що закріпило їхній статус як активної та актуальної загрози. Цей зростаючий ризик особливо помітний в Азії, де на сайтах, що публікують викрадені дані, було зазначено приблизно 660 організацій, включаючи 10 офіційно зареєстрованих атак на великі організації у В'єтнамі за останні два роки. Оскільки навіть значні інвестиції в безпеку не можуть повністю усунути порушення, спричинені людською помилкою або вразливостями сторонніх систем, надзвичайно важливо розробити чітко визначений план реагування на інциденти. Без чітких процесів прогалини в координації між IT-відділом, фінансовим відділом, юридичним відділом та виконавчим керівництвом можуть уповільнити реагування, що призведе до тривалого переривання діяльності, збільшення фінансових втрат та серйозного підризу репутації...»

Щоб допомогти організаціям покращити свою готовність, компанія Aon провела навчальні симуляції з протидії програм-вимагачам для керівників у Хошиміні 26 травня та в Ханой 28 травня. Під час навчань керівники підприємств опинилися в умовах імітованих сценаріїв атак, що дозволило висвітлити кілька ключових пріоритетів. По-перше, реагування на кібератаки — це не виключно завдання IT-відділу; хоча IT-відділ надає критично важливі технічні дані щодо масштабів впливу та термінів відновлення, вище керівництво має спільно приймати рішення з високими ризиками щодо виплати викупу, стратегій комунікації та юридичних повідомлень. По-друге, ринок кіберстрахування перетворився на зрілий, висококонкурентний сегмент, який пропонує покупцям не лише фінансове відшкодування; він забезпечує негайний доступ до критично важливих спеціалізованих ресурсів під час кризи, зокрема до експертів з кіберкриміналістики, юридичних радників та підтримки у сфері зв'язків з громадськістю. Нарешті, оскільки ландшафт загроз постійно змінюється внаслідок стрімкого впровадження штучного інтелекту, геополітичних кібератак, спрямованих на критичну інфраструктуру, та посилення міжнародних нормативних вимог щодо конфіденційності даних та штучного інтелекту, організації повинні регулярно перевіряти та оновлювати свої плани реагування, щоб зберегти стійку конкурентну перевагу». (*Thanh Van. Cyber incidents – a 'litmus test' of a company's management capability // Vietnam Investment Review (<https://vir.com.vn/cyber-incidents-a-litmus-test-of-a-companys-management-capability-156436.html>). 13.07.2026*).

«Університет Маунт-Роял (MRU) у Калгарі підтвердив кібератаку з використанням програм-вимагачів, яка призвела до викрадення та видалення даних, що належать нинішнім і колишнім студентам та співробітникам, а також спричинила збій у роботі критично важливих систем, зокрема систем реєстрації, нарахування заробітної плати, доступу до Інтернету та телефонного зв'язку. Атака, виявлена 17 червня 2026 року, полягала в несанкціонованому доступі до університетських накопичувачів: хакери викрали дані з одного сховища та видалили файли з іншого. Хоча точний характер викрадених даних не розголошується, вони можуть містити особисту інформацію залежно від того, що

там зберігалось. Університет продовжує розслідування за участю зовнішніх експертів з кібербезпеки, одночасно повідомляючи про інцидент постраждалих осіб та відповідні органи влади...

Група зловмисників «CMD Organization» — відносно нова кіберзлочинна організація, що працює за моделлю «вимагальне програмне забезпечення як послуга» (RaaS) — взяла на себе відповідальність за цю атаку, заявивши, що викрала до 10 терабайтів даних, і вимагає 1,9 мільйона доларів, щоб запобігти їх оприлюдненню. Цей інцидент підкреслює зростаючу загрозу для навчальних закладів, які є привабливими цілями через великі обсяги конфіденційних даних, що зберігаються в них, та їхню вразливість до перебоїв у роботі. MRU вжив заходів для відновлення послуг, зокрема розгорнула тимчасову мережу та запропонувала захист від крадіжки особистих даних, але ця атака підкреслює більш загальні занепокоєння щодо ризиків кібербезпеки в освітньому секторі, де подібні порушення нещодавно зачепили й інші заклади та платформи». (*Alicia Hope. Cyber Attack at Mount Royal University Disrupts Operations, Cybercrime Gang Demands \$1.9 Million Ransom // Rezonen Pte. Ltd. (<https://www.cpomagazine.com/cyber-security/cyber-attack-at-mount-royal-university-disrupts-operations-cybercrime-gang-demands-1-9-million-ransom/>). 13.07.2026*).

«Оскільки кіберзагрози, такі як програми-вимагачі, експлойти «нульового дня» та компрометація ланцюгів постачання, стають дедалі більш витонченими та неминучими, традиційна стратегія кібербезпеки, що ґрунтується виключно на превентивних засобах захисту, таких як брандмауери, вже не є достатньою. Організації повинні перенести акцент з простого запобігання проникненню зловмисників на впровадження проактивної стратегії кіберстійкості. Цей підхід надає пріоритет ранньому виявленню загроз, постійному зміцненню систем, адаптивним засобам контролю безпеки та швидкому відновленню, забезпечуючи безперебійність бізнесу та функціонування основних послуг навіть у разі прориву систем захисту... Оскільки справжня вартість кібератаки полягає не лише в самому порушенні безпеки, а й у пов'язаному з ним простої в роботі, що призводить до втрати доходів, штрафів з боку регуляторних органів та шкоди репутації, завдання забезпечення стійкості полягає у запобіганні оперативному паралічу. Однак досягти такого рівня готовності власними силами часто буває складно й дорого. Відтак організації дедалі частіше звертаються до постачальників керованих послуг безпеки (MSSP) для усунення кадрових та операційних прогалин. MSSP забезпечують необхідну структуру, розробляючи та ретельно тестуючи посібники з реагування на інциденти, а також перевіряючи стратегії відновлення даних, що відповідають критично важливим потребам бізнесу... Зрештою, кіберзрілість сьогодні визначається стратегічною здатністю організації передбачати загрози, адаптуватися до них та швидко відновлюватися після них, завдяки чому проактивна стійкість стає фундаментальною бізнес-функцією, а не лише питанням ІТ». (*Ivaan Captieux. Cyber resilience: shifting from defence to proactive security measures // IOL (<https://iol.co.za/ios/opinion/2026-07-14-cyber-resilience-shifting-from-defence-to-proactive-security-measures/>). 14.07.2026*).

«Фінансова динаміка традиційної бізнес-моделі програм-вимагачів, яка базується на шифруванні мережових даних з метою отримання прибутку, починає змінюватися, оскільки жертви все частіше відмовляються платити викуп. Ця тенденція зумовлена тим, що організації інвестують значні кошти в превентивні заходи з кібербезпеки — такі як надійне резервне копіювання даних, захист кінцевих точок та структуроване планування реагування на інциденти — що дозволяє їм самостійно відновлюватися після атак...

Правоохоронні органи, зокрема ФБР, категорично не рекомендують здійснювати виплати, оскільки вони не гарантують безпечного відновлення або видалення даних, часто залишаючи жертв із несправними засобами дешифрування або наражаючи їх на подальший шантаж. Крім того, здійснення виплат безпосередньо фінансує екосистему кіберзлочинців, даючи змогу групам, що використовують програми-вимагачі, купувати сучасні інструменти, вербувати хакерів та розширювати сферу своєї діяльності. Відмовляючись платити, організації спільно послаблюють фінансові стимули цих злочинних мереж, а цьому процесу сприяють міжнародні зусилля урядів, спрямовані на конфіскацію хакерської інфраструктури, відстеження криптовалют та затримання ключових учасників...

Незважаючи на ці перешкоди, програми-вимагачі залишаються надзвичайно витонченою загрозою, оскільки кіберзлочинці адаптуються, застосовуючи тактику «подвійного шантажу»: вони викрадають конфіденційні дані ще до їх шифрування та погрожують оприлюднити їх, якщо їхні вимоги будуть відхилені. Ця еволюція тактики підкреслює нагальну необхідність постійного вдосконалення систем безпеки. Зрештою, зменшення обсягів виплат викупу свідчить про суттєві зміни в економіці кібершантажу, і постійна співпраця між урядами, бізнесом та компаніями з кібербезпеки матиме вирішальне значення для остаточного зниження глобальної прибутковості таких атак». (*Naveen Goud. How receding Ransomware payments are reshaping the Economics of Cyber Extortion // Cybersecurity Insiders (<https://www.cybersecurity-insiders.com/how-receding-ransomware-payments-are-reshaping-the-economics-of-cyber-extortion/>). 20.07.2026*).

«Поширені очікування громадськості щодо надійного, подібного до вакцини, рішення проти програм-вимагачів не враховують фундаментальну різницю між статичними біологічними вірусами та високоадаптивними цифровими загрозами, розробленими розумними зловмисниками. Традиційне антивірусне програмне забезпечення, що базується на сигнатурах, стало застарілим через те, що кіберзлочинці використовують штучний інтелект, інструменти автоматичного генерування та поліморфні техніки, щоб миттєво змінювати зовнішній вигляд шкідливого програмного забезпечення, створюючи тисячі унікальних варіантів. Крім того, програмне забезпечення для вимагання викупу рідко є ізольованим шкідливим файлом; зазвичай це завершальний етап багатоетапного вторгнення в мережу, під час якого використовуються вразливості програмного забезпечення, викрадені облікові дані та скомпрометований доступ

сторонніх осіб, а це означає, що блокування виконуваного файлу не дасть жодного ефекту, якщо зловмисник уже має адміністративний контроль...

Постачальники рішень з безпеки також повинні знаходити баланс між захистом та зручністю використання, оскільки система, яка є настільки обмежувальною, що блокує всі невідомі дії, генеруватиме надмірну кількість помилкових спрацьовувань і серйозно порушуватиме законну ділову діяльність. Відповідно, засоби захисту еволюціонували від виявлення за сигнатурами до динамічних платформ, таких як «Виявлення та реагування на кінцевих точках» (EDR), «Розширене виявлення та реагування» (XDR), поведінкова аналітика та архітектури «нульової довіри», які активно відстежують підозрілу поведінку в мережі. Зрештою, кібербезпека не може усунути всі ризики і має розглядатися як безперервний процес управління ризиками, що вимагає багаторівневих стратегій — включаючи багатофакторну автентифікацію, регулярне управління виправленнями, безпечне резервне копіювання та швидке реагування на інциденти — для досягнення операційної стійкості, а не нереалістичного стану абсолютної непереможності». (*Naveen Goud. Why Security companies can't create an invincible Vaccine against Ransomware // Cybersecurity Insiders (<https://www.cybersecurity-insiders.com/why-security-companies-cant-create-an-invincible-vaccine-against-ransomware/>). 20.07.2026*).

«Нещодавно з'явилася група хакерів-вимагачів D1R заявила, що зламала компанію Synopsys, яка займається проектуванням від мікросхем до систем, скориставшись вразливістю веб-сайту, і, як стверджується, отримала доступ до бази даних клієнтів, що містить 40 000 записів. Кіберзлочинці погрожували оприлюднити викрадені дані, якщо не буде сплачено викуп, а також стверджували, що використали цю викрадену інформацію для проникнення в систему німецького інженерно-технологічного гіганта Bosch — одного з основних клієнтів Synopsys — з метою викрадення цінної інтелектуальної власності. Компанія Synopsys, яка постачає програмне забезпечення для автоматизації електронного проектування та схеми напівпровідників, на які покладаються інженерні команди Bosch при розробці автомобільних та промислових електронних компонентів, рішуче спростувала ці твердження. За результатами внутрішнього розслідування Synopsys заявила, що не виявила жодних доказів несанкціонованого доступу до своєї мережі чи технічних даних клієнтів, назвавши твердження хакерів цілком безпідставними та зазначивши, що група навіть не зв'язувалася з ними...

На підтвердження оцінки компанії Synopsys, знімок екрана, опублікований D1R як доказ злом, виявився інструкцією користувача, яка вже була у відкритому доступі, що підкреслює поширену тенденцію серед кіберзлочинців — оприлюднювати фальшиві дані або перебільшувати свої хакерські можливості. На запитання щодо ймовірного інциденту компанія Bosch відмовилася коментувати конкретні звинувачення, опублікувавши стандартну заяву, в якій ще раз підтвердила свою незмінну прихильність до кібербезпеки, захисту систем з урахуванням ризиків та операційної стійкості». (*Eduard Kovacs. Synopsys Finds No Evidence of Data Breach Amid Bosch Hack Claims // Wired Business Media*

«Згідно з новими даними Comparitech, у першому півріччі 2026 року кількість атак програм-вимагачів на державні установи по всьому світу зросла: було зафіксовано 187 інцидентів, що на 13% більше, ніж за попередні шість місяців, і в середньому становить приблизно одну підтверджену атаку на день. Хоча США, як і раніше, залишалися країною, на яку найчастіше націлювалися зловмисники (58 атак), кількість таких інцидентів у цій країні знизилася на 23%, тоді як активність програм-вимагачів посилилася в інших країнах, таких як Німеччина та Південна Африка. У цей період також відбулися значні зміни в ландшафті загроз: групою, що отримала назву «The Gentlemen», стала найактивнішою — вона взяла на себе відповідальність за 22 атаки, хоча раніше практично не проявляла активності в цій сфері...

Незважаючи на те, що середня сума викупу знизилася з 500 000 до 100 000 доларів, державні установи залишаються постійною та ідеальною мішенню для кіберзлочинців через значні збитки, спричинені шифруванням систем, та величезні обсяги конфіденційних даних, якими вони володіють. Зловмисники часто досягають успіху, використовуючи елементарні прогалини в системі безпеки, про що свідчить атака на латвійську державну лісогосподарську компанію, під час якої було використано вразливість у системі, яка не оновлювалася протягом двох років. Реальні наслідки виявилися серйозними: відновлення роботи німецької транспортної компанії тривало 11 тижнів, у Саффоку (штат Вірджинія) стався масштабний витік даних, а округ Мюррей підтвердив виплату викупу в розмірі 200 000 доларів, що підкреслює постійну та зростаючу загрозу для державного сектору». (*Anna Ribeiro. Government ransomware attacks rose 13% globally to 187 incidents in first half of 2026, with The Gentleman most active // Industrial Cyber* (<https://industrialcyber.co/threats-attacks/government-ransomware-attacks-rose-13-globally-to-187-incidents-in-first-half-of-2026-with-the-gentleman-most-active/>). 21.07.2026).

Програми-трояни

«Зловмисники використовують Microsoft Teams для розповсюдження нового прихованого трояна віддаленого доступу (RAT) під назвою EtherRAT, застосовуючи витончене поєднання методів соціальної інженерії та легального програмного забезпечення, щоб обійти корпоративні засоби захисту. Атака починається з фішингового листа, що містить шкідливий PDF-файл під назвою «Опитування співробітників». Після його відкриття жертва отримує несподіваний голосовий дзвінок у Teams від зловмисника, який видає себе за «системного адміністратора» із зовнішнього домену служби підтримки, що виглядає переконливо. Переконавши жертву увімкнути спільний доступ до екрана,

зловмисник під виглядом звичайної ІТ-підтримки допомагає їй встановити легальні інструменти віддаленого доступу... Отримавши доступ, зловмисник завантажує шкідливий інсталятор у форматі MSI, який використовує справжнє середовище виконання Node.js для розшифрування та запуску EtherRAT. Цей RAT, повністю створений на Node.js для забезпечення міжплатформної гнучкості, може виконувати команди, маніпулювати файлами, викрадати дані та підтримувати персистентність. Варто зазначити, що EtherRAT використовує смарт-контракти Ethereum для визначення місцезнаходження свого сервера управління, що значно ускладнює спроби його нейтралізації. Хоча спочатку цей інструмент пов'язували з операціями, що фінансуються державою, він набув широкого поширення серед різних злочинних угруповань. Оскільки ця тактика ґрунтується на маніпулюванні довірою користувачів до повсякденних інструментів співпраці та використанні легітимних програмних компонентів, які обходять стандартні перевірки безпеки, експерти радять організаціям обмежувати зовнішнє спілкування в Teams, навчати співробітників самостійно перевіряти ІТ-запити та активно відстежувати випадки несподіваної інсталяції програм для віддаленого доступу». **(Tushar Subhra Dutta. Hackers Leverage Microsoft Teams Call to Install RMM Tools and Deploy EtherRAT // Cyber Security News (<https://cybersecuritynews.com/hackers-leverage-microsoft-teams-call/>). 07.07.2026).**

Шпигунське програмне забезпечення

«Європейські законодавці вимагають поновлення розслідування щодо комерційного шпигунського програмного забезпечення після того, як стало відомо, що Стеліос Кулоглу, грецький депутат Європарламенту та колишній член комітету PEGA Європарламенту — який розслідував зловживання програмним забезпеченням «Pegasus» компанії NSO Group — сам став об'єктом стеження за допомогою цього інструменту. У звіті Citizen Lab при Університеті Торонто «з високою впевненістю» підтверджено, що iPhone Кулоглу був заражений «Pegasus» через експлойт «PWNYOURHOME» типу «zero-click» у жовтні 2022 року та повторно — у березні 2023 року... Ці випадки інфікування, зокрема, збіглися з критичними етапами роботи Комітету PEGA, зокрема з підготовкою його первинного звіту та інтенсивними дискусіями щодо його остаточних висновків... Хоча раніше жертвами «Pegasus» ставали й інші депутати Європарламенту, Кулоглу є першим відомим членом комітету PEGA, який потрапив під атаку. Незважаючи на підозрілий збіг обставин, пов'язаний із роботою Кулоглу в комітеті щодо Греції, дослідники не виявили доказів того, що Греція — яка має власний скандал, пов'язаний з іншим шпигунським програмним забезпеченням «Predator» — була винуватцем; натомість атака була пов'язана з тим самим Apple ID, який використовувався для атак на російських та білоруських опозиціонерів. У відповідь Citizen Lab та низка парламентських фракцій закликають до проведення термінових і ретельних розслідувань, вимагаючи від Європейського парламенту суттєво збільшити частоту перевірки пристроїв його

членів та повністю впровадити рекомендації комітету PEGA (Слідча комісія Європейського парламенту, яка розслідує використання шпигунського програмного забезпечення «Pegasus» та аналогічних засобів стеження) на 2023 рік щодо посилення нагляду та прозорості у сфері використання шпигунського програмного забезпечення — сфери, в якій Європа досі відстає від міжнародних ініціатив». *(David Meyer. Lawmaker Probing Pegasus Spyware Infected Using Same Malware // Information Security Media Group, Corp. (<https://www.inforisktoday.com/lawmaker-probing-pegasus-spyware-infected-using-same-malware-a-32153>). 03.07.2026).*

Фішингові атаки

«Незважаючи на широку обізнаність про те, що кількість фішингових атак зростає — про що повідомили 94 відсотки керівників у сфері ідентифікації та безпеки в ході нещодавнього опитування Secret Double Octopus — фінансові установи все ще стикаються зі значними прогалинами в системі аутентифікації персоналу. Хоча 82 відсотки опитаних керівників впевнені у своїй здатності запобігати захопленню облікових записів, лише 28 відсотків методів багатфакторної аутентифікації (MFA), що використовуються на даний момент, є насправді стійкими до фішингу. Замість надійного та уніфікованого захисту організації покладаються на розрізнену комбінацію одноразових паролів, push-повідомлень та апаратних ключів... Це робить застарілі та локальні системи особливо вразливими, оскільки рівень охоплення MFA в них становить лише 50 відсотків, тоді як у сучасних SaaS-додатках — 74 відсотки. Експерти застерігають, що навіть «потужна» MFA не є достатньою, і закликають організації впроваджувати справді безпарольні, стійкі до фішингу рівні інтеграції у всіх окремих додатках та шляхах входу, без необхідності заміни старих систем. Підкреслюючи цю нагальну увагу галузі до ризиків, пов'язаних з ідентифікацією, мадридський стартап з кібербезпеки 8Layers нещодавно залучив додатковий 1 млн євро, що збільшило загальний обсяг його фінансування на етапі pre-seed до 2,5 млн євро для прискорення комерціалізації в Європі... Запущена у травні 2026 року та підтримана такими стратегічними інвесторами, як Bankinter і CriteriaCaixa, платформа 8Layers об'єднує три ключові функції безпеки ідентифікації в єдиний інструмент. Вона поєднує управління станом безпеки ідентифікації (ISPM) для виявлення слабких місць у конфігурації, виявлення загроз ідентифікації та реагування на них (ITDR) для виявлення зламаних облікових записів до того, як зловмисники почнуть поширюватися по системі, а також автоматизовані оцінки відповідності вимогам таких нормативних рамок, як NIS2 та ISO 27001... У сукупності ці події підкреслюють кардинальний зсув у фінансовому секторі в бік всебічного захисту ідентифікаційних даних співробітників та застарілих систем від дедалі більш витончених кіберзагроз». *(Abhishek Jadhav. Financial institutions stumbling into phishing-resistant MFA gaps, report warns // Biometrics Research Group, Inc. (<https://www.biometricupdate.com/202607/financial-institutions-stumbling-into-phishing-resistant-mfa-gaps-report-warns>). 10.07.2026).*

«Нова витончена фішингова кампанія використовує легітимну функцію аутентифікації Microsoft — «Device Authorization Grant» (Device Code Flow) — для отримання несанкціонованого доступу до електронної пошти, файлів та повідомлень у чатах користувачів, навіть не вдаючись до використання підроблених веб-сайтів для входу. Ця функція спочатку була розроблена для того, щоб пристрої без клавіатури, такі як смарт-телевізори, могли входити в обліковий запис за допомогою введення користувачем одноразового коду на окремому пристрої. Під час цієї атаки жертви отримують оманливий електронний лист, наприклад, підроблене повідомлення від юридичної фірми, що містить PDF-файл, захищений паролем... Натискання на посилання в PDF-файлі веде на переконливий підроблений портал, на якому відображається одноразовий код і користувачеві пропонується його скопіювати. Потім жертву перенаправляють на справжню сторінку автентифікації Microsoft для введення цього коду. Оскільки екран входу виглядає справжнім, атака легко обходить стандартні рекомендації щодо перевірки URL-адрес і робить багатфакторну автентифікацію неефективною... Після затвердження коду зловмисник, який таємно ініціював запит, отримує токени доступу до облікового запису жертви, навіть не знаючи її пароля. Дослідники Securelist відстежили цю гнучку кампанію в різних регіонах і настійно рекомендують користувачам ніколи не затверджувати запити на вхід з пристроїв, які вони не ініціювали. Крім того, організаціям настійно рекомендується вимкнути процедуру введення коду пристрою за допомогою політик умовного доступу, якщо вона не потрібна для повсякденної роботи». *(Tushar Subhra Dutta. Microsoft Device Code Phishing Attack Steals Tokens Through Legitimate Login Page // Cyber Security News (<https://cybersecuritynews.com/microsoft-device-code-phishing-attack/>). 06.07.2026).*

«Дослідники з безпеки компанії Seqrite виявили складну фішингову кампанію, спрямовану проти російських аерокосмічних та авіаційних організацій, яку, ймовірно, організував зловмисник, відомий під псевдонімом Rare Werewolf. Ця атака, спрямована на шпигунство, починається з підробленого електронного листа, що імітує повідомлення від легітимного російського науково-дослідного інституту. Лист містить фальшивий рахунок-фактуру в архіві, захищеному паролем, що призначений для обходу автоматичних сканерів безпеки. Як тільки жертва відкриває файл, використовуючи пароль, вказаний у тексті листа, прихований скрипт відображає PDF-файл-приманку, одночасно непомітно завантажуючи та встановлюючи портативну версію легітимного інструменту віддаленого доступу AnyDesk... Щоб забезпечити непомітний і довготривалий контроль, зловмисники використовують утиліту під назвою «Tray Minimizer» для приховування AnyDesk від очей жертви, налаштовують програму на автоматичний доступ із заздалегідь встановленим паролем та автоматично надсилають облікові дані для підключення на свої сервери електронною поштою. Потім скрипт забезпечує свою стійкість, створюючи заплановане завдання, замасковане під звичайне оновлення, і ретельно видаляє всі інсталяційні файли, журнали та

«приманки», щоб унеможливити криміналістичне розслідування... Оскільки ця кампанія повністю базується на звичайному ІТ-програмному забезпеченні, а не на спеціально розробленому шкідливому програмному забезпеченні, вона легко обходить традиційні засоби захисту, що працюють на основі сигнатур. Відповідно, експерти з кібербезпеки радять організаціям у секторах, що стали мішенями, покладатися на моніторинг поведінки систем, закликаючи їх зберігати пильність щодо несподіваних рахунків-фактур з новозареєстрованих доменів, несанкціонованих запланованих завдань, аномальних встановлень програм для віддаленого доступу та підозрілого вихідного поштового трафіку». **(Tushar Subhra Dutta. AnyDesk Phishing Attack Uses Scheduled Task Persistence and Artifact Deletion to Evade Detection // Cyber Security News (<https://cybersecuritynews.com/anydesk-phishing-attack-uses-scheduled-task-persistence/amp/>). 07.07.2026).**

Операції правоохоронних органів та судові справи проти кіберзлочинців

«34-річний громадянин Вірменії Карен Серобович Вардanian, якого минулого року екстрадували з України до США, визнав себе винним у комп'ютерному шахрайстві та змові з метою вчинення шахрайства й вимагання за свою участь у серії атак із використанням програми-вимагача «Ryuk». Діючи з території України та Росії в період з листопада 2019 року по квітень 2020 року, Вардanian та його співники атакували три організації, розташовані в США, зокрема компанію з Мічигану, яка заплатила викуп у розмірі 1,2 мільйона доларів, технологічну фірму з Орегону та школу в Техасі... Широкомасштабна злочинна група, до складу якої входили громадяни України та Вірменії, незаконно отримала доступ до мереж, щоб розповсюдити вірус «Ryuk» на сотнях серверів по всьому світу, вимагаючи у своїх жертв приблизно 1 160 біткойнів (вартість яких на той час становила понад 15 мільйонів доларів). У цей період вірус «Ryuk» набув сумної слави через паралізування діяльності тисяч організацій приватного та державного секторів, зокрема американських лікарень та підприємств водопостачання. Згідно з угодою про визнання вини, Вардanian виплатить майже 1,2 мільйона доларів у якості відшкодування, йому загрожує до 15 років ув'язнення, і він визнає, що після відбуття покарання його буде депортовано зі США». **(Matt Kapko. Armenian national pleads guilty to Ryuk ransomware attacks // cyberscoop (<https://cyberscoop.com/karen-vardanyan-armenian-ryuk-ransomware-guilty/>). 10.07.2026).**

«Двоє молодих хакерів, Оуен Флауерс (18) і Талха Джубайр (20), були засуджені до п'яти років і шести місяців ув'язнення після того, як визнали свою провину у скоєнні руйнівної кібератаки 2024 року на компанію

«Транспорт для Лондона» (Transport For London, TfL). Діючи в складі сумнозвісного колективу Scattered Spider, підлітки отримали доступ до бази даних TfL у суботу ввечері, видавши себе за співробітника та обдурили працівника телефонної служби підтримки, змусивши його скинути їхній пароль. В результаті 16-годинного злом, який дует транслював у прямому ефірі, були скомпрометовані особисті дані до 10 мільйонів клієнтів, всі 27 000 співробітників TfL були змушені особисто змінити свої паролі, а 148 критично важливих технічних систем вийшли з ладу, що призвело до перебоїв у роботі таких важливих сервісів, як «Dial-a-ride». Фінансові збитки TfL виявилися колосальними: 29 мільйонів фунтів стерлінгів прямих збитків та додаткові 10 мільйонів фунтів стерлінгів втраченого прибутку...

Незважаючи на їхній молодий вік та діагноз аутизму, які в суді розглядалися як пом'якшувальні обставини, обидва чоловіки мали тривалий досвід вчинення тяжких кіберзлочинів. Джубайр, відома постать в англomовному кіберзлочинному співтоваристві «The Com», мав 22 попередні судимості, раніше брав участь у хакерських атаках у складі групи Lapsus\$ і досі перебуває в розшуку в США за кіберзлочини, спрямовані проти 47 жертв, які принесли 115 мільйонів доларів викупу. Флауерса заарештували у вересні 2024 року під час операції, коли його спіймали на хакерських атаках проти двох американських медичних закладів, а також на тому, що він жартував про можливі летальні наслідки для пацієнтів, які перебували на штучному життєзабезпеченні. Хоча поліція вилучила у цієї пари криптовалюту на суму приблизно 1 мільйон фунтів стерлінгів, слідчі зазначили, що їхньою основною мотивацією була популярність в Інтернеті, а не фінансова вигода. Підкреслюючи постійну загрозу, яку вони становлять, обох чоловіків було викрито на володінні контрабандними мобільними телефонами під час очікування суду у в'язниці, які вони використовували для планування майбутніх кібератак. Ця справа спонукала Національне агентство з боротьби зі злочинністю попередити, що місцеві молоді хакери становлять одну з найсерйозніших загроз національній безпеці Великої Британії, тоді як аналітики закликають політиків розглядати цю проблему як вкрай токсичну та деструктивну культуру молодіжних онлайн-банд, яку не вдасться легко стримати простими арештами». (*Joe Tidy. Teen hackers who live streamed cyber-attack on TfL jailed // BBC (https://www.bbc.com/news/articles/c4gyg0y6yg2o). 16.07.2026).*

Технічні аспекти кібербезпеки

Виявлені вразливості технічних засобів та програмного забезпечення

«Менш ніж через 24 години після публічного розкриття інформації та випуску засобу виявлення компанією watchTower Labs нова вразливість класу CitrixBleed (CVE-2026-8451) у пристроях Citrix NetScaler стала об'єктом

активної експлуатації. Оператор інфраструктури-приманки Lurovis виявив скоординовану кампанію з IP-адреси, розташованої в Німеччині, в рамках якої методично сканувалися три окремі розгортання датчиків, а цілі перевірялися перед доставкою експлойтерного коду... Уразливість, пов'язана з розкриттям даних пам'яті без аутентифікації, міститься у власному XML-парсері NetScaler для постачальників ідентифікації SAML і дозволяє зловмисникам ініціювати читання за межами дозволеного діапазону, що призводить до витoku конфіденційного вмісту сусідніх ділянок пам'яті, таких як токени сеансів, безпосередньо у файл cookie. Тривожним є те, що ця уразливість вже активно експлуатується в реальних умовах ще до того, як її було внесено до каталогу відомих експлуатованих уразливостей (KEV) CISA... Ця затримка залишає організації, які суворо покладаються на визначення пріоритетності виправлень на основі KEV, вкрай вразливими, що нагадує небезпечні сценарії попередніх інцидентів CitrixBleed у 2023 та 2025 роках, коли зловмисники здійснювали масові атаки за кілька тижнів до офіційного оприлюднення урядом списків вразливостей. Централізована мультисенсорна телеметрія Lurovis виявила, що зловмисники активно перевіряють відповіді серверів перед запуском своїх шкідливих програм, що підкреслює критичну та нагальну необхідність для організацій негайно встановлювати виправлення, а не чекати на попередження від регуляторних органів». (*Guru Baran. CitrixBleed Vulnerability Exploited by Hackers Within 24 Hours of Public Disclosure // Cyber Security News (<https://cybersecuritynews.com/citrixbleed-vulnerability-exploited/>). 02.07.2026*).

«Дослідники з безпеки компанії runZero виявили сім нових вразливостей (CVE) у FatFs — широко розповсюдженому полегшеному драйвері файлової системи FAT/exFAT, який лежить в основі незліченної кількості вбудованих систем та екосистем Інтернету речей (IoT), зокрема промислових контролерів, дронів, банкоматів та криптогаманців. Ці уразливості, рівень ризику яких за шкалою CVSS варіюється від середнього до високого, включають переповнення цілих чисел, необмежену довжину полів, помилки ділення на нуль та примитиви пошкодження пам'яті, які можуть бути спровоковані вставкою спеціально сформованих образів FAT, exFAT або GPT через USB або SD-картки. Оскільки багато з цих вбудованих пристроїв не мають сучасних засобів захисту пам'яті, таких як ASLR, фізичний доступ через знімні носії може легко призвести до повного компрометації системи або відмови в обслуговуванні, особливо під час оновлень через бездротовий канал (OTA)...

Цікаво, що компанія runZero виявила ці вразливості не за допомогою традиційного фузінгу — який не зміг виявити серйозних помилок під час аудиту 2017 року — а завдяки використанню GitHub Copilot та Visual Studio Code, що підкреслює зростаючу ефективність досліджень вразливостей із залученням штучного інтелекту в складних ланцюгах постачання. Незважаючи на численні спроби, runZero та JPCERT/CC не отримали жодної відповіді від розробника FatFs... Отже, оскільки більшість розробників використовують суттєво модифіковані, «вендорні» версії коду FatFs, кінцевим розробникам настійно

рекомендується вручну перевірити свої кодові бази, переглянути обробку буферів та імен файлів, а також підготувати необхідні виправлення для забезпечення безпеки своїх пристроїв». (*Guru Baran. Multiple FatFs Vulnerabilities Expose Millions of Embedded Devices to Cyber Risks // Cyber Security News (<https://cybersecuritynews.com/fatfs-vulnerabilities/>). 04.07.2026*).

«Дослідники з компанії Binarly, що спеціалізується на безпеці прошивок, виявили шість нових вразливостей у U-Boot — широко розповсюдженому та компактному завантажувачі, який використовується для запуску апаратного забезпечення в домашніх маршрутизаторах, «розумних» камерах, промислових контролерах та мікросхемах управління серверами. Ці уразливості, які існували в коді з 2013 року та зачіпають понад 50 стабільних версій, спрацьовують, коли U-Boot зчитує пошкоджений, ненадійний пакет у форматі Flattened Image Tree (FIT) ще до перевірки його цифрового підпису. Оскільки завантажувач працює до завантаження операційної системи, ці уразливості можуть повністю підірвати ланцюг довіри пристрою...

Хоча чотири з цих помилок призводять до збою пристрою та відмови завантажуватися (що вимагає фізичного доступу для усунення), дві найкритичніші вразливості (BRLY-2026-037 та BRLY-2026-038) пов'язані з неперевіреними значеннями, що призводять до пошкодження пам'яті та переповнення буфера стека. Це дозволяє зловмиснику, якому вдалося підмінити шкідливий образ у шляху завантаження — або шляхом фізичного доступу, або шляхом перехоплення процесів віддаленого оновлення — виконати власний код під прикриттям операційної системи, що робить стандартні засоби безпеки неефективними... Хоча ідентифікатори CVE ще не присвоєно і немає доказів того, що ці уразливості експлуатуються в реальних умовах, ризик є серйозним. Оскільки наступний офіційний випуск U-Boot із виправленнями заплановано лише на жовтень 2026 року, компанія Binarly настійно закликає виробників обладнання негайно вручну застосувати виправлення з вихідного коду для захисту свого вбудованого програмного забезпечення, а кінцеві користувачі повинні пильно стежити за цими критичними оновленнями вбудованого програмного забезпечення та встановлювати їх, щойно вони стануть доступними». (*Swati Khandelwal. Six New U-Boot Flaws Could Let Malicious Images Crash Devices or Run Code at Boot // The Hacker News (<https://thehackernews.com/2026/07/six-new-u-boot-flaws-could-let.html>). 10.07.2026*).

«Останній випуск оновлень Microsoft у рамках «Patch Tuesday» став найбільшим за всю історію: він містить виправлення для 622 уразливостей (CVE), що більш ніж утричі перевищує обсяг червневого випуску. Серед них дві уразливості типу «нульового дня», пов'язані з підвищенням привілеїв, які наразі активно експлуатуються в мережі та вимагають негайної уваги, незважаючи на відсутність «критичних» оцінок за шкалою CVSS. Перша, CVE-2026-56164, впливає на локальний сервер SharePoint і дозволяє неавтентифікованому

віддаленому зловмиснику підвищити свої привілеї. Ця вразливість, виявлена командами Mandiant та FLARE від Google під час активних атак, потребує особливо термінового виправлення, оскільки термін розширеної підтримки для SharePoint Server 2016 та 2019 добігає кінця. Друга уразливість, CVE-2026-56155, впливає на служби федерації Active Directory (AD FS); виявлена командою DART компанії Microsoft, вона дозволяє зловмиснику, що пройшов локальну автентифікацію, підвищити свої привілеї в критично важливій системі, яка керує токенами входу...

Крім того, оприлюднена, але ще не використана у зловмисних цілях уразливість, що дозволяє обійти захист BitLocker (CVE-2026-50661), вимагає встановлення виправлення, а важливе виправлення (CVE-2026-55040) усуває уразливість, що дозволяє обійти аутентифікацію JWT у SharePoint, яка порушує ланцюжок віддаленого виконання коду; повне виправлення цієї проблеми заплановано на серпень. Крім того, це оновлення завершує процес зміцнення безпеки протоколу Kerberos RC4 від Microsoft шляхом видалення перемикача відкоту, що означає: адміністратори повинні перевірити та змінити паролі для облікових записів служб, що використовують RC4, перед встановленням виправлення, щоб запобігти помилкам автентифікації...

Цей рекордний обсяг оновлень — що значною мірою зумовлений новою технологією Microsoft зі сканування вразливостей за допомогою штучного інтелекту — свідчить про кардинальні зміни в управлінні виправленнями. Оскільки зловмисники можуть використовувати автоматизацію для швидкого реверс-інжинірингу виправлень і створення експлойтів, а також з огляду на те, що оцінки CVSS дедалі частіше виявляються недостатніми для визначення пріоритетності сотень помилок високого рівня серйозності, організації повинні терміново сортувати свої черги на встановлення виправлень на основі доказів активного використання в зловмисних цілях, а не покладатися на традиційні рейтинги серйозності або чекати на офіційні списки CISA KEV». *(Swati Khandelwal. Microsoft Patches Record 622 Flaws, Including Two Zero-Days Under Active Attack // The Hacker News (<https://thehackernews.com/2026/07/microsoft-patches-record-622-flaws.html>). 14.07.2026).*

«Уразливість у розширенні для браузера «Claude for Chrome» від компанії Anthropic дозволяє зловмисним розширенням імітувати кліки користувача та запускати заздалегідь визначені дії штучного інтелекту, що потенційно може призвести до зловживання доступом Claude до підключених сервісів, таких як Gmail, Google Docs, Календар та Salesforce. Ця вразливість, виявлена Аксом Шармою з Manifold Security, існує через те, що розширення Claude не перевіряє, чи походять події кліків від реального користувача; воно не перевіряє властивість Event.isTrusted браузера, яка відрізняє справжні фізичні взаємодії від подій, згенерованих JavaScript... Отже, якщо користувача обманом змусять встановити шкідливий розширення з правами доступу до «claude.ai», це розширення зможе вставляти елементи на сторінку та генерувати штучні кліки для виконання будь-якого з дев'яти вбудованих робочих процесів Claude. Хоча це не дає можливості

довільного введення команд, це може дозволити зловмиснику маніпулювати підключеними обліковими записами, особливо якщо користувач увімкнув налаштування Claude «Діяти без запиту»... Дослідники також виявили другорядну уразливість, яку неможливо використати, пов'язану з параметром, що дозволяє обійти обмеження доступу. Про обидві уразливості було повідомлено в рамках програми винагород за виявлення помилок компанії Anthropic, проте компанія Manifold Security підтверджує, що вони залишаються не виправленими та можуть бути використані в останній версії розширення (v1.0.80), випущеній 7 липня».

(Lawrence Abrams. Claude Chrome extension flaw lets malicious extensions trigger AI actions // Bleeping Computer® LLC
(<https://www.bleepingcomputer.com/news/security/claude-chrome-extension-flaw-lets-malicious-extensions-trigger-ai-actions/>). 16.07.2026).

«...Технологія оновлення Over-the-Air (OTA), яка дозволяє виробникам бездротово доставляти оновлення програмного забезпечення або вбудованого ПЗ, усунути вразливості та виправити помилки без ручного втручання, стала предметом особливої занепокоєності в сфері кібербезпеки. Дослідження, присвячене підключеним до мережі транспортним засобам, виявило, що до системи управління акумулятором та джерела живлення автобусів, вироблених китайською компанією Yutong, можна отримати доступ через мобільні мережі за допомогою SIM-картки, що теоретично дає змогу виробнику або зловмиснику дистанційно зупинити або вивести з ладу транспортні засоби. Це відкриття, на яке звернуло увагу агентство Reuters у ході свого розслідування, спричинило негайну реакцію регуляторних органів у Данії та Великій Британії, де Міністерство транспорту Великої Британії наразі розслідує цю справу спільно з Національним центром кібербезпеки...

Експерти застерігають, що ця загроза безпеці не є характерною виключно для компанії Yutong чи автомобільної галузі, оскільки технологія OTA стрімко поширюється на інші життєво важливі галузі, такі як морський транспорт, залізничний транспорт, авіація — зокрема дрони — промислове обладнання та робототехніка. Оскільки ці системи непомітно функціонують у фоновому режимі критичної інфраструктури, міжнародні фахівці з питань безпеки наголошують, що зацікавлені сторони, установи та уряди повинні активно брати на себе відповідальність і нести відповідальність за те, як технологія OTA безпечно впроваджується у повсякденне життя».

(Cybersecurity experts warn of the risks of over-the-air (OTA) updates in vehicles // Maaal Company
(<https://maaal.com/en/news/details/cybersecurity-experts-war/>). 19.07.2026).

«Незважаючи на ретельне відстеження вразливостей, опитування Vicarius, в якому взяли участь 300 керівників ІТ-підрозділів, показало, що 79% організацій зазнали зломів через відомі вразливості, які вже були зафіксовані в їхньому реєстрі, що свідчить про те, що основною проблемою є не виявлення, а недосконалий процес усунення вразливостей. Дослідження

підкреслює, що основною причиною невдач є організаційні бар'єри, а не брак інструментів; 82% організацій не можуть усунути вразливість без передачі справи іншій команді, причому відповідальність за це часто залишається нечітко визначеною, а 58% усіх заходів з усунення вразливостей все ще вимагають ручного втручання. Важливо, що саме те, як команда визначає, що робота «виконана», є найкращим показником ймовірності злом... У організацій, які вимагали підтвердженого повторного сканування для підтвердження виправлення, рівень порушень через відомі вразливості становив 65,8%, тоді як у тих, що застосовували менш суворі критерії (наприклад, закритий квиток або розгорнутий патч), цей показник зріс до 89–93%. Невелика, але успішна меншість компаній, які повністю відмовилися від ручного усунення вразливостей, дотримувалися одного й того самого триетапного підходу: вони об'єднали свій робочий процес на єдиній платформі — від виявлення до закриття; надали командам першої лінії повноваження усувати проблеми без необхідності ескалації для затвердження; і, що найважливіше, чітко визначили усунення вразливостей як перевірене повторне сканування... Це доводить, що усунення вразливостей залежить від перегляду системи управління та робочих процесів, щоб гарантувати, що вразливість дійсно усунена, а не лише задокументована». (*Holger Schulze. Vulnerability Remediation Gap: 79% Breached by Known Weaknesses // Cybersecurity Insiders* (<https://www.cybersecurity-insiders.com/vulnerability-remediation-gap-breached-known-weaknesses/>). 20.07.2026).

Технічні та програмні рішення для протидії кібернетичним загрозам

«...Компанія Sophos представила Sophos Fusion — платформу кіберзахисту, в основі якої лежить штучний інтелект, призначену для об'єднання функцій виявлення, запобігання та реагування на загрози в усіх корпоративних середовищах, що свідчить про значний зсув у галузі від ізольованих засобів безпеки до інтегрованих екосистем, що використовують штучний інтелект. Традиційно підприємства покладалися на розрізнені інструменти для захисту кінцевих точок, брандмауерів, хмарних середовищ та електронної пошти, що створювало вразливі прогалини, якими сучасні кіберзлочинці, озброєні штучним інтелектом, легко користуються. Fusion вирішує цю проблему, безперебійно об'єднуючи всі компоненти безпеки — включаючи програмне забезпечення сторонніх розробників — за допомогою машинного навчання, автоматизації та аналітики в режимі реального часу від Sophos X-Ops. Це означає, що загроза, виявлена в одній області, миттєво посилює захист у всій мережі... Важливо, що платформа не замінює людських аналітиків, а використовує штучний інтелект для виконання рутинних завдань, таких як виявлення аномалій та визначення пріоритетності сповіщень, тим самим мінімізуючи «втому від сповіщень» і дозволяючи експертам зосередитися на складних розслідуваннях з

високим рівнем ризику та прийнятті критично важливих рішень. Оскільки кіберзлочинці дедалі частіше використовують генеративний штучний інтелект для автоматизації фішингу, створення шкідливого програмного забезпечення та експлуатації вразливостей з безпрецедентною швидкістю, проактивні інтелектуальні платформи, такі як Sophos Fusion, є необхідним кроком у розвитку кібербезпеки, перетворюючи засоби захисту на адаптивні, взаємопов'язані екосистеми, оптимізовані для робочих процесів, що поєднують людський інтелект та штучний інтелект». (**Soham Halder. Sophos Fusion Explained: The AI-Native Cybersecurity System Every Business Should Know // Analytics Insight** (<https://www.analyticsinsight.net/news/sophos-fusion-explained-the-ai-native-cybersecurity-system-every-business-should-know>). 16.07.2026).

Основи кібергігієни

«Нещодавнє дослідження з питань кібербезпеки, проведене консалтинговою компанією Gallagher, виявило тривожні звички британських співробітників щодо паролів: кожен п'ятий зізнався, що записує або передає свої паролі на зовнішніх нотатках. Така практика, а також той факт, що майже половина співробітників використовує один і той самий пароль як для особистих, так і для робочих облікових записів, створює значні вразливості в системі безпеки підприємств. Дослідження також показало, що 26% співробітників для зручності переносять корпоративні дані на особисті пристрої, що ще більше збільшує ризик витоку даних... Ці недоліки в практиці кібербезпеки мають значні фінансові наслідки: за оцінками, у 2025 році британські підприємства витратили понад 278 мільйонів фунтів стерлінгів на оплату робочого часу співробітників та супутні витрати, пов'язані з реагуванням на кіберінциденти. У звіті наголошується на нагальній необхідності для організацій формувати більш міцну культуру безпеки шляхом навчання співробітників найкращим практикам, таким як використання менеджерів паролів, увімкнення багатофакторної автентифікації та зберігання корпоративних даних на захищених пристроях, що перебувають під управлінням компанії». (**Naveen Goud. What.....one in five UK Employees admit sharing Passwords on External Note // Cybersecurity Insiders** (<https://www.cybersecurity-insiders.com/what-one-in-five-uk-employees-admit-sharing-passwords-on-external-note/>). 03.07.2026).
