

**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

№ 5 (травень)

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. № 5 (травень). 194 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

Міжнародне співробітництво у галузі кібербезпеки	4
Світові тенденції в галузі кібербезпеки	4
Сполучені Штати Америки	31
Країни ЄС та Великобританія	40
Австралія та Нова Зеландія	61
Китай, Індія, Японія, Південна Корея та країни Індостанського регіону	63
Ізраїль, Туреччина та країни Близького сходу	66
Країни Африки	68
Кіберстрахування	70
Кібервійни та протидія зовнішній кібернетичній агресії	74
Кіберзахист критичної інфраструктури	82
Кіберзахист закладів охорони здоров'я	92
Захист персональних даних та соціальні мережі	95
Масштабні витoki персональних даних	98
Кібербезпека Інтернету речей. Штучний інтелект	100
Штучний інтелект, як інструмент боротьби із кіберзлочинністю	123
Штучний інтелект, як зброя кіберзлочинців	127
Кіберзлочинність та кібертероризм	132
Діяльність хакерів та хакерські угруповування	156
Вірусне та інше шкідливе програмне забезпечення	160
Фішингові атаки	172
Операції правоохоронних органів та судові справи проти кіберзлочинців	175
Технічні аспекти кібербезпеки	179
Виявлені вразливості технічних засобів та програмного забезпечення	180
Технічні та програмні рішення для протидії кібернетичним загрозам	190
Основи кібергігієни	192

«Оприлюднено звіт «Формування міцного кіберальянсу між США та Південною Кореєю: спільна стратегія кіберстійкості», у якому викладено, як Сполучені Штати та Південна Корея можуть поглибити співпрацю для протидії дедалі більш витонченим кіберзагрозам з боку таких суб'єктів, як Північна Корея, Китай та Росія... Вважаючи, що традиційні оборонні моделі вже не є достатніми для забезпечення стримування чи стійкості, у звіті пропонується більш інтегрована система, зосереджена на спільній оцінці обстановки та вдосконалених можливостях визначення джерела атак. Ця стратегія виступає за рішучий перехід до проактивних та активних заходів кіберзахисту та запроваджує стандартизовану систему класифікації серйозності кібератак (CSCF) для оптимізації та уточнення процесу прийняття рішень під час криз. Зрештою, у звіті наголошується, що для ефективності альянсу кіберполітика має бути тісно узгоджена з більш широкими дипломатичними, фінансовими та правоохоронними інструментами. Ця спільна дослідницька робота стала можливою завдяки підтримці CSIS (Центр стратегічних та міжнародних досліджень) та Південнокорейського інституту досліджень у сфері національної безпеки». (*Building a Robust U.S.-ROK Cyber Alliance // Center for Strategic & International Studies* (<https://www.csis.org/analysis/building-robust-us-rok-cyber-alliance>). 07.05.2026).

Світові тенденції в галузі кібербезпеки

«Нове дослідження компанії Orange Cyberdefense свідчить, що внутрішні загрози випередили зовнішні атаки як головний ризик для кібербезпеки організацій, збільшившись з 47% до 57% випадків за менш ніж рік. У той час як зовнішня хакерська активність залишилася відносно стабільною на рівні 31%, кількість випадків зловживання з боку співробітників зросла з 29% до 45%, що стало першим випадком, коли ризики, пов'язані з інсайдерами, перевищили зовнішні загрози. У звіті підкреслюється зростаюча роль тіньових ІТ-систем, оскільки співробітники все частіше використовують несанкціоновані інструменти — часто включаючи загальнодоступні програми штучного інтелекту — іноді наражаючи на небезпеку конфіденційні дані компанії. Водночас зловмисники все частіше націлюються на інсайдерів і використовують повсякденну поведінку на робочому місці як точки входу, перетворюючи обходи політик на вразливості безпеки...

Кінцеві пристрої залишаються головним слабким місцем: пристрої співробітників фігурують у 53% інцидентів, а кількість атак, спрямованих на облікові дані, також значно зросла — з 10% до 17% за останній рік. Хоча багато дій зсередини не мають зловмисного характеру, дослідники застерігають, що вони можуть завдати такої ж шкоди, як і складні злами. Orange Cyberdefense радить організаціям усвідомити, що ризик дедалі частіше походить зсередини, і реагувати

на це шляхом посилення контролю доступу, обмеження привілеїв та впровадження таких заходів, як багатофакторна автентифікація, щоб зменшити площу атаки та запобігти несанкціонованому доступу». (*Craig Hale. Employees are now more dangerous to their company than external hackers // Future US, Inc. (<https://www.techradar.com/pro/security/employees-are-now-more-dangerous-to-their-company-than-external-hackers>). 04.05.2026*).

«Центри обробки даних стрімко стають одним із найдинамічніших і найскладніших джерел світового попиту на електроенергію — у 2024 році вони споживатимуть 1,5% світової електроенергії, а їхні обсяги зростуть на 12% — що не тільки ставить під загрозу пропускну здатність енергомереж, а й створює проблеми зі стабільністю, коли до мережі раптово підключаються або відключаються величезні навантаження. Оскільки центри обробки даних забезпечують функціонування широкого спектру важливих економічних процесів, зокрема прогнозування енергоспоживання для комунальних підприємств, їхня стійкість тісно пов'язана зі стабільністю енергетичної системи... Надійний центр обробки даних повинен бути здатний відбивати, виявляти та усувати кіберзагрози без переривання роботи сервісів, що вимагає захисту локальних систем енергопостачання та резервного живлення за допомогою надійних засобів цифрового контролю (наприклад, брандмауерів та закритих портів) та безперервного моніторингу, який об'єднує дані датчиків, виробничі показники та інформацію про події безпеки в системах електропостачання, охолодження та контролю доступу. Щоб витримати перебої в електромережі, центри обробки даних зазвичай прагнуть забезпечити щонайменше 12 годин резервного живлення та водопостачання, використовуючи кілька джерел енергії та дублююче обладнання для усунення одиничних точок відмови. Акумуляторні системи забезпечують миттєве короткочасне підкріплення потужності під час розгону генераторів, що запускаються повільніше, але розробка стратегій диспетчеризації стає складнішою, коли доводиться збалансовувати витрати, викиди та інтеграцію з такими джерелами, як сонячна, вітрова енергія або газові турбіни. Хоча центри обробки даних часто проектуються з урахуванням можливості автономного живлення на місці, вони зазвичай покладаються на енергомережу для забезпечення ефективності, але повільні темпи розбудови нової інфраструктури енергомереж у регіонах із жорстким регулюванням сприяють впровадженню локальних джерел генерації. Інтеграція декількох джерел енергії диверсифікує ризики, але вимагає всебічного контролю за кібербезпекою для управління утвореною «системою систем»... Центри обробки даних також можуть пом'якшувати наслідки локальних перебоїв у електропостачанні за рахунок географічного розподілу робочих навантажень, хоча це може створити проблеми для операторів електромереж в інших регіонах через раптові стрибки навантаження. Зрештою, стійкість центрів обробки даних та електроенергетичного сектору взаємопов'язані: оператори електромереж повинні справлятися з коливаннями навантаження, тоді як центри обробки даних покладаються на надійне та недороге електропостачання, а також на надійні системи резервного живлення. З огляду на те, що перебої в

електропостачанні та кіберінциденти можуть відбуватися одночасно, міжгалузева співпраця та вбудована стійкість мають вирішальне значення для того, щоб звести потенційні кризи до рівня інцидентів, які можна контролювати». **(Leo Simonovich, Filipe Beato. Why data centres are reshaping resilience and cybersecurity for critical infrastructure // World Economic Forum (<https://www.weforum.org/stories/2026/05/data-centre-resilience-cybersecurity-critical-infrastructure/>). 05.05.2026).**

«Багато компаній у сфері кібербезпеки здатні досягати високих технічних результатів — захищати від загроз з боку держав, розробляти архітектури «нульової довіри» та реагувати на атаки програм-вимагачів — проте залишаються практично непомітними, коли корпоративні замовники шукають їх в Інтернеті, що створює розрив у довірі в галузі, яка ґрунтується саме на довірі. З огляду на те, що, за прогнозами, у 2026 році австралійські організації витратять понад 7,5 млрд австралійських доларів на інформаційну безпеку, а багато процесів купівлі починаються з Google, у той же час постачальники послуг безпеки значною мірою ігнорують те, як формуються та оцінюються цифрова довіра й авторитет... Тут проводиться паралель між кіберстійкістю та маркетинговою стійкістю: покладатися на єдиний канал залучення потенційних клієнтів — це все одно, що мати єдину точку відмови, адже сучасні покупці проводять більшу частину своєї оцінки в Інтернеті — читають огляди незалежних джерел, перевіряють, чи посиляються авторитетні джерела на дослідження постачальника, та аналізують результати пошуку — часто задовго до того, як звернутися до відділу продажів. Пошукові системи вимірюють авторитетність за допомогою зовнішніх сигналів довіри, таких як зворотні посилання, що розглядаються як SEO-еквівалент підтвердження від третіх осіб; без цих сигналів постачальник виглядає «неперевіраним» у сенсі нульової довіри і може провалити тест на довіру ще до початку будь-якої розмови. В Австралії гострота проблеми посилюється через впровадження штучного інтелекту, поглиблення дефіциту кваліфікованих кадрів та зростаючу залежність від постачальників керованих послуг з безпеки, що робить ринок більш конкурентним саме в той час, коли прогнозується різке зростання витрат на програмне забезпечення для безпеки. Для зміцнення цифрового авторитету в тексті пропонується структурована, позбавлена хитрощів програма, зосереджена на авторитетних публікаціях, оригінальних дослідженнях, на які посиляються інші (таких як звіти про загрози та дані про місцеві інциденти), а також поширенні лідерських ідей через численні надійні платформи — по суті, це «глибока оборона» для забезпечення авторитету бренду... Керівники служб інформаційної безпеки (CISO) повинні ретельно перевіряти авторитет постачальників у цифровій сфері поряд з їхніми технічними заявами, з'ясовуючи, чи посиляються на них авторитетні незалежні джерела, чи публікують вони ґрунтовні аналітичні матеріали, чи можна знайти їхні рішення для проблем, які вони, за їхніми словами, вирішують, та чи посиляються на їхню роботу інші шановані організації. Адже постачальник, який не може продемонструвати авторитет у своїй галузі, може виявитися недостатньо

надійним партнером для захисту чужих систем». (*Dominic Vivarini. Why your cybersecurity firm's Google rankings are a security risk in disguise // TechDay (<https://securitybrief.com.au/story/why-your-cybersecurity-firm-s-google-rankings-are-a-security-risk-in-disguise>). 08.05.2026*).

«У 2026 році сфера кібербезпеки опиниться під значним тиском, оскільки організації стрімко впроваджують штучний інтелект, водночас маючи необхідність готуватися до ризиків квантової ери — і все це на тлі дефіциту кваліфікованих кадрів, зростаючого операційного навантаження та екосистеми зловмисників, яка тепер має доступ до складних технологій корпоративного рівня, подібних до тих, що використовують захисники. Це створює парадокс: ШІ збільшує швидкість і масштаб атак, але також дає можливість перепроєктувати операції з безпеки шляхом поліпшення виявлення та реагування і зменшення навантаження на аналітиків — за умови впровадження з потужним управлінням, уніфікованою видимістю та людським наглядом, а не як ще один шар ізольованих інструментів. Кіберстійкість повинна перейти від реактивної, фрагментованої безпеки до проактивного, інтегрованого запобігання, реагування та відновлення, заснованих на видимості ризиків у масштабах підприємства та «інтегрованої структури безпеки», що охоплює людей, процеси та технології...

Для керівників служб інформаційної безпеки виділено чотири стратегічні пріоритети. По-перше, дефіцит кваліфікованих кадрів у сфері кібербезпеки дедалі більше стає системною проблемою: організації повідомляють про інциденти, пов'язані з нестачею кадрів, навчання часто не відповідає потребам підприємств, а агентна штучна інтелектуальна система створює попит на нові можливості, такі як автоматизація, управління ризиками моделей та захист від ворожих штучних інтелектуальних систем; для усунення цього дефіциту потрібні швидші та гнучкіші моделі навчання, міжгалузева співпраця та використання агентної штучної інтелектуальної системи в операціях з безпеки (SecOps) для автоматизації сортування, усунення та забезпечення відповідності вимогам, зберігаючи при цьому участь людей у процесі. По-друге, управління вразливостями має еволюціонувати від періодичного сканування та встановлення виправлень до постійного зменшення ризиків за допомогою таких підходів, як безперервне управління вразливістю до загроз (STEM), що поєднує видимість активів у реальному часі, пріоритезацію ризиків на основі ШІ та скоординовані робочі процеси усунення, щоб скоротити час усунення та досягти вимірюваного зниження ризиків, що виходить за межі звітності щодо дотримання вимог. По-третє, виявлення фейкових відео стає необхідним для захисту довіри до бренду та зацікавлених сторін, оскільки голос, згенерований ШІ, та мультимодальне підроблення особистості уможлиблюють шахрайство та дезінформацію, що вимагає сучасних інструментів, більш надійних протоколів комунікації та спільної інформації про загрози, інтегрованої у робочі процеси ідентифікації та реагування на інциденти... По-четверте, безпека в епоху квантових обчислень має стати стратегічним пріоритетом, оскільки майбутні квантові обчислювальні системи можуть зламати широко використовувані криптографічні алгоритми, а

зловмисники вже застосовують стратегії на кшталт «спочатку зібрати дані, потім розшифрувати»; організаціям слід впроваджувати гнучкі плани переходу на нові криптографічні технології, проводити аналіз вразливих активів та розпочинати тестування квантостійких алгоритмів, відібраних NIST. Загалом, найкраще до 2026 року та в подальшому будуть підготовлені ті організації, які спростять архітектуру безпеки, зосередяться на постійному зниженні ризиків та готовності до них, а також інтегрують штучний інтелект із системами управління та оперативною дисципліною для збереження довіри». *(Sheetal Mehta. Four key areas in cybersecurity that need fresh thinking and actionable steps in 2026 // Future US, Inc. (<https://www.techradar.com/pro/four-key-areas-in-cybersecurity-that-need-fresh-thinking-and-actionable-steps-in-2026>). 06.05.2026).*

«Згідно з опитуванням компанії «Касперський», в якому взяли участь 2 800 співробітників та власників підприємств, майже двоє з п'яти фахівців у регіоні Близького Сходу, Туреччини та Африки (META) вважають, що правила кібербезпеки їхніх організацій є надмірними або не відповідають їхній повсякденній роботі. Ця структурна невідповідність змусила 21% респондентів протягом останнього року встановлювати програмне забезпечення на робочі пристрої без дозволу ІТ-відділу — це є чітким показником зростаючого операційного ризику «тіньової ІТ», — тоді як 7% респондентів повідомили, що у них немає правил кібербезпеки або вони про них не знають... Політика щодо використання особистих пристроїв також є неоднорідною: 19% респондентів зазначають, що в їхніх компаніях відсутні правила щодо використання некорпоративних пристроїв; 35% мають доступ до службових даних за умови використання певних засобів захисту (навіть споживчого рівня); 21% повинні пройти офіційні перевірки ІТ-безпеки; і лише 25% можуть користуватися виключно пристроями, виданими ІТ-відділом. Хоча встановлення програмного забезпечення контролюється більш суворо — 50% респондентів зазначають, що встановлювати програмне забезпечення може лише ІТ-відділ, а 31% обмежують це право керівництвом або визначеними користувачами — 8% все ще повідомляють про повну відсутність будь-яких обмежень. Компанія «Касперський» попереджає, що поширення гібридної моделі роботи, хмарних інструментів та штучного інтелекту прискорило несанкціоноване використання програмного забезпечення та пристроїв, що наражає організації на ризик атак програм-вимагачів, витоку даних та порушення нормативних вимог. Щоб усунути цю прогалину в політиці безпеки та захистити розширювані площини атаки, компанія радить організаціям перейти до стратегій, орієнтованих на користувача, які поєднують підвищення обізнаності співробітників із регулярними аудитами «тіньових ІТ», впровадженням EDR/XDR для кращої видимості та рішеннями MDM для забезпечення дотримання базових вимог безпеки на особистих пристроях». *(39% of META employees view cybersecurity rules as excessive, Kaspersky finds // Africa Business Communities (<https://africabusinesscommunities.com/tech-24/39-of-meta-employees-view-cybersecurity-rules-as-excessive-kaspersky-finds/>). 04.05.2026).*

«Компанії, що займаються управлінням об'єктами, стикаються зі зростаючим ризиком у сфері кібербезпеки, який часто виходить за межі їхнього безпосереднього контролю: це їхній ланцюг поставок. Хоча багато організацій інвестують у захист власних систем та підвищення обізнаності персоналу, постачальники, такі як підрядники з технічного обслуговування, інженери з систем опалення, вентиляції та кондиціонування, клінінгові компанії та фахівці з інженерних систем будівель, часто потребують доступу до конфіденційних систем, даних та інфраструктури на об'єктах — і цей доступ, якщо ним неправильно керувати, може створити серйозні вразливості. Кіберзлочинці все частіше цим користуються, обираючи менших, гірше захищених постачальників як точки входу до великих організацій, використовуючи зламани облікові записи для доступу до численних об'єктів або надсилання фальшивих рахунків-фактур...

До типових вразливих місць належать спільні або слабкі паролі, неперевірені або нескасовані облікові дані, а також незахищені віддалені підключення до систем управління будівлею. Для компаній, що займаються управлінням об'єктами, порушення безпеки, пов'язане з постачальниками, може мати наслідки, що виходять далеко за межі втрати даних: це може призвести до збою в роботі систем контролю доступу, опалення, вентиляції та кондиціонування повітря (HVAC), відеоспостереження та інших систем управління будівлею, що матиме значний вплив на безпеку, безперебійність надання послуг та репутацію.

Щоб мінімізувати цю зростаючу загрозу, компанії з управління об'єктами повинні активно управляти своїм ланцюгом поставок, контролюючи та обмежуючи доступ постачальників, регулярно переглядаючи дозволи та забезпечуючи дотримання базових стандартів безпеки, таких як багатофакторна автентифікація та сертифікація Cyber Essentials». *(The Hidden Cyber Risks In Your Supply Chain // Spotted Cow Media Ltd (<https://www.twinfm.com/article/the-hidden-cyber-risks-in-your-supply-chain>). 07.05.2026).*

«Дослідження страхової компанії Beazley показало, що майже третина керівників будівельних та нерухомісних компаній (32%) стурбовані питаннями кібербезпеки, причому цей сектор продемонстрував найнижчий рівень впевненості серед дев'яти галузей, що брали участь в опитуванні: лише 74% респондентів вважають, що сектор достатньо підготовлений до кіберзагроз. Примітно, що кібербезпека посіла перше місце серед проблем, що викликають найбільше занепокоєння, випередивши технологічні збої та застарілість обладнання. У звіті Beazley «2026 Spotlight on Cyber Threats and Tech Advances», підготовленому на основі опитування понад 3 500 керівників підприємств, міститься попередження про те, що кіберризик перетворився з технічної проблеми на системну загрозу, здатну вплинути на кожну ланку організації та її ланцюга поставок. Кіберзлочинці все частіше використовують штучний інтелект для автоматизації масштабних фішингових та розвідувальних кампаній, які є швидшими, більш адаптивними та важчими для виявлення, причому фішингові повідомлення, згенеровані штучним інтелектом, спонукають жертв

надати доступ до мережі, що може уможливити атаки програм-вимагачів. Слабка або відсутня багатофакторна автентифікація залишається значною вразливістю, а загрози ще більше посилюються геополітичною напруженістю, складністю регуляторних вимог та взаємопов'язаними ланцюгами постачання...» (**Greg Pitcher. Construction 'least prepared' industry for cyber threats, poll finds // EMAP Publishing Limited** (<https://www.constructionnews.co.uk/sections/data/construction-least-prepared-industry-for-cyber-threats-poll-finds-06-05-2026/>). 06.05.2026).

«Світова галузь кібербезпеки в оборонній сфері переживає період стрімкого зростання: за прогнозами, її ринкова вартість зросте з 21,3 млрд доларів у 2021 році до 43,4 млрд доларів до 2031 року, що відповідає середньорічному темпу зростання (CAGR) на рівні 7,7%. Це зростання зумовлене насамперед посиленням загрози кібератак з боку організованих злочинних угруповань на об'єкти критичної інфраструктури, а також зростаючою залежністю військових організацій від мереж, що базуються на Інтернеті. Крім того, перехід від традиційних військових засобів до автономних систем та загальне зростання витрат на ІТ у сфері оборони зробили багаторівневі протоколи безпеки необхідними для збереження цілісності та конфіденційності оборонних організацій...

Хоча розвиток ринку зумовлений технологічними вдосконаленнями та урядовими ініціативами — такими як створення у Великій Британії Національних кібервійськ та «Кіберкоридору» — він стикається зі значними перешкодами, зокрема з глобальним дефіцитом кваліфікованих фахівців з кібербезпеки та недостатньою обізнаністю в деяких секторах. Незважаючи на ці виклики, впровадження технологій Інтернету речей (IoT) та зростання кількості цілеспрямованих загроз на адресу урядовців створюють нові можливості для інновацій. Ключові гравці галузі, такі як Thales Group, Northrop Grumman та Safran SA, дедалі частіше укладають довгострокові контракти на інтеграцію передових технологій, зокрема 5G, штучного інтелекту та аналізу даних, у сучасні оборонні системи...

Останні стратегічні зміни свідчать про переорієнтацію галузі на спеціалізовані засоби захисту; наприклад, компанія BAE Systems представила систему Viper Memory Loader Verifier II для захисту винищувачів F-16, а Raytheon уклала партнерську угоду з CrowdStrike з метою вдосконалення послуг з керованого виявлення та реагування. Щодо структури ринку, у 2021 році домінуючими сегментами були захист кінцевих точок та локальне розгортання, при цьому управління ідентифікацією та доступом залишалося ключовою сферою рішень. У географічному розрізі Північна Америка продовжує лідирувати за обсягом доходів завдяки значним інвестиціям у послуги з безпеки. Однак очікується, що до 2031 року найдинамічнішим ринком стане Азіатсько-Тихоокеанський регіон, що зумовлено модернізацією внутрішніх сил безпеки та збільшенням бюджетних видатків на протидію регіональній терористичній діяльності та кіберзагрозам». (**Defense Cyber Security Industry to Reach \$43.4 Billion by 2031 : Sustained Growth**

with a 7.7% CAGR // openPR (<https://www.openpr.com/news/4501499/defense-cyber-security-industry-to-reach-43-4-billion-by-2031>). 05.05.2026).

«...Ескалація глобальної геополітичної напруженості, зокрема конфлікту між США та Іраном, кардинально змінила ринок військової кібербезпеки, перетворивши цифрову оборону з допоміжної функції на пріоритет першої лінії. У міру зростання кількості атак з боку національних держав на супутниковий зв'язок, критичну інфраструктуру та системи управління, обсяг ринку, який у 2024 році становитиме 18,6 млрд доларів, за прогнозами, до 2033 року досягне 50,2 млрд доларів, що відповідає середньорічному темпу зростання (CAGR) на рівні 11,7%. Цей ріст характеризується стратегічним переходом до проактивної оборони, в рамках якої уряди перерозподіляють бюджети для впровадження архітектур «нульової довіри», квантово-стійкого шифрування та аналітики загроз у реальному часі...

Ключовим елементом цієї технологічної революції є інтеграція штучного інтелекту та машинного навчання, що забезпечує автономне виявлення загроз та прогнозний аналіз. Аналізуючи величезні обсяги даних у режимі реального часу, системи на базі штучного інтелекту можуть виявляти та нейтралізувати нові загрози без втручання людини, що є надзвичайно важливим для підтримання оперативної готовності у дедалі складніших умовах. Хоча мережева безпека залишається домінуючим сегментом ринку через критичну важливість захисту комунікацій, спостерігається прискорений перехід до хмарних та гібридних моделей розгортання з метою підвищення масштабованості та гнучкості оборонних операцій...

З географічної точки зору Північна Америка продовжує лідирувати на ринку завдяки значним оборонним видаткам США та добре розвиненій промисловій базі, хоча регіони Азіатсько-Тихоокеанського басейну та Близького Сходу поступово стають важливими зонами з високими темпами зростання. Ця динамічна ситуація сприяла інтенсивній консолідації ринку, в рамках якої такі великі гравці, як Lockheed Martin, Raytheon та Northrop Grumman, використовують злиття та поглинання для завоювання нішевих позицій у сферах штучного інтелекту, хмарної безпеки та шифрування. Зрештою, ситуація у сфері військової кібербезпеки формується під впливом поєднання швидких технологічних інновацій, зростання оборонних бюджетів та еволюції регуляторної політики, що надає пріоритет національній безпеці та стратегічній перевазі...» **(Military Cyber Security Market Size Accelerating at 11.7% CAGR | By Key Players: Lockheed Martin, Raytheon Technologies, Northrop Grumman, BAE Systems, Thales Group, Booz Allen Hamilton // openPR (<https://www.openpr.com/news/4509213/military-cyber-security-market-size-accelerating-at-11-7-cagr>). 11.05.2026).**

«На тлі підвищеної волатильності ринку, спричиненої геополітичною невизначеністю, такою як мирна угода між Вашингтоном і Тегераном, сектор кібербезпеки став стійкою та стратегічно важливою інвестиційною сферою.

Цьому зростанню сприяють два основні чинники: стрімкий бум у галузі штучного інтелекту та зміна характеру сучасної війни. Оскільки, за прогнозами, капітальні витрати великих технологічних компаній на інфраструктуру ШІ до 2027 року перевищать 1 трильйон доларів, попит на цифровий захист зростає паралельно з цим. Інтеграція передових моделей ШІ, які іноді можуть перевершувати людські можливості у хакерських завданнях, створює нові вразливості, що робить надійну кібербезпеку необхідним супутником інвестиційного циклу ШІ. Відповідно, прогнозується, що світовий ринок кібербезпеки зростатиме із середньорічним темпом зростання 13,8% і до 2034 року досягне майже 700 млрд доларів...

Цей сектор також отримує поштовх завдяки зростаючій ролі кібервійни в умовах нестабільної геополітичної ситуації. Цифрові мережі перетворилися на «нове поле бою», де суб'єкти, що діють за підтримки держави, та досвідчені хакери націлюються на критичну інфраструктуру та оборонні системи. Ця зміна перетворила кібербезпеку з допоміжної функції на центральний стовп національної безпеки, і очікується, що ринок військової кібербезпеки зростатиме із середньорічним темпом понад 12% до 2031 року. Цю тенденцію додатково підкріплюють рекордні глобальні військові витрати, які у 2025 році сягнули 2,89 трлн доларів, оскільки уряди надають пріоритет модернізації своїх цифрових систем захисту для протидії загрозам економічній та національній безпеці...

Довіра інвесторів до цієї «історії зростання» відображається у динаміці індексу S&P Kensho Cyber Security Index, який за останній рік зріс майже на 19%. Для тих, хто хоче скористатися цією довгостроковою тенденцією, кілька ETF, зокрема CIBR, HACK та IHAK, пропонують диверсифіковану експозицію в цьому секторі. У міру того, як підприємства стають все більш залежними від цифрового середовища та стикаються з підвищеними ризиками фінансових збитків і шкоди репутації внаслідок витоку даних, інвестиції в кібербезпеку перестали бути лише опцією і стали стратегічною необхідністю як для корпоративних, так і для державних суб'єктів». *(Yashwardhan Jain. Growing AI Risks & Defense Demand Boost Cybersecurity ETFs' Appeal // yahoo! finance. (<https://finance.yahoo.com/sectors/technology/articles/growing-ai-risks-defense-demand-163500071.html>). 08.05.2026).*

«У 2026 році у сфері кібербезпеки відбувається кардинальний перехід від реактивного захисту до прогнозного захисту на основі штучного інтелекту, що зумовлено зростаючою швидкістю та витонченістю сучасних загроз. Традиційні моделі безпеки, побудовані на статичних правилах та виявленні на основі сигнатур, стають дедалі менш ефективними проти експлойтів «нульового дня», шкідливого програмного забезпечення на базі штучного інтелекту, програм-вимагачів як послуги, внутрішніх загроз та складних постійних загроз. Водночас розширення площі атаки у хмарних, гібридних, віддалених та Інтернет-речей (IoT) середовищах перевантажує центри безпеки великим обсягом сповіщень, нестачею персоналу та повільними процесами реагування вручну...

Прогнозна кібербезпека усуває ці прогалини шляхом безперервного збору телеметричних даних з кінцевих точок, мереж, додатків, систем ідентифікації та

хмарних середовищ, а потім застосування машинного навчання, поведінкової аналітики та глобальної розвідки загроз для виявлення аномалій, прогнозування підозрілої активності та запуску автоматизованих захисних заходів ще до того, як відбудеться злом. Штучний інтелект відіграє центральну роль у цій моделі, дозволяючи системам аналізувати величезні обсяги даних, виявляти невідоме та безфайлове шкідливе програмне забезпечення, зменшувати кількість помилкових спрацьовувань та постійно адаптуватися до тактик зловмисників, що постійно еволюціонують. Аналітика поведінки встановлює нормальні базові показники для користувачів, пристроїв та систем, позначаючи відхилення, які можуть вказувати на компрометацію облікових даних, латеральне переміщення або внутрішні загрози. Функції автоматизованого реагування, такі як ізоляція кінцевих точок, блокування трафіку або вимкнення облікових записів, значно скорочують час від виявлення до локалізації...

Серед основних нових тенденцій — автономні центри управління безпекою, пошук загроз на основі штучного інтелекту, генеративний штучний інтелект для аналізу інцидентів та складання звітів, прогнозне управління вразливостями, а також об'єднання SIEM, XDR, SOAR та аналітики загроз у єдині платформи. Прогнозна кібербезпека також зміцнює архітектури «Zero Trust» та безпеку хмарних середовищ завдяки постійній перевірці моделей доступу та моніторингу розподілених робочих навантажень у провідних хмарних провайдерів...

Незважаючи на свої переваги, прогнозна кібербезпека стикається з низкою викликів, серед яких вимоги до якості даних, складність інтеграції з існуючою інфраструктурою, потреба у кваліфікованому персоналі та постійна загроза з боку наступальних інструментів на базі штучного інтелекту. Проте очікується, що організації, які вчасно впровадять прогнозні підходи, зможуть забезпечити вищу стійкість та безперебійність роботи, а проактивна система захисту на базі штучного інтелекту з плином десятиліття стане стандартною вимогою, а не стратегічною перевагою». (*Pushpendra Mishra. Predictive Cybersecurity in 2026: Stopping Threats Before They Happen // Techstrong Group Inc. (<https://securityboulevard.com/2026/05/predictive-cybersecurity-in-2026-stopping-threats-before-they-happen/>). 10.05.2026*).

«Нове опитування SANS/GIAC 2026, в якому взяли участь 947 керівників служб інформаційної безпеки (CISO), показує, що вперше занепокоєння щодо компетентності команд з кібербезпеки випередило турботи про чисельність персоналу: 60% респондентів вказали на «відсутність відповідних фахівців», тоді як 40% — на «недостатню чисельність персоналу». Ця зміна відображає те, як нові технології, такі як штучний інтелект та квантові обчислення, збільшують навантаження на систему безпеки та виявляють прогалини в навичках, тоді як керівники служб інформаційної безпеки намагаються визначити, оцінити та перевірити можливості, якими вони вже володіють або які їм потрібні... Оскільки кваліфіковані фахівці є дефіцитними та дорогими, багато керівників зосереджуються на підвищенні кваліфікації існуючих команд, а не на наймі нових співробітників. Водночас опитування вказує на відсутність чіткості у визначенні

дефіциту кваліфікованих кадрів та на поширену проблему «розбіжності посад», коли посадові назви не відповідають фактичним обов'язкам. Експерти рекомендують впроваджувати стандартизовані системи класифікації посад та навичок, такі як NICE, щоб точніше визначати вимоги до посад, узгоджувати навчання та зменшувати невідповідності у вимогах до кандидатів... Окрім технічних навичок, фахівці наголошують, що ефективна кібербезпека залежить від розуміння операційних процесів — знання того, що забезпечують системи, які наслідки має їхня відмова та як визначити пріоритети щодо відмовостійкості, — що важко навчити і що часто є результатом більш широкого організаційного досвіду. Лідерські якості та вміння вислухати й врахувати думки команди також вважаються надзвичайно важливими, що спонукає до пропозицій щодо двовекторних шляхів розвитку, які поєднують глибоку кіберспеціалізацію з досвідом у сфері бізнесу... Загалом, отримані дані свідчать про те, що багато організацій покращують координацію та структуру програм, але їм все ще бракує технічної компетентності, що виявляється у реальних наслідках, таких як пропущені виявлення загроз, уповільнена реакція та ризики, які до кінця усвідомлюються лише під час кризи». (*Shaun Waterman. Skills Gap Top CISO Concern, Says New SANS Survey // Information Security Media Group, Corp. (<https://www.inforisktoday.com/skills-gap-top-ciso-concern-says-new-sans-survey-a-31603>). 05.05.2026*).

«Незалежне опитування, проведене у квітні 2026 року серед 100 осіб, відповідальних за прийняття рішень у сфері операційних технологій (OT) на американських підприємствах, що займаються видобутком та транспортуванням нафти й газу, було організовано компанією Tosi після операції «Epic Fury». Результати показують, що галузь надзвичайно швидко збільшує витрати на кібербезпеку OT, але все ще стикається з серйозною проблемою у виявленні загроз. Хоча 87% респондентів заявляють, що впевнені у своїй здатності виявити активне порушення безпеки OT протягом 24 годин, більшість з них базують цю впевненість на інструментах та сигналах, які погано підходять для середовищ OT: 51% згадують інструменти IT-безпеки, які, за їхніми визнанням, мають обмежену видимість трафіку OT, 27% покладаються на те, що проблеми помітить персонал на місцях, і лише 16% вказують на постійний моніторинг OT... Результати опитування свідчать про активну реакцію ринку: 63% респондентів з 28 лютого підвищили оцінку кіберризиків через зростаючу конвергенцію IT та OT, атаки, що фінансуються державою, та віддалений доступ сторонніх осіб; 94% затвердили або розглядають питання про виділення позапланових коштів на безпеку OT; 95% очікують на збільшення бюджетів на безпеку OT у наступному році, причому 25% прогнозують зростання на понад 20%. Майже кожен оператор повідомив про принаймні одну категорію кіберінцидентів з кінця лютого, причому 48% стикалися з програмним забезпеченням-вимагачем, що вплинуло на системи, підключені до OT, а 48% повідомили про превентивні відключення OT, спричинені інцидентами на стороні IT... Виявлення та прозорість є головними пріоритетами на найближчу перспективу — безперервний моніторинг,

виявлення та реагування, орієнтовані на операційні технології (ОТ), виявлення активів та безпечний віддалений доступ становлять 71% найважливіших потреб у функціональних можливостях — проте найбільшою перешкодою є не фінансові, а організаційні фактори: 45% респондентів вказують на розбіжності в культурі та рівні кваліфікації фахівців з ІТ та ОТ, 28% — на небажання йти на операційні ризики, тоді як лише 11% називають бюджетні обмеження. Тосі стверджує, що тривала діяльність, спрямована Іраном проти критичної інфраструктури Заходу, підкріплена рекомендаціями уряду США щодо зривів у роботі промислових контролерів, робить нагальним усунення прогалин у виявленні, властивому ОТ, та безпечному віддаленому доступі, попереджаючи, що нові витрати або виправлять видимість ОТ, або ще більше закріплять набори ІТ-інструментів, які, за словами самих операторів, не можуть адекватно «бачити» загрози ОТ». *(Oil And Gas Operators Are Confident They Can Detect A Cyberattack. The Tools They Are Using Cannot. Tosi Reports // VertMarkets, Inc. (<https://www.oilandgasonline.com/doc/oil-and-gas-operators-are-confident-they-can-detect-a-cyberattack-the-tools-they-are-using-cannot-tosi-reports-0001>). 11.05.2026).*

«Кібербезпека — це галузь, що стрімко розвивається та характеризується великою різноманітністю, і яка присвячена захисту приватної інформації та запобіганню злочинним атакам за допомогою креативного підходу до вирішення проблем та стратегічного мислення. Хоча технічні навички є корисними, галузь значною мірою покладається на фахівців, які вміють передбачати зловмисні тактики та ефективно доносити складні концепції, а це означає, що для досягнення успіху не обов'язково бути програмістом. Ця галузь пропонує різноманітні спеціалізовані кар'єрні шляхи, наприклад, етичні хакери, яких наймають для виявлення вразливостей систем шляхом імітації злочинної поведінки, та кіберрозслідувачі, які діють як цифрові детективи, відстежуючи підказки, такі як журнали серверів та ІР-адреси, щоб вирішувати та запобігати крадіжкам особистих даних та шахрайству...

Ця галузь також охоплює як проактивне проектування, так і реактивний аналіз. Розробники систем безпеки для ігор та додатків працюють з самого початку проекту, щоб інтегрувати в програмне забезпечення такі функції, як шифрування та безпечні платіжні системи, тоді як експерти з цифрової криміналістики вступають у справу після порушення безпеки, щоб ретельно проаналізувати пристрої та відновити приховані дані. Крім того, у цій галузі працюють викладачі та активісти, які розширюють обізнаність громадськості, спрощуючи поняття безпеки та пропагуючи відповідальне використання технологій. Незалежно від того, чи йдеться про створення безпечної інфраструктури, розслідування злочинів чи навчання інших, кібербезпека надає численні можливості для тих, хто захоплюється головоломками, захистом та перехитруванням цифрових загроз». *(Five Cybersecurity Careers You Need to Know // TIME USA, LLC. (<https://www.timeforkids.com/your-hot-job/articles/five-cybersecurity-careers-you-need-to-know>). 11.05.2026).*

«Традиційно кібербезпека характеризувалася фундаментальною асиметрією: захисники повинні захищати кожну можливу точку входу, тоді як зловмисникам достатньо виявити лише одну вразливість. Хоча штучний інтелект наразі використовується для автоматизації рутинних робочих процесів у сфері безпеки — таких як сортування сповіщень та нормалізація даних — це лише еволюційний крок, спрямований на підвищення операційної ефективності, а не на усунення структурних недоліків. Справжня трансформація полягає у поєднанні логічних висновків ШІ з високоякісною аналітикою загроз, що створює якісно нові оборонні можливості, які дозволяють захисникам перейти від сліпого, реактивного захисту до проактивної стратегії, що базується на інформації про загрози...

Поєднуючи когнітивні можливості штучного інтелекту з оперативною інформацією про тактику, методи та процедури (ТТР) зловмисників, організації тепер можуть постійно зіставляти дані про зовнішні загрози зі своїм конкретним внутрішнім середовищем — включаючи стан оновлень, конфігурації мережі та охоплення систем виявлення. Такий підхід дозволяє здійснювати прогностичну пріоритезацію, відходячи від абстрактних показників серйозності, таких як бали CVSS, на користь оцінки ризиків, заснованої на тому, як зловмисники насправді діють у реальних умовах. Штучний інтелект дозволяє захисникам визначати найімовірніші шляхи атаки, постійно моделювати свою вразливість та передбачати наступні кроки супротивника під час активних інцидентів, тим самим зосереджуючи обмежені ресурси на найважливіших загрозах...

Крім того, така конвергенція відкриває можливості для нового виду активної оборони на основі інтелектуальних адаптивних заходів маскуванню. На відміну від статичних «медових пасток», пастки, створені за допомогою штучного інтелекту, можуть динамічно еволюціонувати, імітуючи реальну інфраструктуру, що дозволяє ефективно перехопити ініціативу у зловмисників. Розміщуючи такі приманки на найпопулярніших шляхах атак, захисники можуть змусити супротивника витрачати час, підірвати його впевненість та перетворити пасивні засоби виявлення на активні операції зі збору розвідданих, які потім використовуються в оборонному циклі...

Зрештою, таке поєднання робить оборонні системи, що базуються на аналітичних даних, доступнішими для широкого кола користувачів, даючи організаціям змогу діяти з таким рівнем ситуаційної обізнаності, який раніше був притаманний лише елітним «червоним командам». Хоча ШІ не усуває природної переваги зловмисника, він кардинально змінює умови протистояння. Конкурентне середовище переходить від моделі «зловмисник проти захисника» до моделі «підсилені ШІ проти непідсилені», де організації, які інтегрують ШІ з надійною аналітикою загроз, можуть досягти рівня рівності, що раніше був неможливим. Надаючи захисникам можливість прогнозувати, визначати пріоритети та вводити в обману, ШІ допомагає зменшити структурну асиметрію, дозволяючи навичкам, підготовці та оперативній дисципліні стати вирішальними факторами в сучасному, суперечливому цифровому середовищі». (*Staffan Truvé. Beyond Acceleration and Automation: How AI + Intelligence Changes Cyber Defense // Recorded Future®* (<https://www.recordedfuture.com/blog/ai-intelligence-cyber-defense>). 14.05.2026).

«На Глобальному саміті з кібербезпеки Rapid7 2026 обговорювалося, як команди безпеки адаптуються до середовища, яке характеризується зростанням швидкості, масштабу та складності. Основною темою була еволюція початкових векторів доступу, оскільки сучасні атаки дедалі більше покладаються на зловживання ідентифікаційними даними, соціальну інженерію та неправильне налаштування хмарних сервісів – дії, які поєднуються зі звичайною поведінкою та вимагають від аналітиків виявлення тонких, мультисистемних закономірностей. У відповідь на це сучасні команди керованого виявлення та реагування (MDR) і Центру операційної безпеки (SOC) зосереджуються на реагуванні на інциденти за участі людей, підкреслюючи, що координація та здатність приймати рішення в стресових ситуаціях є не менш важливими, ніж самі технології... Щоб боротися зі зростаючою складністю фрагментованих інструментів і даних, організації переходять від традиційного керування вразливостями на основі обсягу до контекстного «керування впливом». Цей підхід, що використовує такі фреймворки, як безперервне керування вразливістю до загроз (CTEM), визначає пріоритетність ризиків на основі доступності активів і фактичного впливу на бізнес. Крім того, поки зловмисники використовують ШІ для масштабування розвідки та соціальної інженерії, захисники застосовують ШІ, щоб прискорити сортування та зменшити втому від оповіщень, зосереджуючись на ШІ як на допоміжному інструменті, а не як на заміні людського нагляду. Зрештою, саміт підкреслив всеосяжний перехід у сфері безпеки до більш раннього та обґрунтованого прийняття рішень, що вимагає тіснішої інтеграції між виявленням загроз, їх виявленням і реагуванням, щоб зупинити інциденти, перш ніж вони загостряться...» (*Emma Burdett. Rapid7's 2026 Global Cybersecurity Summit: Key Takeaways for Security Leaders* // *Rapid7* (<https://www.rapid7.com/blog/post/it-2026-global-cybersecurity-summit-key-takeaways-security-leaders/>). 19.05.2026).

«Глобальне опитування, проведене компанією WatchGuard Technologies серед приблизно 1 000 керівників у сфері ІТ та кібербезпеки у 20 країнах, показало, що сучасні загрози, посилені штучним інтелектом, випередили можливості більшості внутрішніх команд з безпеки, що змушує переходити від самостійного забезпечення безпеки до моделей захисту, що постійно діють і надаються зовнішніми постачальниками. У ході дослідження 91% організацій заявили, що стурбовані кібератаками на основі штучного інтелекту, а 75% повідомили, що за останній рік зазнали принаймні одного кіберінциденту. Водночас 54% визнали, що не можуть забезпечити безперервний цілодобовий моніторинг та реагування, а 67% зазначили, що потребують додаткової підтримки для виконання все більш жорстких вимог щодо дотримання нормативних вимог. Майже половина респондентів (48%) вже покладається на постачальників керованих послуг для доповнення внутрішніх ресурсів, що відображає те, що WatchGuard описує як «дефіцит потужностей», а не простий дефіцит навичок, і багато організацій дедалі частіше розглядають постачальників як стратегічних, проактивних партнерів, а не як базову ІТ-підтримку...

Дослідження також свідчить про те, що штучний інтелект змінює купівельну поведінку: 44% організацій готові платити більше за системи виявлення та реагування на основі штучного інтелекту, а критерії оцінки зміщуються від традиційних показників якості послуг до очікувань, орієнтованих на результат, таких як швидше виявлення та реагування, проактивне запобігання, зменшення складності та підвищення стійкості. Хоча регіональні моделі різняться — керовані послуги більш укорінені на зрілих ринках, таких як США та Франція, реселери з доданою вартістю залишаються більш поширеними в Мексиці, а підходи, орієнтовані на консалтинг, сильніші в Канаді — сигнали попиту збігаються в усьому світі навколо можливостей на основі ШІ, безперервного моніторингу, швидкого реагування та підтримки дотримання вимог. Незважаючи на економічну невизначеність, витрати зростають: 75% організацій очікують збільшення бюджетів на кібербезпеку протягом наступних двох років, що свідчить про те, що кібербезпека стає постійною операційною вимогою та створює значні можливості для MSP перетворитися на повноцінних партнерів з безпеки». *(Neil Trim. SMBs Hit a Cybersecurity Breaking Point as 91% Fear AI-Driven Attacks, Driving Shift to MSP-Led Security Models, WatchGuard Finds // Kingswood Media (<https://technologyreseller.uk/smb-hit-a-cybersecurity-breaking-point-as-91-fear-ai-driven-attacks-driving-shift-to-msp-led-security-models-watchguard-finds/>). 20.05.2026).*

«Кібербезпека повинна постійно розвиватися у відповідь на атаки, що стають дедалі більш автоматизованими та базуються на штучному інтелекті. Хоча багаторівневий захист залишається важливим, одного лише його вже недостатньо; організації повинні трансформувати свою загальну архітектуру безпеки, щоб вона стала динамічною, автоматизованою та адаптивною. Сучасні стратегії роблять акцент на автономних системах кібербезпеки, здатних виявляти загрози та реагувати на них за лічені секунди, скануючи величезні обсяги даних, що значно перевищують людські можливості. Архітектури безпеки також мають бути гнучкими та переконфігурованими, розробленими як еволюційні плани, що адаптуються до потреб бізнесу та нових загроз, а не покладатися на статичні моделі та реактивне виправлення. Зі зникненням традиційних корпоративних меж у зв'язку з переходом на дистанційну роботу та хмарні технології, видимість, розподілений моніторинг та автоматизоване ведення журналів стали необхідними для забезпечення простежуваності у розрізнених середовищах...

Штучний інтелект та машинне навчання відіграють центральну роль у цій трансформації. Хоча ШІ є двосічним мечем — його використовують як захисники, так і зловмисники — він дозволяє швидко виявляти закономірності, проводити масштабний аналіз та автоматично реагувати в режимі реального часу без втручання людини. Однак, оскільки ШІ стає невід'ємною частиною операцій з безпеки, організації також повинні захищати самі системи ШІ, щоб запобігти тому, щоб вони стали точками відмови або джерелами витоку даних.

Широке впровадження хмарних технологій, периферійних обчислень та гібридних середовищ є одним із найважливіших архітектурних зрушень.

Традиційні, чітко визначені межі мережі зникли, поступившись місцем географічно розподіленим системам, що функціонують за спільними моделями безпеки із залученням зовнішніх постачальників. Сучасні архітектури повинні зосереджуватися на захисті ідентичності та даних незалежно від їхнього місцезнаходження, забезпечувати наскрізну простежуваність у локальних та хмарних системах, а також впроваджувати надійне управління даними, включаючи класифікацію та маркування конфіденційної інформації.

Архітектура Zero Trust стала основоположною моделлю сучасної кібербезпеки. Створена на принципі «недовіри за замовчуванням», Zero Trust вимагає постійної верифікації користувачів, пристроїв та даних, незалежно від їхнього місцезнаходження. Ідентифікація стає центральним елементом, замінюючи моделі довіри, засновані на місцезнаходженні, тоді як мікросегментація запобігає горизонтальному переміщенню в мережах, обмежуючи здатність зловмисника вільно переміщатися у разі порушення безпеки...

Стрімке зростання Інтернету речей (IoT) та підключених пристроїв ще більше ускладнює розробку систем безпеки через величезну кількість і різноманітність пристроїв, які часто не є захищеними. Організації повинні покладатися на сегментацію, багаторівневий захист та периферійні шлюзи, що ізолюють пристрої та перевіряють трафік. Такі методи, як віртуальне виправлення вразливостей, допомагають зменшити ризики, водночас слід ретельно зважувати, чи справді в кожному конкретному випадку необхідне підключення до мережі...

Зрештою, архітектори кібербезпеки повинні прийняти динамічний, стійкий підхід. Замість того, щоб проектувати неприступні фортеці, вони повинні виходити з того, що порушення безпеки неминучі, і зосередитися на локалізації, автоматизації та швидкому відновленні, щоб мінімізувати витік даних. Приймаючи нові технології, такі як штучний інтелект, хмарні та квантові обчислення, архітектори повинні залишатися прив'язаними до бізнес-пріоритетів, гарантуючи, що стратегії безпеки, які постійно розвиваються, ефективно захищають те, що має найбільше значення». **(Daniel Consentini. How cybersecurity architecture will evolve: more attacks and more sophisticated ones // Telefónica S.A. (<https://www.telefonica.com/en/communication-room/blog/cybersecurity-architecture-will-evolve/>). 25.05.2026).**

«У міру того як глобальні ланцюги постачання стають дедалі складнішими та все більше залежать від технологій, кібербезпека перетворилася на надзвичайно важливий пріоритет, адже навіть одна слабка ланка може порушити роботу цілих міжнародних мереж. Сучасні ланцюги постачання базуються на взаємопов'язаних постачальниках, логістичних компаніях, виробниках, постачальниках програмного забезпечення та хмарних платформах, що наражає підприємства на такі ризики, як компрометація сторонніх постачальників, атаки на ланцюги постачання програмного забезпечення, викрадення даних та зупинка операційної діяльності. Навіть незначні вразливості можуть спричинити масштабні ланцюгові ефекти в глобальних операціях, що

робить комплексне запобігання ризикам та планування заходів із забезпечення стійкості надзвичайно важливими...

Одним із найяскравіших прикладів стала атака NotPetya на компанію Maersk у 2017 році, яка розпочалася як державна атака, спрямована проти України, а потім поширилася по всьому світу через заражені оновлення програмного забезпечення та незахищені вразливості. Атака заразила понад 45 000 ПК та 4 000 серверів, паралізувала роботу понад 600 офісів і призвела до зупинки 76 портових терміналів по всьому світу, що в підсумку обійшлося компанії, за оцінками, у 300 мільйонів доларів США. Maersk була змушена тимчасово відмовитися від своїх цифрових систем і перейти на ручні, паперові операції, щоб відновити критично важливі функції. Цей інцидент підкреслив важливість управління виправленнями, багатофакторної автентифікації, планування безперервності бізнесу та високої прозорості всіх операцій. У відповідь Maersk розробила спеціальну політику кібербезпеки, в якій наголошується на необхідності контролю та мінімізації ризиків, що виникають у зв'язку з взаємопов'язаними системами та цифровою інфраструктурою...

Недавні атаки ще раз підтвердили ці висновки. У 2025 році кілька британських компаній, що входять до ланцюга постачання продуктів харчування, зокрема Co-op, Peter Green Chilled та Marks & Spencer, стали жертвами кібератак. Компанія Marks & Spencer зазнала шеститижневого збою в роботі цифрових систем, що призвело до припинення доставки товарів додому та послуг «замовлення онлайн — самовивіз», внаслідок чого втрати доходу склали приблизно 300 мільйонів фунтів стерлінгів. Аналогічно, компанія Jaguar Land Rover зазнала кібератаки, яка зупинила виробництво на багатьох виробничих майданчиках, змусивши тисячі співробітників залишитися вдома та затримавши поставки клієнтам. Оскільки JLR працює за моделлю виробництва «точно в строк», це порушення також серйозно вплинуло на постачальників, які залежать від синхронізованих графіків виробництва...

Дані галузі свідчать про масштаби загрози: 63% роздрібних торговців повідомляють про випадки кіберзлочинів, а 61% організацій протягом року стикаються з атаками на сторонніх постачальників або ланцюги постачання, незважаючи на високий рівень впевненості у своїй готовності. Експерти попереджають, що штучний інтелект та стрімка цифровізація розширюють площину атаки швидше, ніж багато організацій встигають її захистити, особливо коли підприємства впроваджують технології штучного інтелекту без належних систем безпеки.

Щоб зменшити ризик, організації повинні надати пріоритет видимості активів, відстеженню залежностей, постійному моніторингу відповідності вимогам, безпеці програмного забезпечення та захисту від програм-вимагачів. Ефективне управління ризиками, пов'язаними з постачальниками та сторонніми організаціями, вимагає ретельної оцінки безпеки до підписання контрактів, а також постійного моніторингу протягом усього терміну партнерства. Зрештою, кібербезпека більше не може зосереджуватися виключно на захисті окремих організаційних периметрів; вона має бути інтегрована у співпраці в усій екосистемі ланцюга постачання через спільну видимість, довіру та планування стійкості». *(Louise Collins. Supply Chain*

«Кібербезпека стала неминучою проблемою для малих та середніх підприємств (МСП), які все частіше стають мішенню для витончених атак, незважаючи на обмежені IT-ресурси та бюджети. Згідно з доповіддю gitnux.org за 2026 рік, 61% МСП зазнали принаймні однієї кібератаки протягом минулого року, причому фішинг та програми-вимагачі були серед найпоширеніших загроз. Хоча більшість компаній використовують антивірусне програмне забезпечення, необхідність застосування численних засобів безпеки створює значне навантаження на управління та все ще залишає небезпечні прогалини...

У відповідь на це все більше малих та середніх підприємств переходять на інтегровані рішення, такі як брандмауери серії USG FLEX N від Zyxel Networks, які забезпечують багаторівневий захист завдяки архітектурі «нульової довіри», аналітиці загроз на основі штучного інтелекту, запобіганню вторгненням у режимі реального часу, технології «пісочниці», веб-фільтрації та розширеному захисту від програм-вимагачів. Управління пристроями здійснюється через безпечну хмарну платформу Nebula, яка підтримує функцію Smart Sync, що автоматично синхронізує політики безпеки на всіх пристроях і в усіх локаціях, зменшуючи кількість ручних помилок та забезпечуючи послідовний захист для організацій з декількома офісами або гібридним персоналом...

Незалежне тестування, проведене компанією Tolly, визнало серію USG FLEX N за її виняткову ефективність у боротьбі з шкідливим програмним забезпеченням, високу продуктивність фільтрації URL-адрес та чудову загальну цінність. Кевін Дрінкалл, старший директор з маркетингу компанії Zyxel Networks, підкреслив, що це рішення було розроблено для забезпечення малих та середніх підприємств захистом корпоративного рівня, який є одночасно потужним і простим в управлінні. У міру зростання залежності від цифрових систем навіть короточасні перебої можуть завдати серйозної шкоди операційній діяльності, фінансам та репутації. З огляду на постійне зростання кіберзагроз експерти застерігають, що малим та середнім підприємствам слід посилити свою захисну систему саме зараз, до того, як зловмисники завдадуть першого удару». (**Why next-gen cybersecurity is a must for small businesses // Times Media Limited** (<https://www.thetimes.com/static/cybersecurity-threats-smb-protection-security-zyxel/>). 20.05.2026).

«Неприбуткова організація Cybermindz, що займається питаннями кіберстійкості, закликає підприємства розглядати вигорання у сфері кібербезпеки не лише як проблему благополуччя на робочому місці, а як серйозний операційний та безпековий ризик. Дослідження, проведене організацією, показало, що вигорання та стрес залишаються поширеними серед фахівців з кібербезпеки: половина опитаних працівників відчуває вигорання

щотижня або щодня. Дослідження також виявило, що 66 відсотків респондентів повідомили про помірне або високе емоційне виснаження, а більше половини продемонстрували одночасно кілька ознак вигорання. За словами засновника Cybermindz Пітера Коронеоса, розгляд вигорання виключно як питання благополуччя часто обмежує залучення організацій та фінансування, оскільки такі ініціативи розглядаються як необов'язкові, а не як необхідні для стійкості кібербезпеки...

Компанія Cybermindz стверджує, що синдром вигорання має прямий вплив на рівень корпоративних ризиків, особливо з огляду на те, що команди з кібербезпеки дедалі частіше стикаються з постійним тиском, великим навантаженням та ескалацією кібератак. Coroneos навела приклади, коли серйозні інциденти, такі як масштабні атаки з використанням програм-вимагачів або атаки зсередини, викликали у співробітників служб кібербезпеки симптоми, схожі на посттравматичний стрес, і призвели до значного відтоку кадрів, що в кінцевому підсумку послабило захисні механізми організації. Розглядаючи психічне здоров'я та психологічну стійкість як складові управління операційними ризиками, керівники служб інформаційної безпеки можуть ефективніше доносити до керівництва компанії інформацію про вплив благополуччя персоналу на бізнес...

Нещодавнє дослідження iRest® Impact Study, проведене цією організацією, показало, що навіть обмежені інвестиції в тренінги з розвитку психологічної стійкості можуть суттєво покращити як самопочуття співробітників, так і оперативну ефективність. У дослідженні, в рамках якого було проаналізовано дані 275 фахівців з кібербезпеки, які брали участь у перевірених у військових умовах програмах тренінгів з розвитку психологічної стійкості, зафіксовано помітне поліпшення якості сну, зниження емоційного виснаження та цинізму, а також підвищення професійної ефективності. Також було виявлено зниження ризику плинності кадрів на 71 відсоток, що свідчить про те, що програми з розвитку психологічної стійкості можуть допомогти організаціям утримати ключових фахівців у сфері кібербезпеки. Cybermindz робить висновок, що зміцнення психологічної стійкості серед фахівців з кіберзахисту є важливим не лише для здоров'я співробітників, а й для забезпечення ефективної роботи систем кібербезпеки та загальної безпеки суспільства». *(Beth Maundrill. Infosecurity Europe: Why Burnout in Cybersecurity Demands Risk-Based Response // Reed Exhibitions Ltd. (<https://www.infosecurity-magazine.com/news/why-burnout-cybersecurity-risk/>). 27.05.2026).*

«Агентства з зв'язків з громадськістю, діяльність яких традиційно ґрунтується на довірі, конфіденційності та репутації, у 2026 році стикаються з цифровими ризиками, що стрімко еволюціонують, через що кіберстійкість перетворилася з ІТ-проблеми на один із головних пріоритетів бізнесу. Як зберігачі надзвичайно чутливої інформації — зокрема, оголошень, що підлягають ембарго, планів дій у кризових ситуаціях та конфіденційних повідомлень керівництва — агентства стають дедалі вразливішими до кібератак, які можуть швидко перерости з технічних порушень у серйозні кризи репутації та довіри

клієнтів. Згідно з доповіддю «Глобальний прогноз кібербезпеки на 2026 рік» Світового економічного форуму, кібершахрайство випередило програмне забезпечення для вимагання викупу як головну проблему для керівників компаній, тоді як 87% респондентів повідомили про зростання вразливостей, пов'язаних зі штучним інтелектом. Дослідження Cisco «Оцінка стану даних та конфіденційності у 2026 році» виявило, що 90% підприємств розширили свої програми захисту конфіденційності через штучний інтелект, а 93% планують подальші інвестиції в управління даними. У ОАЕ ситуація є особливо гострою: щодня фіксується від 90 000 до 200 000 спроб вторгнення, а з початку 2026 року зареєстровано 128 підтверджених кіберінцидентів...

Ця загроза посилюється завдяки витонченим фішинговим атакам та атакам із піддробкою особи, що базуються на штучному інтелекті. Тільки у першому кварталі 2026 року компанія Microsoft виявила 8,3 мільярда фішингових загроз, пов'язаних з електронною поштою, причому кількість фішингових атак із використанням QR-кодів зросла на 146%, а компанія CrowdStrike повідомила про 89-відсоткове зростання активності зловмисників, що використовують штучний інтелект, порівняно з аналогічним періодом минулого року, а також про те, що середній час виявлення кіберзлочинів становить лише 29 хвилин. Один-єдиний злом може поставити під загрозу надійні канали комунікації, призвести до витоку конфіденційних даних клієнтів або сприяти поширенню неправдивої інформації, що безпосередньо підриває довіру до агентств, які наймають для захисту. Оскільки клієнти приділяють все більшу увагу управлінню цифровими ризиками, кіберстійкість стає ключовим фактором конкурентної переваги. Агентствам тепер необхідно розглядати її як невід'ємну частину управління, забезпечення безперебійної роботи, підготовки співробітників та управління репутацією — виходячи далеко за межі технічних контрольних списків — щоб захистити інформацію клієнтів, забезпечити безперебійність роботи та зберегти власну репутацію у дедалі більш ворожій цифровій середовищі». *(Nidal Abou Zaki. Cyber resilience has become business priority for PR agencies in 2026 // PRmoment.com (<https://www.prmoment.com/mena/why-cyber-resilience-has-become-business-priority-for-pr-agencies-in-2026>). 21.05.2026).*

«...За словами Суніти Чалам, партнера компанії Brunswick Group, кіберінциденти вже не є рідкісними подіями типу «чорного лебедя», а стали для організацій звичним явищем: частка організацій, які щороку стикаються принаймні з одним кіберінцидентом, зросла з семи з десяти п'ять років тому до майже дев'яти з десяти сьогодні. Виступаючи з вступною промовою на ITWeb Security Summit 2026 у Кейптауні, Чалам зазначила, що очікування громадськості та зацікавлених сторін суттєво змінилися. Глобальне опитування понад 4 000 осіб у США, Великій Британії, Франції та Південній Кореї показало, що 71% респондентів оцінюють компанії більше за те, як вони реагують на атаку, ніж за сам інцидент, а 85% заявили, що правильно вирішений інцидент може навіть підвищити довіру. Аналогічно, 86% вважають, що якість реакції компанії на кібератаку відображає загальний рівень управління організацією...

Аналіз 59 американських компаній, які протягом трьох років повідомляли про кіберінциденти, не виявив ознак серйозного або тривалого зниження курсу акцій, причому будь-які початкові падіння зазвичай тривали не більше 30–60 днів. Як зазначив Чалам, зацікавлені сторони не очікують досконалості — вони хочуть бачити чіткі докази того, що організація зберігає контроль над ситуацією завдяки швидкому та прозорому інформуванню, оперативному відновленню послуг та очевидним висновкам, які сприяють зміцненню систем і процесів...

Однак розробка ефективних заходів реагування ускладнюється через те, що кіберзлочинність охоплює території різних юрисдикцій. Культурні відмінності в очікуваннях можуть бути значними — наприклад, публічні вибачення мають велике значення в Південній Кореї, але набагато менш важливі у Франції чи Великій Британії. Тому найефективніші заходи реагування поєднують у собі єдину глобальну позицію з комунікацією, адаптованою до місцевих умов, та залученням зацікавлених сторін.

Чалам порадила організаціям ретельно підготуватися заздалегідь, провівши аудит своїх даних, нормативних зобов'язань та процесів прийняття рішень; розробивши лаконічні, практичні та регулярно перевірені плани дій на випадок кіберкризи; перевіривши ефективність заходів з відновлення роботи за допомогою реалістичних моделювань; налагодивши чуйне спілкування як із постраждалими зацікавленими сторонами, так і з працівниками; а також приділяючи пильну увагу безпеці ланцюга поставок, оскільки слабкі місця у сторонніх партнерів можуть легко поставити під загрозу навіть добре захищені компанії...» (*Joanne Carew. Managing cyber risks in global economy // ITWeb Limited (<https://www.itweb.co.za/article/managing-cyber-risks-in-global-economy/LPp6VMrBVzKMDKQz>). 26.05.2026*).

«...З оновленням концепції Дена Сазерленда від 2019 року роль юриста з питань кібербезпеки стає дедалі важливішою — і складнішою — через поширення програм-вимагачів, розвиток штучного інтелекту, глобальні кіберконфлікти та хвилю нових регуляторних вимог, таких як CIRCIA та правила звітності SEC. Незважаючи на ці зростаючі загрози, останні опитування показують, що юридичні відділи багатьох компаній як і раніше не мають достатніх ресурсів, стикаються з труднощами у налагодженні активної співпраці з державними органами та часто не доносять інформацію про кіберризики до рівня ради директорів. Щоб ефективно протидіяти цим сучасним загрозам, організації повинні глибоко інтегрувати юристів з питань кібербезпеки у свою основну діяльність, надаючи їм повноваження виступати важливим посередником між технічними керівниками, такими як керівники служб інформаційної безпеки (CISO) та керівники інформаційних служб (CIO), та більш широкими бізнес- та юридичними підрозділами. Сучасний юрист з кібербезпеки повинен мати глибоке розуміння як базових законодавчих актів, так і швидко розвиваючихся федеральних, державних та міжнародних рамок щодо даних, а також вільно володіти базовими технологіями...

Сфера діяльності юридичної практики з кібербезпеки значно розширилася, що вимагає від юристів активної співпраці з урядовими та правоохоронними органами — такими як CISA, ФБР та галузеві регуляторні органи — замість того, щоб лише реагувати на перевірки дотримання нормативних вимог. Від юристів, що спеціалізуються на кібербезпеці, тепер очікують, що вони братимуть активну участь у розробці стратегій реагування на інциденти, вирішуватимуть складні правові та нормативні дилеми, пов'язані з виплатами викупу за програмне забезпечення-вимагач, а також допомагатимуть керівництву компаній у створенні реалістичних моделей загроз з використанням таких усталених методологій, як NIST CSF 2.0. Окрім негайного реагування на інциденти, їхні щоденні обов'язки розширилися і тепер включають управління ризиками ланцюга постачання програмного забезпечення та сторонніх постачальників за допомогою суворих договірних умов, проведення комплексної перевірки під час злиттів та поглинань з акцентом на національній економічній безпеці та іноземних інвестиціях, а також ретельне вивчення мінливих обмежень полісів кіберстрахування, включаючи нові виключення щодо «актів війни»... Зрештою, орієнтування в цьому мінливому середовищі вимагає тісної співпраці; налагоджуючи міцні зв'язки між керівництвом, інженерними командами та партнерами з державного сектору, юристи, що спеціалізуються на кібербезпеці, відіграють незамінну роль у захисті не лише своїх конкретних організацій, а й критичної інфраструктури країни та цифрового суспільства в цілому...» (*Spencer R. Fisher, Terence A. Check, Jr. What Is a Cybersecurity Legal Practice, 2.0? // The Lawfare Institute* (<https://www.lawfaremedia.org/article/what-is-a-cybersecurity-legal-practice--2.0>). 27.05.2026).

«У міру того як сучасні кіберзагрози стають дедалі витонченішими, динамічнішими та базуються на штучному інтелекті, організації повинні перестати розглядати кібербезпеку як суто технологічну проблему і зосередитися на формуванні надійної кіберстійкості як серед персоналу, так і в інфраструктурі. З огляду на стрімке зростання вразливостей штучного інтелекту та ризиків, пов'язаних із ланцюгами постачання сторонніх постачальників, метою вже є не лише запобігання атакам, а й забезпечення безперебійної роботи бізнесу шляхом надання всім співробітникам можливості приймати обґрунтовані рішення в умовах тиску. Щоб досягти цього, керівники повинні дотримуватися чотирьох ключових принципів: проактивне запобігання атакам, виявлення та локалізація загроз, швидке відновлення нормальної роботи та адаптація процесів на основі отриманого досвіду... Важливо, що в умовах стирання межі між ІТ та фізичними операціями — про що свідчить майже 20-відсоткове зростання кількості кібератак, що спричиняють фізичні наслідки — організації повинні сприяти конвергенції ІТ-та ОТ-команд за допомогою перехресного навчання та створення єдиного реєстру активів. На практиці підвищення кіберстійкості вимагає розгортання агентських засобів захисту на основі штучного інтелекту для протидії автоматизованим атакам, впровадження динамічних моделей «нульової довіри» з мікросегментацією, а також запровадження суворого та безперервного управління постачальниками з

метою мінімізації ризиків, пов'язаних із залученням сторонніх організацій... Крім того, надзвичайно важливо регулярно проводити навчальні тренування, що дозволяють перевірити ефективність реагування в умовах стресових ситуацій. Зрештою, кіберстійкість вимагає постійної заангажованості всього колективу, коли захист критично важливих систем та забезпечення безперебійної роботи є спільною відповідальністю всього персоналу, а не лише керівників служб безпеки». (*Sean Toohey. Building cyber resilience for mission-critical operations in 2026 // Information Security Buzz* (<https://informationsecuritybuzz.com/cyber-resilience-for-mission-critical-operations/>). 27.05.2026).

«Сьогодні, у міру зростання залежності від даних та взаємопов'язаної бізнес-інфраструктури, кожна компанія повинна розглядати себе як технологічну організацію, а кібербезпеку — як фундаментальний ризик для підприємства, а не лише як проблему ІТ-відділу. Ефективний нагляд за кібербезпекою починається з сильного лідерства з боку вищого керівництва, зокрема ради директорів (BoD), яка відіграє вирішальну роль у нагляді за стратегією керівництва щодо виявлення, визначення пріоритетності та управління кіберризиками. Важливо, що нагляд полягає не в тому, щоб керівництво займалося технічними деталями, а в тому, щоб встановлювати очікування, забезпечувати підзвітність та підтверджувати наявність відповідних засобів контролю для зменшення ризиків.

Однак ради директорів часто потрапляють у дві типові пастки: або залишаються на занадто високому рівні, надаючи лише загальні запевнення без глибокого розуміння фактичних ризиків, або занурюються у технічну термінологію, яка не сприяє обґрунтованому прийняттю рішень. З огляду на посилення регуляторного контролю, судові позови акціонерів та питання корпоративного управління, пов'язані з кіберінцидентами, директори потребують обґрунтованого, принципового підходу до своїх обов'язків з нагляду...

Основні принципи ефективного нагляду передбачають розуміння кібербезпеки як корпоративного ризику, інтегрованого в загальну стратегію та систему управління. Члени ради директорів повинні формувати базові компетенції шляхом постійного навчання, розглянути можливість залучення до складу ради експертів з кібербезпеки та оцінювати кіберризики так само, як і інші бізнес-ризики — шляхом визначення рівня прийнятного ризику, виявлення загроз та контролю за рішеннями керівництва щодо запобігання, мінімізації або передачі ризиків. Питання кібербезпеки мають бути невід'ємною частиною обговорень щодо злиттів, розробки продуктів, цифрових ініціатив та стратегічних партнерств.

Практичні кроки включають наймання або консультації з експертами з кібербезпеки, забезпечення навчання на рівні ради директорів, встановлення чіткого курсу на те, що кібербезпека є стратегічним пріоритетом, проведення регулярного навчання співробітників та взаємодію з партнерами з галузі та уряду. Рада директорів повинна щонайменше раз на рік отримувати оновлену інформацію від керівництва, виділяти час у порядку денному для обговорення кіберризиків та документувати рішення щодо нагляду. Від керівництва слід очікувати

впровадження комплексної системи управління ризиками, такої як NIST Cybersecurity Framework (NIST CSF 2.0), яка слугує орієнтиром для оцінки та зменшення кіберризиків. Хоча членам ради директорів не потрібно розуміти кожну систему контролю, вони повинні стежити за тим, щоб така система була впроваджена, застосовувалася послідовно, а прогалини усувалися за допомогою відповідних ресурсів...

Ради директорів також можуть залучати зовнішніх аудиторів або консультантів для проведення незалежних оцінок, що дають об'єктивну інформацію щодо ефективності програм кібербезпеки. Нагляд часто делегується спеціалізованим комітетам — зазвичай з питань аудиту, ризиків або технологій — з чітко визначеними обов'язками, зафіксованими в статутах. Ці комітети повинні отримувати щоквартальні звіти, переглядати внутрішні звіти та мати доступ до зовнішніх експертів. Їхня роль полягає у перевірці того, чи відповідає впровадження керівництвом рамкам управління ризиками підприємства, а також у нагляді за оперативними заходами з кібербезпеки, такими як перевірка надійності сторонніх постачальників, управління вразливостями, аналіз загроз та протоколи резервного копіювання...

Ради директорів також можуть залучати зовнішніх аудиторів або консультантів для проведення незалежних оцінок, що дають об'єктивну інформацію щодо ефективності програм кібербезпеки. Нагляд часто делегується спеціалізованим комітетам — зазвичай з питань аудиту, ризиків або технологій — з чітко визначеними обов'язками, зафіксованими в статутах. Ці комітети повинні отримувати щоквартальні звіти, переглядати внутрішні звіти та мати доступ до зовнішніх експертів. Їхня роль полягає у перевірці того, чи відповідає впровадження керівництвом рамкам управління ризиками підприємства, а також у нагляді за оперативними заходами з кібербезпеки, такими як перевірка надійності сторонніх постачальників, управління вразливостями, аналіз загроз та протоколи резервного копіювання». *(Ericka Johnson. The Cyber Brief | What Every Board Needs to Know About Cyber Risk Oversight // National Law Forum, LLC (<https://natlawreview.com/article/cyber-brief-what-every-board-needs-know-about-cyber-risk-oversight>). 27.05.2026).*

«Загрози кібербезпеці стають дедалі більш витонченими, частими та важкими для стримування, що зумовлено розвитком технологій та вдосконаленням методів атак. Сьогодні організації стикаються з постійно мінливим середовищем, яке включає кібератаки та засоби захисту на основі штучного інтелекту, програми-вимагачі, вразливості хмарних систем, порушення безпеки ідентифікаційних даних та ризики, пов'язані з використанням сторонніх сервісів. Розуміння цих нових тенденцій є життєво важливим для посилення заходів безпеки, зменшення ризиків та підготовки до майбутніх викликів. У 2026 році провідні тенденції у сфері кібербезпеки підкреслюють інтеграцію штучного інтелекту як в наступальні, так і в оборонні стратегії, причому злочинці використовують інструменти штучного інтелекту для виявлення вразливостей систем, створення переконливих фішингових листів та розробки шкідливого

програмного забезпечення, здатного обходити традиційні засоби захисту. З іншого боку, команди з безпеки використовують штучний інтелект для постійного моніторингу, виявлення незвичайної активності, такої як невдалі спроби входу або незвичайні моделі трафіку, тим самим покращуючи можливості реагування...

Поява «агентного III» — систем, що приймають рішення без контролю з боку людини, — та «тіньового III» — несанкціонованих зовнішніх інструментів, що використовуються в організаціях, — створює нові ризики, пов'язані з контролем даних, управлінням та наглядом. Щоб мінімізувати ці ризики, організації зосереджуються на управлінні III, моніторингу та розробці чітких політик використання. Безпека за принципом «нульової довіри» стала стандартним підходом, що передбачає сувору верифікацію в кожній точці доступу, дозволи на основі ролей, сегментацію мережі та постійний моніторинг активності, особливо з огляду на те, що сучасні робочі середовища передбачають віддалений доступ з різних пристроїв та місць...

Захист ідентифікаційних даних та облікових даних залишається ключовим аспектом кібербезпеки: організації впроваджують більш суворі процедури входу, багатофакторну автентифікацію та моніторинг активності для запобігання несанкціонованому доступу. Хмарні середовища тепер перебувають під постійним наглядом із використанням автоматизованих сповіщень та реагування на підозрілу активність, що сприяє ранньому виявленню та нейтралізації потенційних загроз. Законодавство про захист даних та вимоги регуляторних органів ще більше спонукають організації відповідально поводитися з конфіденційною інформацією, забезпечуючи оперативне повідомлення про інциденти та постійну відповідність нормам.

Загрози від програм-вимагачів перетворилися на цілеспрямовані кампанії, що часто супроводжуються крадіжкою даних та порушенням роботи систем, що змушує компанії вдосконалювати стратегії резервного копіювання та плани реагування на інциденти. Тим часом прогрес у галузі квантових обчислень стимулював підготовку до постквантової криптографії, спрямованої на розробку шифрування, стійкого до майбутніх квантових атак, особливо для забезпечення довгострокової безпеки даних. Дефіцит фахівців у галузі кібербезпеки залишається серйозною проблемою, що змушує організації інвестувати в навчання, залучення зовнішніх експертів та послуги з управління безпекою, щоб заповнити прогалини в кваліфікації...

Крім того, взаємопов'язані ризики, що впливають із вразливостей ланцюгів постачання та сторонніх систем, підкреслюють важливість ретельного управління ризиками, регулярної оцінки вразливостей та посиленого контролю доступу в рамках зовнішніх партнерських відносин. У міру зростання складності та масштабів загроз надзвичайно важливо бути в курсі останніх тенденцій у сфері безпеки. Проактивний підхід, що охоплює модель «нульової довіри», засоби захисту на основі штучного інтелекту, заходи захисту ідентичності, безпеку хмарних середовищ, дотримання нормативних вимог та перспективні технології шифрування, має вирішальне значення для створення стійких і довгострокових систем кіберзахисту. Для фахівців, які прагнуть поглибити свої знання, комплексні навчальні програми з кібербезпеки можуть надати практичні навички, необхідні

для орієнтування в цьому динамічному середовищі та просування по кар'єрних сходах». (*Kusum Saini. Emerging Cybersecurity Trends to Watch Out in 2026 // Simplilearn Solutions (<https://www.simplilearn.com/top-cybersecurity-trends-article>). 25.05.2026*).

«За прогнозами MarketsandMarkets, світовий ринок кібербезпеки в оборонній сфері зросте з приблизно 20,34 млрд доларів у 2026 році до 34,53 млрд доларів до 2031 року, що відповідає середньорічному темпу зростання на рівні 11,2%. Прогноз пов'язує зростання з підвищенням попиту на захист військових ІТ-мереж, систем виконання місій, платформ управління та контролю, а також конфіденційних даних оборонного сектору, оскільки оборонні операції все більше покладаються на хмарні сервіси, підключені датчики, програмно-визначені системи та цифрові ланцюги постачання, що розширюють площу атаки. Уряди реагують на це, інвестуючи в моделі «нульової довіри», шифрування, моніторинг загроз, кіберверифікацію та посилення вимог до безпеки для оборонних підрядників та критичної інфраструктури національної безпеки, що стимулює попит на керовані послуги, операції з безпеки, управління ідентифікацією та доступом, а також захист даних...

Очікується, що на цьому ринку найшвидше зростатиме сегмент послуг (середньорічний темп зростання — 12,0%), тоді як військовий сектор, за прогнозами, залишиться домінуючим кінцевим споживачем із часткою 93,6% у 2026 році; очікується, що сегмент внутрішньої безпеки продемонструє найвищі темпи зростання, оскільки підрозділи прикордонної, берегової та спеціальних операцій збільшують витрати на безпеку мереж, кінцевих точок, хмарних систем та даних, IAM, криптографію та кібертестування для систем спостереження та громадської безпеки. Щодо платформ, очікується, що оборонна промислова база та центри обробки даних займатимуть значну частку, оскільки вони зберігають та обробляють конфіденційні програмні та оперативні дані і потребують комплексного захисту та моніторингу. У регіональному розрізі найшвидше зростання очікується в Європі, оскільки кіберзагрози та гібридні загрози зумовлюють збільшення оборонних бюджетів на кібербезпеку, що підкріплюється визнанням НАТО кіберпростору як оперативної сфери та ініціативами ЄС у сфері кіберзахисту. У звіті наведено перелік основних постачальників у цій галузі, серед яких Booz Allen Hamilton, General Dynamics, Leidos, BAE Systems та CACI...» (*Defense Cybersecurity Market worth \$34.53 billion by 2031 - Exclusive Report by MarketsandMarkets™ // PR Newswire Europe Limited. (<https://www.prnewswire.co.uk/news-releases/defense-cybersecurity-market-worth-34-53-billion-by-2031---exclusive-report-by-marketsandmarkets-302782829.html>). 27.05.2026*).

«Згідно з результатами ринкового дослідження, проведеного компанією Spherical Insights and Consulting, ринок послуг з керованого виявлення та реагування (MDR) зросте з приблизно 4 млрд доларів у 2025 році до близько 16

млрд доларів до 2035 року, що відповідає середньорічному темпу зростання на рівні 13%. Це пов'язано з тим, що кіберзагрози стають дедалі агресивнішими та все частіше базуються на штучному інтелекті, тоді як організації не в змозі забезпечити цілодобовий моніторинг та оперативне реагування лише силами власних внутрішніх команд. Послуги MDR набирають популярності, оскільки забезпечують безперервний моніторинг загроз через центри оперативного реагування (SOC), швидше розслідування та локалізацію інцидентів, вдосконалене виявлення на основі штучного інтелекту та аналізу загроз, а також економічно вигідну альтернативу у вигляді передплати замість створення власних ресурсів, особливо в умовах, коли підприємства розширюють площу атаки через гібридну роботу, хмарні платформи, пристрої Інтернету речей (IoT) та віддалений доступ. Впровадження цих послуг відбувається в секторах, що є об'єктом інтенсивних атак та підлягають суворому регулюванню, таких як охорона здоров'я, фінанси, виробництво, роздрібна торгівля/електронна комерція та державне управління. Ключові тенденції включають виявлення на основі штучного інтелекту, інтеграцію хмарної безпеки, впровадження моделі «нульової довіри», а також посилення автоматизації та координації, причому багато постачальників адаптують свої пропозиції для малих та середніх підприємств...

У звіті також висвітлюються кроки галузі, що відображають це зростання, зокрема розширення компанією Vodafone Business партнерства з Google Cloud для запуску послуги MDR на базі Google Security Operations для європейських малих та середніх підприємств (починаючи з Німеччини) разом із штучним інтелектом-консьєржем на базі Gemini, а також розширення Google Cloud партнерських відносин у сфері телекомунікацій, наприклад із Proximus Global, для підтримки хмарних комунікацій. У звіті проводиться розмежування між MDR та традиційними послугами з керованої безпеки (які більше зосереджуються на використанні інструментів безпеки) та відзначається перехід до більш широких моделей керованого XDR, що інтегрують телеметрію з кінцевих точок, мереж, хмари та електронної пошти для покращення виявлення та реагування. Запуск Acronis нової служби MDR, спрямованої на MSP, наводиться як ще один приклад того, як постачальники створюють масштабовані можливості MDR на основі штучного інтелекту та автоматизації, щоб допомогти постачальникам послуг забезпечити безперервний моніторинг, швидше реагування, зменшення операційної складності та більшу стійкість для клієнтів, які стикаються зі зростаючими загрозами від програм-вимагачів, фішингу та хмарних загроз...» (*Why MDR Services Are Becoming Essential for Modern Cyber Defense: Expert View by Spherical Insights // Spherical Insights* (<https://www.sphericalinsights.com/blogs/why-mdr-services-are-becoming-essential-for-modern-cyber-defense>). 05.2026).

«У міру поширення цифрової трансформації та зростання таких загроз, як програми-вимагачі, атаки з використанням штучного інтелекту, вразливості хмарних систем та витоки даних, у 2026 році організації інвестують значні кошти в кіберзахист, що робить кібербезпеку однією з найдинамічніших та найпривабливіших сфер професійної діяльності... Посади, на які існує високий

попит: аналітики з кібербезпеки, які моніторять мережі та реагують на інциденти практично в усіх секторах; етичні хакери або тестувальники на проникнення, які проактивно виявляють вразливості в додатках та інфраструктурі; інженери з хмарної безпеки, які розробляють та захищають архітектури на таких платформах, як AWS, Azure та Google Cloud; а також фахівці з безпеки штучного інтелекту, які захищають системи штучного інтелекту від маніпуляцій, одночасно створюючи інтелектуальні засоби виявлення для протидії дедалі більш автоматизованим зловмисникам... Також відзначається зростання попиту на фахівців з цифрової криміналістики, які аналізують випадки порушення безпеки та відновлюють докази для правоохоронних органів і корпоративних справ, на архітекторів безпеки, які розробляють стратегію корпоративної безпеки та стійку інфраструктуру, а також на керівників служб інформаційної безпеки (CISO), які керують управлінням ризиками та дотриманням нормативних вимог на рівні вищого керівництва. Загалом привабливість кар'єри у сфері кібербезпеки зумовлена високою заробітною платою, глобальним попитом, можливістю дистанційної роботи, постійним навчанням та довгостроковою стабільністю, оскільки кібербезпека стає основною бізнес-необхідністю, а не нішевою ІТ-функцією». *(Naveen Goud. Top Irresistible Cybersecurity Jobs in 2026 // Cybersecurity Insiders (<https://www.cybersecurity-insiders.com/top-irresistible-cybersecurity-jobs-in-2026/>). 27.05.2026).*

Сполучені Штати Америки

«У новому звіті Управління генерального інспектора Міністерства внутрішньої безпеки (DHS) виявлено значні недоліки в системі кібербезпеки Управління розвідки та аналізу цього відомства, зокрема ризики, пов'язані з використанням службових смартфонів у 2023 та 2024 роках. Розслідування показало, що розроблені DHS додатки, широко розповсюджені в публічних магазинах додатків і завантажені близько 375 000 разів службами екстреної допомоги, містили вразливості безпеки. Також було виявлено, що 76% додатків, встановлених на смартфонах співробітників розвідки, були заборонені через властиві їм ризики безпеки або тому, що вони дозволяли здійснювати заборонені дії, зокрема використання сторонніх VPN, платформ для обміну приватними повідомленнями, сервісів потокового відео та ігор...

У звіті містилося застереження, що дозвіл на використання таких додатків може дати зловмисникам можливість виконувати шкідливий код, отримувати доступ до конфіденційних даних або порушувати безпеку систем DHS. Крім того, відомство вело облік лише 11% смартфонів, виданих співробітникам розвідувальних підрозділів, а під час більшості перевірених закордонних поїздок не дотримувалися належних протоколів безпеки щодо використання пристроїв за кордоном. Наглядний орган попередив, що скомпрометовані мобільні пристрої можуть бути використані для прослуховування через камери, мікрофони або GPS, або для здійснення атак на мережі DHS. DHS погодився з рекомендаціями

генерального інспектора і заявив, що планує вирішити ці проблеми до січня 2027 року, тоді як речник відомства пов'язав ці вразливості з діяльністю попередньої адміністрації...» (*Jackie Llanos. Inspector General Says DHS Staff Risked Cyberattacks With Government Smartphones // NOTUS* (<https://www.notus.org/us-news/homeland-security-risked-cyberattacks-internal-watchdog-vulnerabilities-audit-biden-trump>). 04.05.2026).

«...У зв'язку з тим, що федеральний уряд, зокрема CISA, суттєво скоротив свій бюджет та підтримку місцевих ініціатив у сфері кібербезпеки, утворився небезпечний вакуум, через що організації з обмеженими ресурсами, такі як муніципалітети, школи та некомерційні організації, змушені самотійно захищатися від руйнівних кібератак. Цей відхід убік відкрив шлях для незалежних організацій, таких як Центр довгострокової кібербезпеки (CLTC) Каліфорнійського університету в Берклі, які можуть втрутитися та надати критично важливу практичну допомогу. CLTC визнає, що менші організації, які все частіше стають мішенями як для складних програм-вимагачів, так і для простих шахрайських схем, таких як підроблені рахунки-фактури, не мають ресурсів для придбання дорогих засобів безпеки і натомість потребують безпосередньої людської підтримки... Завдяки таким ініціативам, як студентські консультаційні центри з кібербезпеки, CLTC пропонує безкоштовні оцінки вразливості, фактично надаючи послуги, які в іншому випадку були б фінансово недоступними. Шляхом створення коаліцій, проведення досліджень та просування загальногалузових стандартів безпеки серед постачальників EdTech, CLTC вирішує важливе завдання «останньої милі» кібербезпеки, підкреслюючи, що захист організацій на рівні місцевих громад має вирішальне значення для національної безпеки в цілому...» (*Arielle Waldman. Research Hub Bridges Cybersecurity Gap for Under-Resourced Organizations // TechTarget, Inc.* (<https://www.darkreading.com/cyber-risk/research-hub-bridges-cybersecurity-gap-organizations>). 05.05.2026).

«Опитування, проведене у грудні 2025 року серед 212 осіб, відповідальних за прийняття рішень у сфері кібербезпеки в уряді США — на замовлення компаній Carahsoft і Broadcom та за участю Forrester Consulting — свідчить про те, що державний сектор стикається з труднощами в управлінні складними цифровими середовищами після скорочення бюджетів та штату на початку 2025 року. Дослідження виявило поширену фінансову нестабільність: 38% бюджетів відомств класифіковано як переважно або повністю нестабільні, а понад половина респондентів повідомила, що обмеження помірковано або значно погіршили їхню здатність підтримувати основні операції з безпеки. Як наслідок, лише 38% керівників відчувають впевненість у своєму рівні безпеки... Дефіцит ресурсів помітно погіршив ефективність роботи: приблизно 60% респондентів повідомляють про частіші інциденти безпеки, 65% зазначають, що середній час усунення інциденту (MTTR) погіршився, а 86% очікують зростання кількості порушень безпеки протягом наступного року, причому найбільш гострі проблеми з

уразливістю спостерігаються у сферах мережевої безпеки, захисту даних та реагування на інциденти. Щоб пристосуватися до, ймовірно, тривалого періоду обмежених ресурсів, відомства надають пріоритет захисту критичної інфраструктури та впровадженню штучного інтелекту... Розуміючи, що просто найняти більше співробітників не вирішить проблему, 72% респондентів готові впроваджувати засоби автоматизації для виконання таких завдань, як аналіз мережевого трафіку, перевірка відповідності політикам безпеки та сортування сповіщень, що дозволить зменшити виснаження персоналу та дасть змогу меншим командам зосередитися на найбільш ймовірних загрозах, таких як витік даних. Поряд з штучним інтелектом та автоматизацією, Forrester рекомендує агентствам консолідувати свої стеки безпеки, щоб усунути надмірне розширення інструментарію та впровадити уніфіковані платформи, перепроєктувавши свої операційні моделі для досягнення більш адаптивного, масштабованого та стійкого стану безпеки, який працює ефективніше з наявними ресурсами». **(Brian Snell. Doing More with Less: How Government Agencies are Rethinking Cybersecurity // Broadcom (https://www.security.com/expert-perspectives/government-agencies-rethinking-cybersecurity). 07.05.2026).**

«Попит на консультантів з кібербезпеки стрімко зростає на тлі поширення кіберзлочинності та випадків порушення безпеки, які обходяться організаціям у великі кошти, а іноді становлять загрозу для безпеки. Прогнози Бюро статистики праці США показують, що кількість вакансій аналітиків з інформаційної безпеки зросте майже на 30% до 2034 року, тоді як Statista повідомляє про понад 15 мільйонів випадків кіберзлочинності у всьому світі у 2024 році та понад 10 трильйонів доларів, що витрачаються щорічно на усунення збитків від кіберзлочинності, часто спричинених фішингом, спуфінгом, вимаганням та порушеннями безпеки даних; реальні наслідки можуть виходити за межі втрати даних, як, наприклад, у випадку в США, де були виведені з ладу скомпрометовані алкотестери в автомобілях, що призвело до того, що водії залишилися без допомоги... Щоб допомогти кандидатам виділитися серед інших, IEEE Computer Society опублікувала 23-сторінковий посібник про те, що робить консультанта з кібербезпеки успішним, у якому містяться поради практикуючого фахівця Джона Д. Джонсона та наукового дослідника Рікардо Дж. Родрігеса. У посібнику наголошується, що сильні консультанти потребують як твердих навичок — широких знань в галузі ІТ (операційні системи, протоколи, мережева архітектура, програмування на таких мовах, як C++, Java та Python), а також навичок у сфері безпеки, таких як аудит, управління брандмауерами, тестування на проникнення, шифрування та етичний хакінг, — так і м'яких навичок, таких як критичне мислення, управління проектами, гнучкість, робота в команді та чітка комунікація, оскільки консультанти повинні пояснювати ризики та рішення і часто очолюють різноманітні команди клієнтів. У ньому також висвітлюються сучасні інструменти та тенденції, що формують цю галузь, зокрема платформи SOAR для автоматизації робочих процесів та реагування, DNSSEC для посилення автентичності DNS, а також зростаюче використання штучного інтелекту, блокчейну та квантових

обчислень у сфері оборони, причому очікується, що штучний інтелект покращить аналіз даних... Сертифікати розглядаються як основний доказ професійної компетентності, а також надаються рекомендації щодо узгодження кваліфікації з кар'єрними цілями та прогалинами в навичках; серед прикладів — CISM, CCSP, CEH та OSCP, при цьому іноді можуть знадобитися додаткові галузеві сертифікати. Наостанок у посібнику рекомендується бути в курсі останніх тенденцій та розбудовувати мережі контактів за допомогою конференцій та спільнот IEEE, а також інших навчальних ресурсів, публікацій та наукових бібліотек IEEE». **(Kathy Pretz. Learn What It Takes to Become a Cybersecurity Consultant // IEEE (<https://spectrum.ieee.org/ieee-guide-cybersecurity-consultant>). 06.05.2026).**

«Коли державні органи та приватні організації стають жертвами кібератак, чиновники часто називають це надзвичайними ситуаціями та обіцяють оперативне усунення загрози, проте нещодавнє опитування, проведене Національною асоціацією головних інформаційних директорів штатів (NASCIO) та компанією Deloitte, викриває глибшу й тривожну реальність: лише 26% головних директорів з інформаційної безпеки штатів (CISO) впевнені у своїй здатності захиститися від кіберзагроз. Майже три чверті цих ключових керівників визнають, що вони недостатньо підготовлені до протидії сучасним цифровим атакам, і ця вразливість значною мірою зумовлена зростаючою витонченістю кіберзагроз та появою генеративного штучного інтелекту (Gen AI)... Кіберзлочинці, зокрема іноземні суб'єкти, що діють за підтримки держав, використовують штучний інтелект для автоматизації атак, створення переконливих фішингових кампаній та експлуатації вразливостей з безпрецедентною швидкістю, що скорочує час на виявлення та реагування до меж, які перевищують людські можливості. Цю технологічну відсталість поглиблює постійний брак фінансування; державні бюджети на кібербезпеку постійно відстають від потреб у захисті, оскільки пріоритет надається іншим сферам, таким як охорона здоров'я та освіта... Ця фінансова напруга посилюється через припинення дії федеральних програм допомоги у зв'язку з COVID-19, які тимчасово підтримували ініціативи у сфері кібербезпеки, а також через постійний глобальний економічний та геополітичний тиск і невизначеність щодо продовження дії Програми грантів на підтримку кібербезпеки на державному та місцевому рівнях. Відповідно, у той час як кіберзагрози стрімко розвиваються, готовність захисників до боротьби з ними гальмується, а це означає, що без збільшення інвестицій, посилення політичної підтримки та швидшої адаптації до таких технологій, як штучний інтелект, критично важливі системи ставатимуть дедалі вразливішими, оскільки розрив між зловмисниками та захисниками продовжує збільшуватися». **(Naveen Goud. State Cybersecurity officials not fully prepared for Cyber Attacks // Cybersecurity Insiders (<https://www.cybersecurity-insiders.com/state-cybersecurity-officials-not-fully-prepared-for-cyber-attacks/>). 05.05.2026).**

«Оскільки галузь кібербезпеки стикається зі зростаючим дефіцитом кваліфікованих кадрів, багато коледжів та університетів США заповнюють прогалини в досвіді кандидатів на посади початкового рівня, інвестуючи в центри оперативної безпеки (SOC), якими керують самі студенти. Ці центри надають студентам безцінний практичний досвід, дозволяючи їм здійснювати моніторинг мереж, розслідувати підозрілу активність та реагувати на реальні інциденти ще до закінчення навчання. Моделі функціонування цих програм значно різняться: тоді як такі навчальні заклади, як Університет Північної Флориди та Університет штату Луїзіана, використовують структуровані, прогресивні програми навчання, в рамках яких студенти проходять шлях від спостереження за роботою персоналу до сортування інцидентів, інші — наприклад, Каліфорнійський політехнічний університет у Помоні — працюють більш гнучко завдяки ініціативам під керівництвом волонтерів, пов'язаним із клубами з кібербезпеки...

Сфера діяльності цих центрів SOC також різниться залежно від навчального закладу. Деякі з них зосереджуються виключно на захисті внутрішніх мереж кампусу, тоді як інші розширили свою діяльність, щоб обслуговувати регіональних партнерів, зокрема некомерційні організації, органи місцевого самоврядування та шкільні округи, яким часто бракує коштів на виділення коштів на спеціальні служби безпеки. Такі зовнішні партнерства, до яких іноді залучаються приватні компанії або Національна гвардія, дають студентам можливість ознайомитися з ширшим спектром загроз та програмним забезпеченням корпоративного рівня. У рамках цих програм адміністратори наголошують на поєднанні технічних навичок, таких як аналіз журналів, пошук загроз та реагування на інциденти, та необхідних м'яких навичок, таких як документація та комунікація. Крім того, ці центри все частіше використовують інструменти штучного інтелекту, що дозволяє студентам разом зі своїми колегами вивчати найсучасніші технології захисту. Надаючи випускникам портфоліо, що базуються на показниках, галузеві сертифікати та реальний досвід роботи, ці програми виявилися надзвичайно успішними: учасники отримують посади у провідних технологічних компаніях, а деякі програми демонструють майже ідеальні показники працевлаштування». *(Abby Sourwine. Universities Turn SOC's Into Cybersecurity Career Pipelines // e.Republic LLC (<https://www.govtech.com/education/higher-ed/universities-turn-socs-into-cybersecurity-career-pipelines>). 08.05.2026).*

«Білий дім закликає Конгрес продовжити дію Закону про обмін інформацією з питань кібербезпеки 2015 року, який було тимчасово відновлено в рамках пакету тимчасового фінансування, але термін дії якого закінчиться у вересні 2026 року, якщо його не буде продовжено. Закон, дія якого на короткий час припинилася під час 43-денного закриття уряду минулого року, перш ніж його було продовжено, забезпечує правовий захист, що дозволяє приватним компаніям обмінюватися інформацією про кіберзагрози з федеральними агентствами, навіть якщо дані можуть містити конфіденційну інформацію про жертв або компанії... Національний директор з питань кібербезпеки Шон Кернкросс заявив на виставці AI+ Expo у Вашингтоні, що адміністрація Трампа

прагне отримати довгострокове продовження повноважень у рамках ширшої стратегії кібербезпеки, яка передбачає прискорення двостороннього обміну інформацією між державним і приватним секторами та посилення наступальних заходів з метою зриву роботи мереж супротивників. У минулому ця концепція була політично суперечливою через побоювання щодо конфіденційності, що посилювалися після розкриттів Сноудена у 2013 році, але підтримка зросла після того, як у 2015 році внаслідок злом Управління кадрового менеджменту були оприлюднені дані про понад 21 мільйон федеральних службовців». (*Edward Graham, David DiMolfetta. Trump admin will push for 'long-term' reauthorization of key cyber data-sharing law // Government Media Executive Group LLC. (https://www.nextgov.com/cybersecurity/2026/05/trump-admin-will-push-long-term-reauthorization-key-cyber-data-sharing-law/413395/). 07.05.2026*).

«Ситуація у сфері кібербезпеки для федеральних підрядників США зазнала кардинальних змін у зв'язку із впровадженням програми сертифікації за Моделлю зрілості кібербезпеки (СММС), яка набула чинності для контрактів 10 листопада 2025 року. Ця програма відходить від попередньої моделі самосертифікації та тепер вимагає від підрядників, які працюють з контрольованою несекретною інформацією (CUI), отримання обов'язкової сертифікації від незалежної сторони, що робить кібербезпеку обов'язковою умовою для участі в тендерах... Ця зміна в законодавстві супроводжується різким зростанням кількості випадків притягнення до відповідальності за Законом про неправдиві заяви (FCA): лише у 2025 фінансовому році Міністерство юстиції домоглося виплати понад 52 мільйонів доларів у рамках угоди про врегулювання справ щодо кібершахрайства — це втричі більше, ніж два роки тому. Ці угоди ґрунтуються не на фактах витоку даних, а на невідповідності між заявленим рівнем безпеки підрядника та його фактичними практиками... Оскільки вимоги щодо дотримання нормативних вимог поширюються на всіх субпідрядників, а інвестори з сектору приватного капіталу несуть відповідну відповідальність, для керівників підприємств все зрозуміло: СММС — це не просто формальність, а важлива передумова для отримання федеральних контрактів, і відмова від інвестицій у реальну підготовку створює значні юридичні та комерційні ризики». (*What Business Leaders Need to Know About Cybersecurity Certification and Enforcement in 2025–2026 // Shumaker, Loop & Kendrick, LLP. (https://www.shumaker.com/insight/what-business-leaders-need-to-know-about-cybersecurity-certification-and-enforcement-in-2025-2026/). 08.05.2026*).

«Президент Дональд Трамп заявив, що він та президент Китаю Сі Цзіньпін обговорили питання кібератак та шпигунства під час двосторонньої зустрічі цього тижня. Трамп повідомив журналістам, що обидві країни займаються хакерством та шпигунством, натякнувши на взаємну обізнаність щодо таємної діяльності, хоча конкретні операції не називалися. Його коментарі пролунали на тлі посилення занепокоєння щодо ймовірних вторгнень Китаю в

телекомунікаційні мережі, урядові системи та критичну інфраструктуру США, зокрема діяльності, яку приписують групі Volt Typhoon і яка, за словами чиновників, має на меті підготовку до потенційного порушення роботи таких служб, як електромережі та водоочищення, у разі надзвичайної ситуації на Тайвані, хоча Трамп зазначив, що не може підтвердити ці твердження. Ці заяви є надзвичайно відкритим визнанням наступальних та розвідувальних операцій США проти Китаю і відображають дипломатичну позицію, яка визнає складність встановлення відповідальності за кібероперації, водночас натякаючи на мовчазне визнання Пекіном спроб проникнення в кіберпростір, незважаючи на регулярні заперечення з боку Китаю. Ширший контекст включає зусилля розвідки США з вербування китайських чиновників, повідомлення про підозри щодо спроб Китаю налагодити контакти з колишніми співробітниками уряду США, а також тиск адміністрації Трампа на посилення позиції щодо іноземних хакерів, що стимулює попит на наступальні кіберможливості, які прямо розглядаються як інструмент нової стратегії боротьби з тероризмом». *(David DiMolfetta. Trump says he and Xi discussed cyberattacks and spying between US, China // Government Media Executive Group LLC. (<https://www.nextgov.com/cybersecurity/2026/05/trump-says-he-and-xi-discussed-cyberattacks-and-spying-between-us-china/413582/>). 15.05.2026).*

«Кілька провідних телекомунікаційних компаній США, серед яких AT&T, Charter, Comcast, Cox, Lumen, T-Mobile, Verizon та Zayo, заснували новий галузевий орган з обміну інформацією про кібербезпеку — Центр обміну та аналізу інформації з кібербезпеки в сфері комунікацій (C2 ISAC). Про це було оголошено у вівторок на тлі того, як галузь продовжує стикатися з постійними загрозами, про які наочно свідчить масштабна китайська хакерська кампанія «Salt Typhoon». Головою правління нової групи стане директор з інформаційної безпеки AT&T Річ Байч, а виконавчим директором — колишня співробітниця CISA/FBI Валері Мун. Члени групи стверджують, що жоден оператор окремо не має повного уявлення про мінливі загрози і що обмін досвідом та оперативною інформацією покращить виявлення та реагування на них... Цей крок став наслідком інформації про те, що угруповання Salt Typhoon здійснило атаки на декількох телекомунікаційних провайдерів у США та за кордоном, зламало системи законного перехоплення, що використовуються для стеження за рішенням суду, і, за повідомленнями, діє щонайменше з 2019 року, при цьому немає чіткого публічного підтвердження того, що зловмисників було повністю усунено; ймовірний злом системи стеження ФБР на початку цього року, пов'язаний, як підозрюють, із Китаєм, також міг призвести до витоку телефонних номерів об'єктів стеження. Створення незалежного ISAC є значущим, враховуючи, що раніше група з обміну інформацією щодо безпеки комунікацій існувала в рамках CISA — агентства, яке зазнає скорочення штату, — і це відбувається в той час, коли федеральні агентства продовжують зусилля з виявлення та мінімізації ризиків, пов'язаних з телекомунікаційним та спостережним обладнанням, пов'язаним з Китаєм, причому у звіті GAO зазначається, що Міністерства оборони та енергетики виявили деякі вразливі пристрої та працюють над їх усуненням». *(David DiMolfetta.*

Telecom firms form new cyber information-sharing group // Government Media Executive Group LLC (<https://www.nextgov.com/cybersecurity/2026/05/telecom-firms-form-new-cyber-information-sharing-group/413636/>). 19.05.2026).

«Нове опитування 200 керівників у сфері кібербезпеки в США показало, що відступи від вимог безпеки та нормативних стандартів стали стандартною практикою в організаціях, що значно підвищує як бізнес-ризик, так і ризик кібербезпеки. Опитування, проведене компанією Opinion Matters на замовлення Replica Cyber, показало, що кожна організація (100%) зробила принаймні одне виключення з правил безпеки або дотримання вимог за останні 12 місяців. Хоча 63% з них були офіційними, 36% вирішувалися за допомогою неофіційних обхідних шляхів, що викликає занепокоєння щодо непослідовності нагляду та прихованих вразливостей...»

Дослідження показує, що багато винятків, які спочатку планувалося зробити тимчасовими, швидко стають постійними. Типовим прикладом є надання маркетинговим командам постійних винятків на використання ризикованих інструментів штучного інтелекту з відкритим кодом з міркувань підвищення продуктивності, незважаючи на відомі проблеми безпеки. Опитування показує, що чим вищим є керівник, який просить про виняток, тим більша ймовірність його затвердження, що часто створює негативний прецедент, який поширюється по всій організації. В результаті, командам з кібербезпеки, що не мають достатніх ресурсів, доводиться самотійно справлятися зі зростаючим ризиком, часто виявляючи тіньові IT-ініціативи лише після того, як винятки вже були зроблені...

Наслідки виходять за межі сфери управління. Майже 40% респондентів повідомили, що їхні організації відклали або скасували плани з розширення ринків, виведення продуктів на ринок, злиття та поглинання або впровадження штучного інтелекту через неможливість безпечної реалізації цих ініціатив, при цьому 20% зазначили, що в деяких випадках проекти з високим рівнем ризику були скасовані взагалі. Отримані дані вказують на поширену організаційну культуру, яка послідовно ставить швидкість, продуктивність та гнучкість бізнесу вище за політику безпеки, залишаючи команди з кібербезпеки вирішувати наслідки таких рішень». **(Mike Vizard. Security exceptions are increasing cybersecurity risk, survey finds // Barracuda Networks, Inc. (<https://blog.barracuda.com/2026/05/20/security-exceptions-cybersecurity-risk>). 20.05.2026).**

«Нове дослідження компанії QBE North America, проведене на основі опитування 400 керівників у сферах IT, адміністрації та страхування в американських компаніях зі штатом від 100 до 2 000 співробітників, показує, що дві третини американських підприємств зазнали кіберінциденту протягом минулого року, причому більше половини з них повідомили про прямі фінансові збитки внаслідок цього. Результати дослідження малюють картину загроз, які стали скоріше звичним явищем, ніж винятком: кожна четверта компанія зазнала перебоїв у роботі, що тривали більше одного повного робочого дня.

Примітно, що 58% постраждалих компаній пов'язали принаймні одну атаку з постачальником або стороннім підрядником, що підкреслює, як швидко кіберризика можуть поширюватися у взаємопов'язаних бізнес-екосистемах... З огляду на майбутнє, занепокоєння щодо загроз залишається високим: 77% респондентів висловили стурбованість щодо кіберзагроз, з якими, на їхню думку, їм доведеться зіткнутися протягом наступних дванадцяти місяців, а три з чотирьох планують відповідно збільшити бюджети на кібербезпеку, причому 29% розраховують збільшити витрати більше, ніж на рівень інфляції. Штучний інтелект змінює ландшафт загроз у двох напрямках одночасно. Хоча 81% підприємств вже використовують ШІ переважно для підвищення продуктивності та операційної ефективності, а 92% очікують, що це матиме позитивний вплив протягом двох років, ця ж технологія стає значним вектором атак. Майже кожна десята компанія повідомила про принаймні один інцидент, у якому, як вважається, відіграв роль ШІ, найчастіше через фішингові повідомлення з використанням ШІ, про що зазначили 51% постраждалих компаній, або через шкідливе програмне забезпечення та зловмисний код, згенеровані ШІ, про що зазначили 49%... Ризики, пов'язані з використанням штучного інтелекту постачальниками, також викликають дедалі більшу стурбованість: 70% підприємств переймаються потенційними ризиками, що виникають у результаті використання штучного інтелекту їхніми постачальниками. Незважаючи на зростання обізнаності та обсягів інвестицій, у готовності до таких ситуацій залишаються значні прогалини. Лише 67% середніх підприємств мають кіберстрахування, тоді як 24% взагалі не мають страхового покриття, і хоча 81% повідомляють про наявність офіційного плану реагування на інциденти, 15% визнають, що такого плану не мають, що залишає значну частину компаній без структурованого плану дій на випадок атаки. Серед підприємств, які вже використовують ШІ, 60% проводять навчання персоналу щодо його безпечного використання, а 53% перевіряють якість даних, що використовуються для навчання їхніх моделей, але, можливо, темпи управління ризиками доведеться прискорити, щоб не відставати від темпів впровадження ШІ та ускладнення атак із використанням ШІ. Загальна картина свідчить про те, що середні підприємства США перебувають на переломному етапі: вони все більше усвідомлюють кіберризика та починають інвестувати в засоби захисту, але ще не повністю захищені від загроз, які швидко поширюються та еволюціонують». *(Majority of Businesses Faced Cyber Events Last Year as AI-Enabled Attacks Rise // Risk & Insurance® (<https://riskandinsurance.com/majority-of-businesses-faced-cyber-events-last-year-as-ai-enabled-attacks-rise/>). 26.05.2026).*

«Законодавці-республіканці з Підкомітету з кібербезпеки та захисту інфраструктури Комітету з внутрішньої безпеки Палати представників попередили, що органи влади штатів та місцеві органи влади стикаються з ситуацією, коли кіберзагрози стрімко зростають. Причиною цього є угруповання, що використовують програми-вимагачі, державні суб'єкти з Китаю, Росії та Ірану, а також дедалі більш витончені атаки з використанням штучного інтелекту, спрямовані проти шкіл, муніципалітетів, служб екстреної допомоги,

транспортних систем та критичної інфраструктури. Під час слухань під головуванням конгресмена Енді Оглеса свідки, серед яких були керівники інформаційних служб штатів Теннессі, Нью-Йорк та Флорида, а також експерти з питань політики з Центру демократії та технологій, наголосили на серйозній асиметрії між передовими можливостями супротивників та обмеженою кількістю персоналу з кібербезпеки, застарілою інфраструктурою та обмеженими бюджетами, з якими стикаються багато місцевих органів влади...

Під час слухань було підкреслено, що штучний інтелект одночасно підвищує оборонні можливості, такі як виявлення загроз, і водночас дає зловмисникам змогу автоматизувати фішинг, прискорювати виявлення вразливостей, масштабувати операції та переміщатися по системах у поперечному напрямку за лічені секунди. Свідки наголосили, що федеральна підтримка залишається надзвичайно важливою, зокрема через Програму грантів на кібербезпеку для штатів та місцевих органів влади (SLCGP), дія якої закінчується у вересні, якщо її не буде продовжено. Вони закликали Конгрес ухвалити закон PILLAR, зменшити тягар розподілу витрат для менших та сільських юрисдикцій, спростити адміністрування, розширити доступ до інформації про загрози через CISA, відновити фінансування таких програм, як MS-ISAC, та розробити кращу підтримку щодо ризиків, пов'язаних зі штучним інтелектом, операційними технологіями та безпекою ланцюгів постачання...

Законодавці та свідки погодилися з тим, що, хоча багато штатів розробили інноваційні загальнодержавні стратегії, системи спільного використання ресурсів, програми підготовки кадрів та моделі обміну інформацією, ці зусилля не можуть повністю подолати дефіцит ресурсів без сталого та передбачуваного партнерства з федеральним урядом. У свідченнях наголошувалося, що кібератаки на органи державної та місцевої влади мають серйозні реальні наслідки, зокрема витік конфіденційних даних громадян, порушення роботи життєво важливих служб та більш широкі наслідки для національної безпеки, що робить постійні федеральні інвестиції та координацію не просто корисними, а й необхідними». (*Anna Ribeiro. House Republicans scrutinize escalating ransomware, nation-state, AI-driven cyber threats targeting state and local governments // Industrial Cyber (https://industrialcyber.co/threat-landscape/house-republicans-scrutinize-escalating-ransomware-nation-state-ai-driven-cyber-threats-targeting-state-and-local-governments/). 26.05.2026*).

Країни ЄС та Великобританія

«Згідно з оцінками дослідження KPMG, проведеного на замовлення Китайської торгової палати при ЄС (CCCEU), поступове витіснення китайських постачальників із 18 критично важливих секторів відповідно до запропонованого ЄС переглянутого Закону про кібербезпеку обійдеться в 367,8 млрд євро (432,8 млрд доларів) у період з 2026 по 2030 рік. Заплановані правила перетворять існуючі м'які обмеження щодо «високоризикових» постачальників, таких як Huawei та ZTE, на обов'язковий режим, що вимагатиме вилучення

компонентів від визначених постачальників з ключової інфраструктури — включаючи енергетику, транспорт, охорону здоров'я, банківську справу, цифрові мережі та космічну галузь — протягом 36 місяців, із застосуванням штрафних санкцій за невиконання вимог. Згідно з дослідженням, витрати будуть пов'язані з заміною інфраструктури, перебоями в роботі, втратами взаємодії та впливом на продуктивність у наступних ланках ланцюга постачання, якщо припустити, що китайське обладнання буде замінено європейськими, японськими або корейськими альтернативами; ССCEU розглядає цю оцінку як мінімальну, а не максимальну...

Оскільки дослідження було проведено на замовлення організації, що представляє комерційні інтереси Китаю, наведена цифра, ймовірно, відображає пропагандистську позицію, і майбутня оцінка впливу, яку проведе Європейська комісія, може дати нижчу оцінку. Проте аналітики зазначають, що загальний обсяг є цілком ймовірним, зважаючи на масштаби проникнення китайських постачальників у такі сфери, як телекомунікаційне обладнання, традиційні напівпровідники, обладнання для електромереж та залізнична сигналізація, де альтернативи можуть бути обмеженими або дорогими. Дебати щодо витрат розгортаються на тлі більш широких зусиль ЄС, спрямованих на зміцнення технологічного суверенітету та посилення безпеки ланцюгів постачання, тоді як Китай прагне зберегти доступ своїх компаній до ринку. Подальша доля пропозиції залежатиме від власного аналізу витрат, проведеного Комісією, від того, чи приймуть країни-члени, що зазнають значного впливу, такі як Німеччина, суворі терміни виведення обладнання — зокрема обладнання Huawei з мереж 5G — та чи відповість Пекін комерційними контрзаходами. Незалежно від остаточної цифри, дослідження KPMG визначило початкові умови того, що, ймовірно, стане значною політичною та економічною дискусією в ЄС». *(Ana-Maria Stanciuc. Chinese chamber of commerce puts a \$432bn price tag on the EU's cybersecurity overhaul // Cogneve, INC. (<https://thenextweb.com/news/eu-cybersecurity-china-suppliers-432-billion-cost-study>). 06.05.2026).*

«Десятки європейських законодавців з різних політичних таборів закликають Європейську комісію вжити негайних заходів для захисту кібербезпеки континенту від загрози, яку становлять нові високопродуктивні моделі штучного інтелекту. У листі, адресованому Хенні Вірккунен, виконавчій віцепрезиденті з питань технологічного суверенітету та безпеки, депутати Європарламенту попередили, що моделі ШІ, такі як Mythos від Anthropic — яку компанія не випустила у загальний доступ через її хакерські можливості — «кардинально змінюють ландшафт кібератак». Вони висловили занепокоєння з приводу повідомлень про те, що сторонні особи отримали доступ до Mythos, зазначивши, що Європа не готова до цього і що жодна інституція ЄС ще не отримала доступу до «Project Glasswing» від Anthropic — закритої коаліції з раннього доступу... Законодавці наголосили, що загроза виходить за межі Mythos, оскільки інші нові моделі та їхні аналоги з відкритим кодом (наприклад, Kimi K2.6) у поєднанні з агентурними системами можуть знизити бар'єр для здійснення складних атак на державні служби та критичну інфраструктуру. У листі міститься

заклик до Комісії забезпечити участь ЄС у проєкті Glasswing, прискорити впровадження архітектур «нульової довіри» та засобів захисту з використанням ШІ, реформувати процедури розкриття вразливостей та виправлення помилок, щоб вони відповідали швидкості роботи ШІ, а також сприяти зменшенню площі атаки та сегментації мережі; що важливо, у листі підкреслюється, що це не закликає до обмеження використання ШІ у сфері кібербезпеки, яке залишається незамінним. Паралельно з цим президент Єврогрупи Кіріакос П'єракакіс попередив, що передові моделі ШІ можуть становити системні виклики. Поява Mythos потрясла світових політиків: як повідомляється, адміністрація Трампа переглядає свою політику невтручання і може запровадити офіційну процедуру урядового контролю після отримання доступу до системи від Google DeepMind, Microsoft та xAI ще до її розгортання; Британський Інститут безпеки штучного інтелекту, який отримав ранній доступ до Mythos, виявив, що система здатна самостійно атакувати слабо захищені системи; а Національна служба охорони здоров'я Англії тимчасово заблокувала свої репозиторії з відкритим кодом на GitHub, щоб оцінити вплив цих стрімких розробок у сфері штучного інтелекту». (*David Meyer. European MEPs Push for Stronger Post-Mythos Cybersecurity // Information Security Media Group, Corp.* (<https://www.bankinfosecurity.com/european-meps-push-for-stronger-post-mythos-cybersecurity-a-31599>). 05.05.2026).

«Опитування щодо кіберінцидентів у Великій Британії, проведене на замовлення Департаменту з питань цифрових технологій, інфраструктури та транспортних систем (DSIT) та Міністерства внутрішніх справ, показує, що кількість кіберінцидентів зростає і все більше впливає на формування бізнес-стратегії: 43% підприємств та 28% благодійних організацій повідомили про порушення безпеки або атаки протягом останнього року. Великі організації стають об'єктом атак непропорційно частіше — 69% великих компаній та 65% середніх підприємств повідомили про інциденти, порівняно з 46% малих та 42% мікропідприємств, — що свідчить про те, що ризик зростає у міру розширення компаній, а кіберстійкість стає ключовим компонентом сталого зростання... Керівництво компаній дедалі частіше надає цьому питанню пріоритетного значення: 72% підприємств і 60% благодійних організацій вважають кібербезпеку одним із найважливіших пріоритетів (серед великих організацій цей показник становить 100%), проте експерти застерігають, що така прихильність має втілюватися у перевірених оперативних готовностях, особливо з огляду на те, що впровадження штучного інтелекту розширює площину атаки, а багато компаній, які вивчають можливості ШІ, не мають належних систем безпеки. Фішинг залишається домінуючою та найбільш руйнівною загрозою, яка зачіпає 38% підприємств та 25% благодійних організацій і яку 69% тих, хто зазнав атак, оцінюють як найбільш руйнівну, причому фішинг, генерований ШІ, ще більше підвищує рівень витонченості та масштаб атак. Хоча багато організацій використовують такі засоби захисту, як шифрування чи анонімізація, значна частина з них все ще зберігає незахищені персональні дані, що створює ризики як з точки зору дотримання нормативних вимог, так і з комерційної точки зору; при цьому фінансові збитки від

інцидентів, про які повідомляється, зросли більш ніж удвічі порівняно з минулим роком (з 2% до 5%), а репутаційні збитки також збільшилися (з 1% до 3%). Ризики ланцюга поставок є значною «сліпою зоною»: лише 15% підприємств аналізують кіберризики від безпосередніх постачальників і лише 6% оцінюють ширші ланцюги поставок, незважаючи на факти гучних порушень безпеки у сторонніх організаціях, які свідчать про те, що зловмисники дедалі частіше використовують постачальників... Офіційні стратегії з кібербезпеки набагато частіше зустрічаються у великих компаніях, ніж у малих, а багато мікропідприємств досі не надають належної уваги кібербезпеці, що може обмежувати можливості для партнерства та зростання, оскільки великі підприємства посилюють вимоги до безпеки своїх постачальників. Загалом, результати опитування свідчать про те, що рівень кібербезпеки дедалі тісніше пов'язується з конкурентоспроможністю, захистом доходів, довірою та успішною цифровою експансією». (*Alec McDonnell. Cyber Breaches Survey: Business Cybersecurity is at Risk // Business Chief* (<https://businesschief.com/news/cyber-breaches-survey-phishing-supply-chain-risks-soar>). 07.05.2026).

«Виробники стикаються з трьома взаємопов'язаними викликами — посиленням кіберзагроз, жорсткістю нормативних вимог та дедалі складнішими умовами роботи — що робить традиційні підходи до забезпечення безпеки операційних технологій (OT) недостатніми. У звіті ARC Advisory Group, опублікованому у квітні 2026 року, стверджується, що фрагментовані стеки безпеки на основі «точкових рішень» тепер є тягарем, оскільки вони створюють складність, яку важко управляти та інтегрувати, а також збільшують вразливість до ризиків, тоді як кіберінциденти спричиняють дорогі незаплановані простої, вартість яких, за оцінками ARC, перевищує 1 трильйон доларів у всьому світі... Водночас команди операційних технологій (OT) стикаються з дефіцитом кваліфікованих кадрів, бюджетними обмеженнями та розширенням кола обов'язків, що робить управління інструментами від різних постачальників нежиттєздатним. Нормативно-правові рамки, такі як NIS2 та Закон ЄС про кіберстійкість, прискорюють необхідність змін, вимагаючи посилення управління, звітності та управління ризиками в IT та OT, включаючи доказову прозорість та детальну документацію — потреби, яким розрізнені набори інструментів не в змозі задовольнити. Як результат, багато виробників переходять до «платформізації», об'єднуючи резервне копіювання, кібербезпеку та управління в інтегровані платформи, щоб зменшити складність, покращити прозорість та координацію, пришвидшити виявлення та реагування, а також спростити дотримання вимог, надаючи єдине джерело достовірної інформації. У звіті компанія Acronis наводиться як приклад такого підходу: описується її інтегрована платформа кіберзахисту, яка поєднує в собі функції безпеки, захисту даних та управління інфраструктурою, підтримує застарілі операційні системи, поширені в промислових середовищах, а також використовує архітектуру з одним агентом для спрощення розгортання та забезпечення узгодженості. У ньому також підкреслюється роль штучного інтелекту та машинного навчання в сучасному

захисті ОТ, використання базових показників поведінки для виявлення аномалій, зупинки програм-вимагачів та загроз «нульового дня» в режимі реального часу, а також автоматизації реагування та усунення наслідків — можливостей, які вважаються необхідними там, де простої мають безпосередні операційні наслідки. Загалом, у звіті кібербезпека на основі платформ розглядається як стратегія, що стає дедалі необхіднішою для забезпечення стійкості промислових систем та дотримання нормативних вимог у міру зростання рівня підключеності та ризиків». *(Lee Pender. Simplifying industrial cybersecurity in a time of rising risk // Acronis International GmbH. (<https://www.acronis.com/en/blog/posts/simplifying-industrial-cybersecurity-in-a-time-of-rising-risk/>). 07.05.2026).*

«Європейський економічний і соціальний комітет схвалив запропонований ЄС перегляд Закону про кібербезпеку, підтримавши реформи Європейського агентства з кібербезпеки (ENISA), системи сертифікації кібербезпеки ЄС та безпеки ланцюгів постачання ІКТ, при цьому наголосивши, що наступний етап кіберполітики ЄС має залишатися практичним. У своїй думці комітет розглядає кібербезпеку та безпеку ланцюгів постачання як питання економічної безпеки та геополітичної стійкості, що впливають на конкурентоспроможність ЄС та правову визначеність, і вітає зусилля щодо узгодження оновленого Закону з NIS2 таким чином, щоб спростити дотримання вимог та зменшити дублювання зобов'язань... Він підтримує посилення повноважень ENISA, але застерігає, що розширення обов'язків має супроводжуватися відповідним фінансуванням, залученням спеціалістів та обов'язковим планом кадрового забезпечення. Комітет також закликає до оптимізації процедури повідомлення про інциденти шляхом створення єдиного контактного центру, щоб один комплексний звіт міг задовольнити паралельні вимоги, передбачені NIS2, DORA та галузевими режимами. Щодо безпеки ланцюга поставок ІКТ, комітет підтримує створення в ЄС системи для визначення ключових активів та управління постачальниками з високим рівнем ризику, але наголошує на тому, що будь-які обмеження або поступове припинення діяльності мають бути прозорими та пропорційними і супроводжуватися реалістичними планами переходу, що враховують терміни заміни, безперебійність надання послуг, витрати, вплив на ринок праці та ризик перекладання тягаря дотримання вимог на менші підприємства. Нарешті, у висновку стверджується, що кіберполітика має також враховувати питання демократичної стійкості, і пропонується чіткіше визначити роль ENISA у забезпеченні безпеки виборів та підвищенні обізнаності громадськості щодо кіберзагроз, дезінформації та безпечної поведінки в цифровому просторі. Загалом, у висновку висловлюється підтримка більш централізованого підходу ЄС до кібербезпеки, водночас застерігаючи від розширення регулювання швидше, ніж інституції та підприємства можуть його впровадити, щоб уникнути фрагментації зобов'язань або створення непропорційного навантаження». *(EESC backs revised Cybersecurity Act with warnings on ENISA and supply chains // Geneva Internet Platform (<https://dig.watch/updates/cybersecurity-act-2-eesc-opinion>). 08.05.2026).*

«Група з питань співпраці в галузі NIS затвердила єдині шаблони для повідомлення про інциденти в сфері кібербезпеки на території Європейського Союзу, що є важливим кроком на шляху до гармонізації вимог відповідно до Директиви NIS2. Шаблони були затверджені під час 39-го пленарного засідання групи на Кіпрі і призначені для встановлення єдиного формату повідомлень про інциденти у всіх державах-членах. Розроблені спільно державами-членами ЄС, Європейською комісією та Агентством ЄС з кібербезпеки (ENISA), стандартизовані шаблони мають на меті зменшити адміністративне навантаження, спростити зобов'язання щодо звітування для компаній, які зазнали впливу, та мінімізувати фрагментацію, спричинену різними національними вимогами...»

Комісія має намір затвердити ці шаблони шляхом прийняття імплементаційного акту, що зробить їх використання обов'язковим на всій території ЄС. Ця ініціатива також узгоджується з більш широкою пропозицією щодо «цифрового омнібусу», спрямованою на створення єдиного пункту прийому повідомлень про інциденти. Очікується, що завдяки спрощенню процедур та підвищенню узгодженості цей крок зробить дотримання нормативних вимог більш передбачуваним для компаній, що ведуть діяльність у різних юрисдикціях, покращить координацію між національними органами влади та, зрештою, зміцнить загальну стійкість кібербезпеки в усьому блоці». ***(EU adopts unified cyber incident reporting templates under NIS2 // GIP Digital Watch (<https://dig.watch/updates/eu-adopts-unified-cyber-incident-reporting-templates-under-nis2>). 27.05.2026).***

«Компанія OpenAI оголосила про запуск «Плану дій ЄС у сфері кібербезпеки», спрямованого на розширення доступу до своїх передових інструментів штучного інтелекту для кібербезпеки — GPT-5.5 та GPT-5.5-Cyber — для перевірених фахівців з кіберзахисту по всій Європі, зокрема для підприємств, урядів, національних кіберагентств та інституцій ЄС, таких як Офіс ЄС з питань штучного інтелекту. План базується на ширшій концепції OpenAI «Trusted Access for Cyber» — структурі, що ґрунтується на верифікації та призначена для надання затвердженим захисникам розширеного доступу до робочих процесів у сфері безпеки з використанням штучного інтелекту, зберігаючи при цьому обмеження щодо шкідливого використання...»

У рамках цієї платформи GPT-5.5 з функцією Trusted Access for Cyber позиціонується як стандартна відправна точка для виконання оборонних завдань, таких як безпечний огляд коду, сортування вразливостей, аналіз шкідливого програмного забезпечення, розробка засобів виявлення та перевірка патчів. GPT-5.5-Cyber, доступний у обмеженому попередньому доступі, дозволяє більш гнучку поведінку для авторизованих спеціалізованих робочих процесів, включаючи контрольовані атаки «червоної команди», тестування на проникнення та роботи з валідації, з більш суворими вимогами до верифікації. OpenAI зазначає, що GPT-5.5-Cyber набрав 81,9% у тесті CyberGym, трохи випередивши GPT-5.5 та значно випередивши попередні моделі та системи конкурентів. Доступ побудовано на основі верифікації ідентичності, контролю на рівні облікового запису, визначення

обсягу дозволеного використання та моніторингу, а з червня 2026 року окремі користувачі повинні будуть увімкнути розширену безпеку облікового запису або підтвердити використання аутентифікації, захищеної від фішингу...

Керівник відділу політики у сфері штучного інтелекту компанії OpenAI охарактеризував цей крок як надання Європі можливостей у сфері кіберзахисту, яких раніше в регіоні не було, і назвав готовність до кіберзагроз спільним завданням, що вимагає використання передових інструментів у поєднанні з відповідними заходами безпеки та наглядом. Ця система передбачає обмеження щодо крадіжки облікових даних, прихованих операцій, розповсюдження шкідливого програмного забезпечення та зловживання системами третіх сторін незалежно від рівня доступу. До широкої екосистеми кіберпартнерів OpenAI входять провідні постачальники рішень у сфері безпеки, такі як Cisco, CrowdStrike, Palo Alto Networks та інші. План дій ЄС у сфері кібербезпеки надає OpenAI більш чіткий шлях до інфраструктури кіберзахисту Європи, хоча реалізація його потенціалу залежатиме від того, чи зможуть європейські партнери розгорнути передовий штучний інтелект у рамках надійних структур навчання, управління та перевірених сценаріїв використання, що виходять за межі спеціалізованих команд». *(Emma Thompson. OpenAI expands GPT-5.5 cyber defense access to Europe through new EU action plan // (<https://www.edtechinnovationhub.com/news/openai-expands-gpt-55-cyber-defense-access-to-europe-through-new-eu-action-plan>). 11.05.2026).*

«Наразі Велика Британія стикається зі сплеском кібератак: протягом 2025 року Національний центр кібербезпеки (NCSC) щотижня реагуватиме в середньому на чотири інциденти, що мають загальнонаціональне значення. Ці загрози значною мірою походять від суб'єктів, що використовують стратегії «розширених постійних загроз» (APT), зокрема від груп, що діють за підтримки держави, таких як російська «Midnight Blizzard», які дедалі частіше використовують вразливості систем ідентифікації та хмарні інструменти для спільної роботи. Організації державного сектору є особливо вразливими, оскільки вони намагаються модернізувати застарілу інфраструктуру, водночас стикаючись із постійним дефіцитом кадрів та жорсткими циклами закупівель. З огляду на те, що середня вартість порушення безпеки у 2025 році сягне 2,86 млн доларів, інвестиції уряду Великої Британії у розмірі 210 млн фунтів стерлінгів у захист державного сектору є критично важливою реакцією на ці високі ризики, особливо після таких серйозних інцидентів, як атака на Раду Кенсінгтона та Челсі наприкінці 2025 року...

З метою підвищення стійкості до загроз багато організацій переходять на модель безперервного управління ризиками (СТЕМ) та впроваджують підхід до безпеки на основі краудсорсингу. Ця модель розширює внутрішні можливості організації за рахунок залучення перевіреної глобальної спільноти дослідників для виявлення вразливостей за допомогою програм винагород за виявлення помилок, програм розкриття вразливостей (VDP) та послуг з пентестування. Цей підхід виявився надзвичайно ефективним: завдяки структурованим програмам за останній рік вдалося запобігти потенційним збиткам на суму понад 3 мільярди доларів.

Визначивши чіткий обсяг робіт та залучивши цих дослідників, керівники служб інформаційної безпеки можуть виявляти ризики на ранніх етапах та усувати їх, перш ніж ними скористаються зловмисники...

Безпека на основі краудсорсингу має низку стратегічних переваг порівняно з традиційним тестуванням, що проводиться одноразово. Вона забезпечує доступ до різноманітних глобальних фахівців, які володіють експертизою в нових галузях, таких як штучний інтелект та захист даних, а також імітує реальну поведінку зловмисників за допомогою креативних, нестандартних методів атак. Крім того, ця модель є високомасштабованою та забезпечує кількісно вимірюваний «показник віддачі від заходів з мінімізації ризиків» (RoM), що допомагає продемонструвати правлінню та керівництву реальну цінність проактивної безпеки. Замість того, щоб замінювати внутрішні команди, краудсорсингова безпека виступає стратегічним розширенням, що дозволяє організаціям узгоджувати інтенсивність своїх захисних заходів із фактичним рівнем ризику в умовах дедалі більш мінливого середовища загроз». (*Laurie Mercer. How Crowdsourced Security is Transforming the Public Sector Cybersecurity Landscape // Reed Exhibitions Ltd. (<https://www.infosecurity-magazine.com/opinions/crowdsourced-public-sector-cyber/>). 08.05.2026*).

«Оскільки запропонований у Великобританії законопроект про кібербезпеку та кіберстійкість продовжує проходження через парламент після промови короля 13 травня, уряд закликає підприємства приєднатися до нової Ініціативи з кіберстійкості, запуск якої заплановано на кінець цього року. Ця обіцянка, вперше озвучена міністром з питань безпеки Деном Джарвісом на конференції NCSC CyberUK, вимагає від організацій вжити трьох конкретних заходів: зробити кібербезпеку відповідальністю на рівні правління, зареєструватися в службі раннього попередження NCSC та вимагати сертифікації Cyber Essentials у своїх ланцюгах постачання. Міністри представили цю ініціативу як частину ширших зусиль, спрямованих на зміцнення національної оборони проти швидко розвиваючихся загроз, пов'язаних із штучним інтелектом, та встановлення чіткіших стандартів для основних послуг...

У повідомленні також наголошувалося на зростанні британського кіберсектору, який у 2025 році приніс економії 14,7 млрд фунтів стерлінгів (зростання на 11%), збільшився на 20% до 2 063 компаній та створив близько 2 300 нових робочих місць. Уряд закликав підприємства використовувати інновації вітчизняних стартапів та впроваджувати більш безпечні практики, зокрема ширше використовувати мови програмування з безпечною пам'яттю, такі як Java та Rust, і вказав на дослідження Інституту безпеки штучного інтелекту як доказ того, що традиційних засобів захисту вже недостатньо. Уряд зазначив 68-відсоткове зростання кількості продуктів та послуг у сфері безпеки, орієнтованих на штучний інтелект, у 2025 році та позиціонував Велику Британію як країну, що оперативно реагує на нові загрози. Цей крок зроблено на тлі попереджень МВФ про те, що неконтрольовані кібератаки на основі штучного інтелекту можуть загрожувати глобальній фінансовій стабільності, особливо в країнах з перехідною економікою, і що для усунення прогалин в управлінні в умовах поширення передових моделей

штучного інтелекту буде потрібна більш тісна міжнародна координація та обмін інформацією». **(Alex Scroxton. UK government renews calls to sign Cyber Resilience Pledge // TechTarget, Inc. (<https://www.computerweekly.com/news/366642938/UK-government-renews-calls-to-sign-Cyber-Resilience-Pledge>). 11.05.2026).**

«Уряд Великої Британії розглядає можливість запровадження «аварійного вимикача» для систем штучного інтелекту на основі поправки, яку ініціював депутат від Лейбористської партії Алекс Собел і яку підтримали щонайменше 11 інших депутатів. Ця поправка дозволить міністру з питань технологій видавати розпорядження про негайне відключення сучасних систем штучного інтелекту, якщо вони становлять загрозу національній безпеці або життю людей. Цей захід буде додано до законопроекту про кібербезпеку та стійкість, і він вимагатиме безпечних, зашифрованих каналів зв'язку для таких надзвичайних розпоряджень, тоді як в рамках окремої реформи також оновлюється Закон про неправомірне використання комп'ютерних систем як частина ширшого пакету заходів з національної безпеки... Ця пропозиція відображає більш інтервенціоністську позицію Великої Британії у відповідь на зростаючу міжнародну стурбованість ризиками, пов'язаними з розвиненим штучним інтелектом, хоча традиційно ця країна віддавала перевагу підходу, більш сприятливому для інновацій, ніж ЄС. Це також має наслідки для криптовалютних та цифрових ринків, де широко використовуються торговельні системи та боти на базі штучного інтелекту, оскільки припинення роботи сервісів ШІ може порушити роботу ринкової інфраструктури, хоча більш чітке регулювання в кінцевому підсумку може підвищити довіру інституційних інвесторів. Водночас пропозиція порушує невирішені питання щодо того, як таке екстрене відключення працюватиме в децентралізованих системах ШІ, які важче контролювати, ніж централізовані сервіси». **(United Kingdom proposes AI 'kill switch' in cyber security bill // Decentral Media and Crypto Briefing® (<https://cryptobriefing.com/uk-ai-kill-switch-cyber-security-bill/>). 17.05.2026).**

«Опитування MSP 2026 від CyberSmart, проведене на основі відповідей 350 керівників компаній-постачальників керованих послуг у Великій Британії та Ірландії, показало, що економічний тиск змушує багатьох клієнтів із числа малих та середніх підприємств відсувати кібербезпеку на другий план у списку пріоритетів, навіть попри зростання загроз, а також що MSP (Постачальник керованих послуг) дедалі частіше перетворюються на «постачальників послуг із забезпечення відповідності вимогам» поряд зі своїми традиційними функціями в галузі ІТ та безпеки. Майже половина MSP (46%) зазначила, що їхні клієнти більше турбуються про операційні проблеми, такі як інфляція та зростання витрат, ніж про кібербезпеку, а MSP також визначили інфляцію як головну загрозу для клієнтів (46%), випередивши програмне забезпечення для вимагання викупу/шкідливе програмне забезпечення (41%), загрози на основі штучного інтелекту (37%) та ризики ланцюга поставок (25%), незважаючи на те, що 59% MSP

вважають, що клієнти наражаються на більший ризик, ніж рік тому. Самі MSP продовжують бути об'єктом інтенсивних атак: три чверті з них повідомили про щонайменше один випадок порушення безпеки за останні 12 місяців, а багато хто стикався з повторними порушеннями, тоді як загрози, пов'язані зі штучним інтелектом, другий рік поспіль залишаються їхньою головною внутрішньою проблемою безпеки (49%); ризики ланцюга поставок також піднялися в рейтингу MSP, що відображає підвищену увагу, пов'язану з пропонуванням у Великобританії законопроектів про кібербезпеку та стійкість та роллю MSP у ланцюгах поставок...

Результати опитування свідчать про те, що рівень уваги клієнтів до MSP стабілізується, а не зростає: 70% респондентів відзначають посилення контролю порівняно з 77% роком раніше, проте попит на підтримку у сфері дотримання нормативних вимог стрімко зростає: 61% клієнтів зараз очікують від MSP допомоги у дотриманні нормативних вимог, а інвестиції MSP у сферу дотримання нормативних вимог та регулювання зросли з 64% до 72%. CyberSmart стверджує, що кіберризики та економічний тиск стають дедалі більш нерозривними, що ускладнює продаж безпеки як окремої послуги та зміщує практичний фокус на відповідальність, підзвітність та інтеграцію безпеки в повсякденну діяльність. Щоб задовольнити мінливі очікування, MSP планують надати пріоритет навчанню, постійному моніторингу та проактивному управлінню ризиками протягом наступних одного-трьох років, оскільки малі та середні підприємства шукають допомоги у дотриманні поточних стандартів, таких як Cyber Essentials». *(Neil Trim. Economic strain pushes cybersecurity down the priority list for MSP customers, CyberSmart research reveals // Kingswood Media (<https://technologyreseller.uk/economic-strain-pushes-cybersecurity-down-the-priority-list-for-msp-customers-cybersmart-research-reveals/>). 14.05.2026).*

«За даними CONTEXT, у квітні 2026 року доходи європейського ринку кібербезпеки зросли на 10% у порівнянні з аналогічним періодом минулого року, що свідчить про відновлення зростання після слабкого початку року та відображає чітку зміну пріоритетів у витратах. Покупці перерозподіляють бюджети на користь безпеки, орієнтованої на ідентифікацію, дотримання нормативних вимог та дані, причому сегмент управління ідентифікацією та доступом є найдинамічнішим із зростанням на 18% з початку року, за ним йдуть безпека даних (13%) та захист інфраструктури (9%), тоді як традиційні категорії, орієнтовані на периметр, зазнали спаду: безпека мереж знизилася на 4%, а захист кінцевих точок — на 1%. Дані свідчать про те, що організації реагують на розширення площі атаки, більшу розподіленість хмарних та сторонніх середовищ, а також посилення регуляторного контролю, інвестуючи більше коштів у контроль доступу, управління та відмовостійкості...

У звіті також наголошується на значному зростанні у сфері керованих послуг з безпеки: доходи від кібербезпеки через канал MSP по всій Європі зросли на 17% у порівнянні з минулим роком, що зумовлено дефіцитом кваліфікованих кадрів, вимогами щодо дотримання нормативних вимог та потребою у цілодобовому

моніторингу. Темпи зростання значно різняться залежно від країни: в Італії зафіксовано стрибок на 67%, в Іспанії — на 39%, а в Німеччині — на 14%, що свідчить про нерівномірне впровадження аутсорсингових рішень з безпеки в регіоні. CONTEXT пов'язує ці зміни з посиленням занепокоєння, викликаного серйозними інцидентами та технологічними розробками, зокрема автономними інструментами штучного інтелекту для виявлення вразливостей, гучними випадками використання програм-вимагачів та порушеннями безпеки в освітньому секторі, а також зростанням ризиків, пов'язаних із ланцюгами постачання та сторонніми організаціями. Усі ці фактори спонукають організації до підвищення рівня прозорості, забезпечення ідентичності та операційної стійкості, а не покладатися переважно на застарілі засоби захисту периметра мережі». (*Joseph Gabriel Lagonsin // TechDay (<https://securitybrief.co.uk/story/europe-cybersecurity-revenues-rise-as-identity-leads-shift>). 21.05.2026*).

«З 11 грудня 2027 року Закон ЄС про кіберстійкість (CRA) запровадить обов'язкові вимоги щодо кібербезпеки для продуктів із цифровими елементами (PDE), що розміщуються на європейському ринку, у відповідь на зростання кількості кібератак на підключене апаратне та програмне забезпечення. Цей регламент поширюється на всіх суб'єктів господарювання в ланцюгу постачання — виробників, імпортерів та дистриб'юторів — які розміщують на ринку ЄС кінцеві продукти або автономні цифрові компоненти після цієї дати. Продукти, що не відповідають вимогам, більше не можуть продаватися або розповсюджуватися, а порушення можуть призвести до штрафів, заходів з нагляду за ринком і навіть відкликання продукції...

Вплив CRA поширюється не лише на кінцеві продукти, а й на компоненти, що входять до їхнього складу. Навіть якщо компоненти реалізуються окремо, недоліки в їхній кібербезпеці можуть призвести до того, що весь продукт не відповідатиме вимогам. Якщо інтегровані компоненти містять вразливості, не мають необхідних оновлень безпеки або більше не підтримуються виробником, це може поставити під загрозу здатність продукту в цілому відповідати основним вимогам CRA щодо кібербезпеки та управління вразливостями. Це є особливо проблематичним для продуктів із вбудованим програмним забезпеченням, термін експлуатації якого закінчився і яке більше не отримує оновлень безпеки...

Існує обмежене виключення для запасних частин, призначених для заміни ідентичних компонентів, виготовлених за тими самими технічними характеристиками, зокрема для застарілих виробів, випущених на ринок до дати введення в дію, або для деталей, які вже пройшли оцінку відповідності CRA. Однак це виключення має вузьке застосування і не усуває більш загальних ризиків щодо відповідності вимогам.

Тому дата введення в дію має вирішальне значення не тільки для кінцевих продуктів, але й для компонентів та запасних частин у всьому ланцюгу постачання. Якщо компоненти, що не підтримуються, ставлять під загрозу відповідність вимогам, а компенсаційні заходи є недостатніми, виробники можуть бути змушені замінити компоненти або перепроектувати продукти, що потребує значних витрат.

Щоб зменшити ці операційні та економічні ризики, компанії повинні діяти завчасно, вимагаючи від постачальників на договірній основі забезпечення довгострокового технічного обслуговування, оновлень та управління вразливостями, а також встановлюючи чіткі терміни підтримки. Вони також повинні розробити плани дій у надзвичайних ситуаціях, зменшити залежність від компонентів, що не підтримуються, та вчасно управляти або ліквідувати запаси, що залишилися до настання дати припинення підтримки. Згідно з CRA, кібербезпека стає основною вимогою до якості у всьому ланцюгу постачання, що робить проактивне планування конкурентною перевагою». (*Andreas Scheibenpflug. Cybersecurity in the Supply Chain: Components and Spare Parts under the Cyber Resilience Act – what Economic Operators need to consider until 11 December 2027 // Noerr Career (<https://www.noerr.com/en/insights/cybersecurity-in-the-supply-chain-components-and-spare-parts-under-the-cyber-resilience-act>). 26.05.2026*).

«Згідно з індексом ділової кон'юнктури Barclays за 1 квартал 2026 року, британські підприємства нарешті визнають кібербезпеку пріоритетним питанням на рівні керівництва: 68% організацій планують збільшити інвестиції в безпеку протягом наступного року. Ця зміна відображає відхід від історичної самовпевненості до більш реалістичної оцінки ризиків, оскільки лише 29% компаній на даний момент вважають себе повністю готовими до відбиття масштабної кібератаки, висловлюючи глибоке занепокоєння щодо перебоїв у роботі, втрати даних та підризу довіри клієнтів... Поряд із кібербезпекою компанії приділяють велику увагу інвестиціям у штучний інтелект, що створює певну напругу між швидкими інноваціями та управлінням ризиками. Хоча понад половина опитаних підприємств стверджує, що ШІ та автоматизація вже підвищили продуктивність, а 61% повідомляють про використання агентного ШІ, майже половина визнає, що впровадження цих нових технологій суттєво збільшує їхню вразливість до кіберзагроз та проблем із безпекою даних. Незважаючи на ці визнані ризики, впровадження технологій триває швидкими темпами, що змушує експертів галузі ставити під сумнів реальну, вимірювану віддачу від інвестицій у ШІ... Критики зазначають, що хоча інструменти штучного інтелекту можуть прискорити такі процеси, як програмування, швидкість виконання не завжди гарантує безпеку, надійність або високу якість результатів. Зрештою, хоча збільшення фінансування у сфері кібербезпеки є позитивним кроком, залишається незрозумілим, чи зможуть організації ефективно збалансувати своє агресивне впровадження штучного інтелекту, яке інколи зумовлене страхом пропустити щось важливе (FOMO), із реальним підвищенням рівня цифрової безпеки та операційної стійкості». (*Penny Horwood. UK business boosts cybersecurity spending // The Channel Company EMEA (<https://www.computing.co.uk/news-analysis/2026/business-boosts-cyber-spending?itc=refresh>). 27.05.2026*).

«Британські компанії все частіше ставлять кібербезпеку в число пріоритетних питань на рівні керівництва та відповідно збільшують

інвестиції, хоча залишаються сумніви щодо того, чи призведе збільшення бюджетів до суттєвого підвищення рівня безпеки. Згідно з Індексом процвітання бізнесу Barclays за 1 квартал 2026 року, майже сім з десяти британських підприємств (68 відсотків) планують збільшити витрати на кібербезпеку протягом наступних 12 місяців, що зумовлено зростаючою обізнаністю щодо фінансових, операційних та репутаційних ризиків, пов'язаних із кіберінцидентами, а також очікуваними змінами в законодавстві, зокрема прийняттям Закону про кібербезпеку та стійкість. Однак рівень впевненості залишається низьким: менше третини компаній (29 відсотків) вважають, що вони повністю готові ефективно реагувати на серйозні кібератаки, що свідчить як про значний розрив у стійкості, так і про більш здорову та реалістичну оцінку кіберризиків, яка замінила попередню самовпевненість...

Підприємства висловлюють особливе занепокоєння щодо шкоди репутації (28%), перебоїв у роботі (27%) та втрати доходів (26%), тоді як великі організації особливо турбуються про крадіжку даних та інтелектуальної власності (33%). Впровадження ШІ викликає додаткові побоювання: 46% опитаних вважають, що нові технології підвищують вразливість, а 26% турбуються щодо точності та надійності результатів роботи ШІ. Проте, незважаючи на ці побоювання, підприємства прискорюють впровадження ШІ: 52% повідомляють про підвищення продуктивності завдяки ШІ та автоматизації, а 61% вже використовують агентний ШІ. Однак дослідження показують, що обережність є виправданою, оскільки багато організацій мають труднощі з вимірюванням та обґрунтуванням заявленого підвищення продуктивності від інвестицій у ШІ...

З огляду на посилення загроз компанія BT Business випустила комплексний пакет рішень з кібербезпеки, розроблений спеціально для британських малих та середніх підприємств (МСП), які є основною мішенню зловмисників. Нещодавнє дослідження BT показало, що кількість зловмисних сканувань зросла на 300% порівняно з минулим роком, причому підключені пристрої піддаються скануванню в середньому 4 000 разів на день. Незважаючи на те, що половина малих та середніх підприємств вважає кіберзагрози головним джерелом занепокоєння, приблизно 1,8 мільйона британських підприємств — близько третини від загальної кількості малих та середніх підприємств — не мають навіть базового захисту від кіберзагроз. З огляду на те, що середні витрати на усунення наслідків порушення безпеки становлять 3 550 фунтів стерлінгів на одне британське підприємство, а 43 відсотки підприємств щорічно стикаються принаймні з одним порушенням або атакою, потреба у доступній підтримці є нагальною...

Нові інструменти BT на базі штучного інтелекту, розроблені спільно з CrowdStrike, вперше забезпечують малим підприємствам кібербезпеку корпоративного рівня. Цю пропозицію доповнює безкоштовний «Центр кіберпідтримки», що включає інструмент самооцінки «Cyber Health Check», спеціалізованих кіберконсультантів, які надають допомогу по телефону та в режимі онлайн, цілодобового кібер-асистента на базі штучного інтелекту, а також платформу з практичними посібниками та пояснювальними матеріалами. Ці ресурси, розроблені відповідно до рекомендацій Національного центру кібербезпеки, враховують результати досліджень, які показують, що понад 80

відсотків малих та середніх підприємств вважають, що індивідуальні консультації з фахівцем покращили б їхню безпеку. Удосконалене рішення забезпечує моніторинг підозрілої активності в режимі реального часу та швидке автоматичне усунення загроз, допомагаючи запобігати атакам, перш ніж вони завдадуть шкоди. Ця ініціатива відображає усвідомлення того, що британські малі та середні підприємства зараз стикаються з тими самими складними загрозами, що й великі підприємства, маючи при цьому набагато менше ресурсів для захисту». (**Ray Sharma. BT Business Launches AI Cybersecurity Tools for UK SMEs to Combat Rising Cyber attacks // THE FAST MODE** (<https://www.thefastmode.com/technology-solutions/48605-bt-business-launches-ai-cybersecurity-tools-for-uk-smes-to-combat-rising-cyber-attacks>). 25.05.2026).

«Кібератаки та цифрова залежність стали основними інструментами примусу, дестабілізації та впливу в широкому сусідстві ЄС, спрямованими проти державних служб, критичної інфраструктури, виборчих процесів, ланцюгів постачання та інформаційного простору. Оскільки цифрова інфраструктура та потоки даних за своєю природою є транскордонними, держави-члени ЄС та партнери з розширення на Західних Балканах і в Східному сусідстві пов'язані спільним та взаємозалежним цифровим середовищем, що робить прогалини в кіберстійкості прямою загрозою європейській безпеці. Проте цифрова політика та кібербезпека в контексті розширення залишаються значною мірою вбудованими в повільний, орієнтований на дотримання вимог процес приєднання, зосереджений на узгодженні нормативно-правових баз, що не дуже добре узгоджується з мінливим та транснаціональним ландшафтом загроз. Такий підхід гальмує здатність до колективного реагування, оскільки співпраця залишається фрагментованою та часто реактивною, виявляючи постійні недоліки в ресурсах, координації та доступі до оперативної співпраці...

Ситуація з загальними загрозами є вкрай серйозною. Атака російської компанії «Віасат» на мережу КА-SAT продемонструвала, як кібероперація, спрямована проти України, також порушила роботу користувачів супутникового широкосмугового доступу в усій Європі. Складні атаки, здійснені державними суб'єктами, зокрема Китаєм, Росією, Іраном та Північною Кореєю, а також недержавними угрупованнями в рамках таких операцій, як «Volt Typhoon», «NotPetya», «WannaCry» та «Andariel», мають системні наслідки, здатні порушити функціонування життєво важливих служб та підірвати демократичні процеси. ENISA зафіксувала 4 875 інцидентів у період з липня 2024 року по червень 2025 року, причому все частіше у зловмисних діях використовується штучний інтелект, а близько 80 відсотків атак мають ідеологічне підґрунтя. Партнери з розширення ЄС стикаються з не менш інтенсивним тиском: Україна зафіксувала понад 5 900 кібератак у 2025 році, що на 37 відсотків більше, ніж у попередньому році, тоді як Молдова зазнала понад 1 000 атак лише у першій половині 2025 року, багато з яких приписують групам, пов'язаним з Росією. Виборчі процеси стали основною мішенню: під час парламентських виборів у Молдові 2025 року було зафіксовано

понад 16 мільйонів спроб зловмисних підключень, що змусило тимчасово заблокувати 4 000 веб-сайтів...

Усунення цих вразливостей ускладнюється низкою взаємопов'язаних викликів. По-перше, акцент на дотриманні нормативних вимог — таких як відповідність Директиві NIS2 та «Інструментарію 5G» — не повинен йти на шкоду оперативній стійкості, оскільки формальна відповідність не гарантує готовності. Рівень впровадження залишається неоднаковим навіть серед держав-членів ЄС, а інструменти, розроблені для внутрішньої архітектури Союзу, важко оперативно застосувати в умовах розширення. По-друге, зберігається гостра нестача фахівців з кібербезпеки: 52% європейських організацій мають труднощі з утриманням кваліфікованого персоналу, що послаблює оборонні можливості та обмежує розвиток вітчизняної експертизи та альтернатив на основі відкритого програмного забезпечення. По-третє, обмін інформацією залишається асиметричним: мережа CSIRT ЄС не відкрита для партнерів з розширення, а існуючі механізми або мають занадто обмежений обсяг, або є надто рестриктивними, щоб відповідати фактичному рівню цифрової інтеграції, що вже існує. По-четверте, структурна залежність від неєвропейських постачальників — зокрема американських та китайських компаній у сфері хмарних послуг, де Amazon, Google та Microsoft контролюють 63% європейського ринку — створює ризик закріплення тих самих вразливостей, які ЄС прагне зменшити, оскільки партнери з розширення схильються до дешевших та доступніших іноземних рішень...

Щоб підвищити стійкість до вступу, ЄС має діяти на трьох напрямках. Політична стійкість вимагає чітких інституційних повноважень, сумісних процедур кризового управління, надійних каналів обміну інформацією та більш доступної взаємодії зі структурами ЄС, зокрема альтернативних форматів тіснішої співпраці з європейськими CSIRT у випадках, коли повна участь ще неможлива. Суспільна стійкість вимагає надійних цифрових архітектур для критичної інфраструктури, підвищення цифрових навичок серед населення, кращої кібергігієни, орієнтованої на практику університетської підготовки та більшої стійкості до дезінформації — зусиль, які можна було б підсилити за допомогою масштабних навчань, таких як вісім, проведених Україною з 2023 року, та ініціатив ЄС з розбудови потенціалу, таких як GLACY-е та Octopus Project. Промислова стійкість вимагає створення надійної цифрової промислової бази, яка зменшить залежність від неєвропейських постачальників завдяки диверсифікованим ланцюгам постачання ІКТ, стратегічній політиці закупівель, стабільним інвестиціям у дослідження та інновації, а також більш інтегрованому європейському цифровому ринку, що дасть змогу регіональним постачальникам розширювати свою діяльність та пропонувати життєздатні альтернативи... Такі платформи, як Центр кіберпотенціалу Західних Балкан, можуть слугувати осередками не лише для навчання, а й для сприяння впровадженню технологій у промисловості регіону та транскордонній співпраці. Зрештою, ЄС повинен вийти за межі формального узгодження та зосередитися на практичних умовах, за яких можна забезпечити та підтримати стійкість, визнаючи, що партнери з розширення є провідними учасниками, чий потенціал, за умови його ефективнішого використання, міг би зміцнити регіональну безпеку в цілому».

(Clotilde Bômont, Bojana Zorić. Shared threats, shared resilience: Integrating

«Запропонований урядом Великої Британії законопроект про кібербезпеку та стійкість (CSRB), який, як очікується, набуде чинності пізніше цього року, є наймасштабнішою реформою системи кібербезпеки країни з часів прийняття у 2018 році Положень про мережі та інформаційні системи. Для місцевих органів влади в Англії та Уельсі цей законопроект означає кардинальну зміну, в результаті якої кібербезпека переходить з розряду суто технічних ІТ-питань у сферу ключових питань лідерства, управління та операційної стійкості. Оскільки органи влади все більше покладаються на складні цифрові системи, зовнішніх постачальників, хмарні платформи та спільні послуги для надання основних державних послуг — таких як соціальна допомога дорослим, захист дітей, житло, доходи, освіта та демократичні функції — вони також стикаються зі зростаючими обсягами конфіденційних персональних даних та частішими й більш витонченими атаками програм-вимагачів та кібератаками...

Законодавство має на меті підвищити стійкість організацій, що надають життєво важливі послуги, посилити відповідальність за кіберризики в державних органах та їхніх ланцюгах постачання, а також запровадити більш суворі зобов'язання для постачальників, посилені вимоги щодо повідомлення про інциденти, розширити повноваження з контролю за дотриманням нормативних вимог та посилити контроль за ризиками в ланцюгах постачання. Від керівників вищого рівня, включаючи генеральних директорів та відповідальних за моніторинг, очікується активне управління кіберризиками, причому кіберінциденти все частіше розглядаються не просто як збої в роботі ІТ-систем, а як більш широкі недоліки в управлінні та операційній стійкості. Практичні наслідки серйозного порушення можуть включати тривале переривання надання послуг, ризики для безпеки, фінансові втрати, штрафи за порушення захисту даних, ретельний контроль з боку регуляторних органів, шкоду репутації та втрату довіри громадськості...

У відповідь на це місцеві органи влади повинні терміново переглянути існуючі договори з постачальниками, процедури закупівель, плани реагування на інциденти, структури управління та механізми управління ризиками, щоб переконатися, що вони містять належні зобов'язання щодо кібербезпеки, чіткі лінії підзвітності, надійні процедури повідомлення та адекватні положення про відшкодування збитків. З огляду на перехресні регуляторні вимоги, що впливають із британського GDPR, обов'язків щодо забезпечення безпеки та зобов'язань за публічним правом, надзвичайно важливо підготуватися заздалегідь. Організації, які вже зараз вживають заходів для посилення кіберуправління, нагляду за постачальниками та забезпечення на рівні правління, матимуть набагато кращі можливості для захисту державних послуг, задоволення вимог регуляторних органів та обмеження більш широких правових, фінансових та репутаційних наслідків у разі виникнення інцидентів. Ті, хто зволікає, можуть зіткнутися з тим, що кіберзлочин швидко переросте у значну кризу в сфері управління та

регулювання». (*Cyber Security and Resilience Bill: Why Local Authorities Cannot Afford to Wait // Local Government Lawyer* (<https://www.localgovernmentlawyer.co.uk/information-law/344-information-law-features/100568-cyber-security-and-resilience-bill-why-local-authorities-cannot-afford-to-wait>). 20.05.2026).

«Болгарський національний системний інтегратор «Bulgaria Information Services» (BIS) впровадив сервіс Google Cloud Cybershield з метою зміцнення національного потенціалу країни у сфері кіберзахисту, ставши однією з перших європейських країн, що розгорнули цю платформу на базі штучного інтелекту. За підтримки фінансування Європейського Союзу, спрямованого на покращення безпеки вздовж східного кордону ЄС, ініціатива має на меті централізувати кіберрозвідку та моніторинг загроз для 54 болгарських урядових та державних організацій. Проект розроблено з метою скорочення часу, необхідного для виявлення та реагування на кіберзагрози, а також для переходу стратегії кібербезпеки Болгарії від реактивної моделі до проактивного підходу, що базується на розвідці...

Це впровадження є ключовою складовою Національної стратегії кіберзахисту Болгарії, яка спрямована на створення об'єднаного міжвідомчого центру оперативного реагування, здатного протидіяти кіберзагрозам, що швидко розвиваються на основі штучного інтелекту. За допомогою «Cybershield» BIS використовуватиме Google Cloud Security Operations, Google Threat Intelligence та оперативні аналітичні дані про загрози від Mandiant для покращення можливостей виявлення та реагування в усіх установах-учасниках. Система також забезпечує безпечну хмарну інфраструктуру та спеціалізовану підтримку аналітиків, що допомагає виявляти та нейтралізувати складні кібервтручання, одночасно зміцнюючи внутрішню експертизу Болгарії у сфері кібербезпеки...

Google Cloud охарактеризував цей проєкт як приклад того, як засоби захисту на основі штучного інтелекту можуть протистояти дедалі витонченішим атакам, що використовують штучний інтелект, і назвав Болгарію провідним прикладом централізованої кібербезпеки в Європі. Cybershield, спочатку запущений у 2023 році під назвою Chronicle Cybershield, був спеціально розроблений для урядів з метою покращення обміну інформацією в режимі реального часу та оцінки ситуації щодо сучасних кіберзагроз. На його створення вплинуло різке зростання кількості кібератак на урядові установи після вторгнення Росії в Україну, що значно підвищило попит на послуги Mandiant з реагування на інциденти. Болгарія тепер приєднується до таких країн, як Кувейт, у впровадженні Cybershield для побудови централізованих національних інфраструктур кібербезпеки, здатних протистояти сучасним цифровим загрозам». (*Alex Scropton. Bulgaria fires up Google Cloud for national cyber security // TechTarget, Inc.* (<https://www.computerweekly.com/news/366643458/Bulgaria-fires-up-Google-Cloud-for-national-cyber-security>). 20.05.2026).

«Нещодавно в Європейському парламенті відбулися дебати щодо здатності Європейського Союзу реагувати на зростаючий вплив штучного інтелекту, зокрема у сфері кібербезпеки та технологічного суверенітету. Законодавці зосередили увагу на значній залежності Європи від американських технологічних компаній, таких як OpenAI та Anthropic, які розробляють передові моделі ШІ, орієнтовані на кібербезпеку, — наприклад GPT-5.5-Cyber та Mythos, — що незабаром можуть з'явитися на європейському ринку. Під час обговорення було висловлено занепокоєння щодо того, чи здатні європейські компанії створювати аналогічні системи штучного інтелекту, та наскільки вразливою може стати Європа, якщо її інфраструктура кібербезпеки та конфіденційні дані залишатимуться залежними від іноземних технологій...

Представники ЄС наголосили як на можливостях, так і на небезпеках, пов'язаних із сучасними системами штучного інтелекту. Заступниця міністра з європейських справ Кіпру Марілена Рауна попередила, що штучний інтелект дедалі більше інтегрується в економіку та систему безпеки Європи, але його також можуть використовувати кіберзлочинці та ворожі держави шляхом складних фішингових атак, експлуатації вразливостей та дезінформаційних кампаній. Виконавча віцепрезидентка Європейської комісії з питань технологічного суверенітету Хенна Вірккунен також визнала, що ШІ може посилити захист інфраструктури, водночас створюючи нові ризики для безпеки завдяки своїй здатності виявляти вразливості набагато швидше, ніж раніше...

Під час дискусії було наголошено на тому, що в Європі наразі бракує компаній, здатних розробляти системи штучного інтелекту, які б не поступалися за рівнем розвитку тим, що створюються у Сполучених Штатах, через що критично важлива інфраструктура, така як лікарні, бази даних та військові системи, залишається залежною від іноземних постачальників технологій. Занепокоєння з приводу цієї залежності вже змусило європейські інституції обмежити використання певних інструментів штучного інтелекту з міркувань безпеки. Проте будь-які іноземні системи штучного інтелекту, що виходять на ринок ЄС, повинні будуть відповідати європейським нормам, таким як Закон про штучний інтелект та Закон про кіберстійкість...

Політичні фракції в Європейському парламенті в цілому погоджуються з необхідністю зміцнення європейського технологічного суверенітету шляхом сприяння розвитку вітчизняних технологій штучного інтелекту та зменшення залежності від зовнішніх гравців. У цьому контексті ЄС покладає значні надії на такі компанії, як французька Mistral AI, щодо створення конкурентоспроможних європейських рішень у сфері кібербезпеки. Під час обговорення також проявилися загальна невизначеність та амбіції щодо майбутньої ролі штучного інтелекту в суспільстві, при цьому законодавці визнали, що співпраця між інституціями ЄС та державами-членами буде мати вирішальне значення для орієнтування у швидкозмінному технологічному середовищі». ***(Javier Rubio Monte. The EU seeks to reduce its reliance on US AI in cybersecurity // Digital Shield (<https://www.escudodigital.com/en/defense/europe/eu-seeks-reduce-reliance-us-ai-cybersecurity.html>). 22.05.2026).***

«Компанія Marks & Spencer скасувала виплату премій усьому своєму персоналу, що налічує 63 000 осіб, включаючи генерального директора Стюарта Мачіна, голову правління Арчі Нормана, членів правління, керівників вищої ланки та менеджерів понад 1 000 магазинів, у зв'язку з масштабною кібератакою, яка суттєво позначилася на прибутках ритейлера. Це рішення, прийняте комітетом з винагород, має на меті продемонструвати відповідальність за фінансові та операційні наслідки інциденту, який стався приблизно на Великдень 2025 року. Мачін пояснив, що «з огляду на вплив кіберінциденту на результати діяльності компанії, комітет з винагород та наші виконавчі директори домовилися не застосовувати систему премій», додавши, що ніхто в M&S, включаючи його самого та виконавчу команду, не отримає премію цього року. Він визнав, що персонал «працював важче, ніж будь-коли, у дуже складний період», та висловив вдячність за їхні зусилля...

Кібератака призвела до падіння ринкової вартості компанії на понад 1 млрд фунтів стерлінгів, а вартість акцій одразу після інциденту впала більш ніж на 12%; крім того, вона спричинила витрати у розмірі 131,3 млн фунтів стерлінгів, пов'язані з відновленням систем, управлінням ризиками та послугами спеціалізованих консультантів. Незважаючи на ці перебої, компанія M&S все ж продемонструвала загальне зростання обсягу продажів на 24,8% до 17,4 млрд фунтів стерлінгів за рік, повернувшись до більш високих показників у другому півріччі. Мачін охарактеризував цей період як «надзвичайний» рік, що складався з двох частин: на початку відбулися серйозні перебої через кібератаку, а потім відбулося стійке відновлення обсягів продажів та прибутку». *(M&S axes all staff bonuses after major cyber attack hits profits hard // Executive Grapevine International Ltd (<https://www.hrgrapevine.com/content/article/2026-05-22-ms-axes-all-staff-bonuses-after-major-cyber-attack-hits-profits-hard>). 23.05.2026).*

«Новий звіт Статистичного бюро Нідерландів (CBS) свідчить про значне зменшення кількості кіберінцидентів, що зачепили нідерландські підприємства за останнє десятиліття. Згідно з доповіддю «Монітор кібербезпеки 2025», підготовленою на замовлення Міністерства економіки та кліматичної політики, у 2024 році лише 4% компаній зазнали хоча б одного кіберінциденту, що на 11% менше, ніж у 2016 році. У доповіді, яка оцінює кіберстійкість підприємств, кіберінцидент визначається як ситуація, коли компанія стикається з наслідками кібератаки, такими як збій ІТ-системи, спричинений програмним забезпеченням-вимагачем. Кількість інцидентів, пов'язаних із зовнішніми атаками, також зменшилася порівняно з 2023 роком, за одним помітним винятком: підприємства з 250 і більше працівниками повідомили про стабільний рівень інцидентів у 16 відсотків в обох роках. Серед секторів найбільш постраждав від зовнішніх атак сектор інформації та комунікацій, де 7 відсотків компаній повідомили про інцидент... Навпаки, сектор послуг з розміщення та харчування, а також сектор охорони здоров'я та соціальної допомоги постраждали найменше — у кожному з них цей показник становив лише 2%. CBS зазначає, що низький рівень у

секторі послуг з розміщення та харчування не є несподіванкою, оскільки ці підприємства менше покладаються на ІТ-системи, що зменшує їхню вразливість до збоїв апаратного чи програмного забезпечення. Сектор охорони здоров'я та соціального забезпечення виграє від суворих політик інформаційної безпеки, які забезпечують більш надійний захист від зовнішніх загроз. У звіті також підкреслюється сильна кореляція між розміром компанії та кіберстійкістю, причому великі підприємства частіше впроваджують численні заходи безпеки. Наприклад, 86 відсотків великих компаній із 250 і більше співробітниками застосували десять або більше з дванадцяти розглянутих заходів, у порівнянні з лише 13 відсотками малих компаній із 2–10 співробітниками». **(Sharp Decline in Cyber Incidents Among Dutch Businesses, CBS Report Shows // IndexBox, Inc (<https://www.indexbox.io/blog/sharp-decline-in-cyber-incidents-among-dutch-businesses-cbs-report-shows/>). 28.05.2026).**

«Директорка GCHQ (Головне управління урядових комунікацій) Енн Кіст-Батлер у своїй щорічній лекції попередила, що Велика Британія опинилася на «переломному етапі», оскільки супротивники посилюють гібридні операції, а технологічна конкуренція набирає обертів, створюючи, за її словами, нову еру радикальної невизначеності та стрімких технологічних змін. Вона зазначила, що Росія невпинно націлена на критичну інфраструктуру, демократичні процеси, ланцюги постачання та довіру громадськості у Великій Британії та Європі, тоді як швидкість розвитку штучного інтелекту, квантових обчислень та космічних систем зводить до нуля можливості для Великої Британії та її союзників щодо збереження стратегічної переваги та збільшує ризик прорахунків. Кіст-Батлер закликала урядові та промислові кола приділяти «вдесятеро більше уваги» питанням кібербезпеки та повідомила, що GCHQ розробило план створення нових національних сил кіберзахисту, які передбачають впровадження агентного штучного інтелекту в оборонні системи, що працюють зі швидкістю машин, а також відповідальне використання передових технологій штучного інтелекту в операціях з таких завдань, як вдосконалення алгоритмів, переклад мов та швидше виявлення загроз...

Вона підкреслила, що технології та дані сьогодні є рушійними силами перетворень, які можуть бути використані як зброя в умовах, що не досягають порогу традиційної війни, зазначивши зростання Китаю як технологічної супердержави, а також діяльність Росії в «сірій зоні», що охоплює кіберпростір і морське дно, включаючи загрози підводним кабелям і трубопроводам. Кіст-Батлер також підкреслила, що квантова технологія наближається швидше, ніж передбачалося раніше: квантове зондування вже застосовується для виявлення таких ознак, як запуски ракет, а майбутні квантові комп'ютери можуть зламати сучасне шифрування, що вимагає термінового захисту критично важливих систем та підготовки до постквантової безпеки. Вона поширила це попередження на космічну сферу, вказавши на стрімке зростання кількості супутників та потоків даних, а також на повідомлення про супутникові знімки, що підтверджують

іранські атаки, і зазначила, що GCHQ співпрацює з партнерами для забезпечення безпеки космічних технологій...

З метою підвищення стійкості вона закликала як окремих осіб, так і організації вжити практичних заходів: від відмови від паролів на користь ключів-паролів до вбудовування засобів безпеки в нові технології, захисту ланцюгів постачання та розширення державно-приватного співробітництва з представниками промисловості, наукових кіл та стартапів. Вона наголосила, що такі альянси, як «П'ять очей», залишаються ключовими для протидії державним загрозам, запобігання тероризму та боротьби з серйозною кіберзлочинністю. Коментатори зазначили, що її зауваження підкреслюють, що кібербезпека більше не є другорядним питанням і що слід прискорити реалізацію таких програм, як планування постквантової криптографії, закликаючи європейські організації розробити до кінця 2026 року дорожні карти переходу на PQC, криптографічні інвентарі та пілотні проекти». (*Anna Ribeiro. UK faces 'moment of consequence,' as GCHQ advances AI-driven cyber defence against hybrid threats // Industrial Cyber* (<https://industrialcyber.co/critical-infrastructure/uk-faces-moment-of-consequence-as-gchq-advances-ai-driven-cyber-defence-against-hybrid-threats/>). 28.05.2026).

«Кабінет міністрів Німеччини схвалив законопроект, який розширить повноваження уряду щодо безпосереднього втручання у разі кібератак шляхом виведення з ладу програмного забезпечення, серверів та інфраструктури, що використовуються зловмисниками, включаючи системи, розташовані за кордоном. Міністр внутрішніх справ Олександр Добріндт назвав цей законопроект важливим кроком на шляху до «проактивної» або «активної» кіберзахисту, стверджуючи, що влада повинна мати можливість нейтралізувати загрози та позбавити зловмисників можливості діяти, коли об'єктом атаки стає Німеччина. Хоча Добріндт наголосив, що ці заходи не мають на меті стати «відповідними хакерськими атаками», Німеччину неодноразово попереджали, що вона стикається зі складними кіберопераціями з боку іноземних держав та пов'язаних з державою угруповань, спрямованими проти промисловості, малих та середніх підприємств, наукових установ, урядових органів та політичних партій...

Згідно з проектом закону, нові повноваження будуть надані Федеральному управлінню кримінальної поліції (ВКА), Федеральній поліції та Федеральному управлінню з інформаційної безпеки (BSI). Законопроект також розширить можливості BSI щодо збору, зберігання та аналізу даних, включаючи виявлення діяльності, що вказує на підготовку до нападу, та зобов'яже телекомунікаційних провайдерів і великі цифрові платформи передавати користувачам попередження BSI про «конкретні небезпеки». Законопроект тепер передається до парламенту для обговорення і має бути схвалений законодавцями, перш ніж він зможе набути чинності». (*Ayhan Simsek. German government approves draft for new powers to fight cyber threats // Anadolu Ajansı* (<https://aa.com.tr/en/europe/german-government-approves-draft-for-new-powers-to-fight-cyber-threats/3949933>). 27.05.2026).

«...Австралія створила Раду з аналізу кіберінцидентів для проведення незалежних, безпричинних розслідувань значних кібератак на урядові та промислові об'єкти з метою винесення системних висновків та зміцнення національної стійкості. Рада, яку очолює глобальний керівник з інформаційної безпеки компанії Telstra Нарел Девайн і до складу якої входять переважно жінки з різних галузей, таких як авіація та юриспруденція, є відповіддю на нещодавні гучні випадки порушення безпеки в компаніях Medibank та Optus...

Створений за зразком розформованої Ради з питань кібербезпеки США, австралійський орган має ключову перевагу: юридичні повноваження вимагати інформацію від суб'єктів, які відмовляються співпрацювати, чого не мала його американська колега. Хоча робота американської ради, зокрема, сприяла масштабним культурним змінам у компанії Microsoft після розслідування великого китайського хакерського нападу, її зрештою було скасовано адміністрацією Трампа під час розслідування операції «Salt Typhoon». Приєднавшись до невеликої кількості юрисдикцій, таких як ЄС, що створили подібний механізм, Австралія прагне забезпечити, щоб кожна серйозна атака стала можливістю для навчання з метою зміцнення загальної кіберзахисту країни». *(Alexander Martin. Australia launches cyber review board modeled on version disbanded in US // Recorded Future News (<https://therecord.media/australia-launches-cyber-review-board>). 05.05.2026).*

«Дослідження, проведене на замовлення компанії Optus, виявило значний розрив у рівні готовності до кіберзахисту серед австралійських малих підприємств: лише 40% з них надають пріоритет цифровій безпеці, хоча кожне третє підприємство стикалося з кіберінцидентом. Результати показують, що 60% малих підприємств не мають офіційного плану реагування на кібератаки, і ця вразливість особливо гостро відчувається серед приватних підприємців, 79% яких не готові до таких ситуацій. Ця невідповідність значною мірою зумовлена помилковим відчуттям безпеки: понад половина власників бізнесу не вважають себе цілями атак, і в середньому малі підприємства приділяють лише дві години на місяць заходам з профілактики, тоді як кожне п'яте підприємство не витрачає на це часу взагалі...

Експерти попереджають, що малі підприємства дедалі частіше стають мішенню як «легка здобич», особливо з огляду на те, що інструменти штучного інтелекту роблять кібератаки більш автоматизованими та ситуативними. До найпоширеніших загроз належать фішинг та шахрайство через електронну пошту, а також шкідливе програмне забезпечення та видавання себе за надійних контактів. Коли трапляються такі інциденти, наслідки є значними: це призводить до ресурсомістких заходів з відновлення, перебоїв у роботі систем, що гальмують продуктивність, та прямих фінансових втрат. Окрім безпосередньої загрози з боку хакерів, підприємства також стикаються з посиленням регуляторним контролем. Управління комісара з питань інформації Австралії (OAIC) розпочало перевірки на відповідність вимогам, щоб переконатися, що політика конфіденційності відповідає

суворим законодавчим стандартам, зосередившись на секторах з високим ризиком, таких як нерухомість, аптеки та автосалони, які збирають конфіденційні особисті дані...

Щоб мінімізувати ці ризики, експерти рекомендують дотримуватися суворих правил безпеки щодо паролів, запровадити багатофакторну автентифікацію та інвестувати в навчання з питань кібербезпеки. З огляду на те, що брак часу та досвіду часто заважає власникам малого бізнесу вживати необхідних заходів, у рамках таких ініціатив, як програма Optus FutureFit, з кінця травня розпочинаються загальнонаціональні семінари за участю експертів, покликані допомогти підприємствам свідомо зміцнювати свою цифрову стійкість». (*Lilia Guan. Aussie small businesses still not prioritising cyber security // FoundryCo, Inc. (<https://www.arnnet.com.au/article/4167510/aussie-small-businesses-still-not-prioritising-cyber-security.html>). 06.05.2026*).

«Австралійські малі та середні підприємства стикаються зі стрімко зростаючими кіберзагрозами, при цьому залишаючись вкрай недостатньо підготовленими до їх відбиття. Австралійський центр кібербезпеки зареєстрував майже 94 000 повідомлень про кіберзлочини у 2023-2024 роках, що на 23% більше, ніж у попередньому році, проте багато МСП досі покладаються на застарілі системи, реактивні заходи безпеки або перевантажених внутрішніх співробітників замість спеціалізованих ресурсів з кібербезпеки. У міру того як підприємства продовжують цифровізацію та розширюють використання хмарних послуг, віддаленого доступу та підключених систем, їхня вразливість до кібератак відповідно зростає. Незважаючи на це, багато власників малих підприємств досі вважають, що їхні компанії занадто малі, щоб привернути увагу зловмисників, хоча насправді кіберзлочинці дедалі частіше обирають ціллю саме малі та середні підприємства, оскільки вони часто мають слабкішу систему захисту, погане управління оновленнями та обмежені можливості моніторингу...

Сучасні кіберзагрози, такі як програми-вимагачі, фішинг та компрометація ділової електронної пошти, є високоавтоматизованими і вже не залежать від розміру компанії. Влада неодноразово наголошувала, що багатьох інцидентів можна уникнути завдяки дотриманню базових заходів кібербезпеки, таких як багатофакторна автентифікація, своєчасне оновлення програмного забезпечення, безпечне резервне копіювання та постійний моніторинг кінцевих пристроїв. Однак ці заходи вимагають постійного управління та відповідальності. Наслідки кіберінцидентів для малих та середніх підприємств можуть бути серйозними і виходити за межі безпосереднього порушення операційної діяльності, включаючи шкоду репутації, регуляторні ризики, втрату клієнтів і навіть довгостроковий провал бізнесу. Крім того, великі клієнти та ланцюги постачання все частіше вимагають від компаній дотримання належних стандартів кібербезпеки, а це означає, що слабка безпека може безпосередньо вплинути на бізнес-можливості та контракти...

Оскільки створення повноцінного внутрішнього підрозділу з кібербезпеки часто є недосяжним для малих підприємств, постачальники послуг з керованих ІТ-

рішень, що пропонують інтегровані послуги з кібербезпеки, стають незамінними. Ефективні постачальники забезпечують безпеку у всьому ІТ-середовищі, включаючи хмарні системи, захист електронної пошти, управління ідентифікацією, захист кінцевих пристроїв та моніторинг мережі, одночасно здійснюючи постійний нагляд за загрозами. Такий проактивний підхід дозволяє підприємствам виявляти та локалізувати ризики до того, як вони переростуть у серйозні інциденти, а також гарантує працездатність систем резервного копіювання та відновлення у разі потреби. Кібербезпека також є найбільш ефективною, коли вона інтегрована в ширшу ІТ-стратегію, яка розвивається разом із зростанням компанії, включаючи довгострокове планування, аналіз ризиків, управління постачальниками та стратегічне керівництво. У міру того, як кіберзагрози стають все більш витонченими, а нормативні вимоги — жорсткішими, підприємства, які зволікають з інвестиціями у належний захист кібербезпеки, ризикують поставити під загрозу свою діяльність, дані та репутацію, тоді як ті, хто співпрацює з досвідченими постачальниками послуг з управління ІТ, можуть досягти надійного захисту без необхідності у бюджетах корпоративного рівня або великих внутрішніх командах».

(Why Australian SMEs can't afford to treat cybersecurity as an afterthought // TechDay (<https://securitybrief.com.au/story/why-australian-smes-can-t-afford-to-treat-cybersecurity-as-an-afterthought>). 22.05.2026).

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

«Нещодавно створена в Туреччині Рада з питань кібербезпеки проведе своє перше засідання у вівторок під головуванням президента Реджепа Таїпа Ердогана, на порядку денному якого стоїть національна дорожня карта з кібербезпеки. Обговорення будуть зосереджені на захисті критичної інфраструктури від кібератак та розвитку кадрового потенціалу у сфері кібербезпеки. До складу ради входять президент і віце-президент, ключові міністри (зокрема міністри юстиції, закордонних справ, внутрішніх справ, національної оборони, промисловості та технологій, а також транспорту та інфраструктури), високопосадовці з питань безпеки та розвідки, а також керівники відповідних органів оборони та кібербезпеки. Рада може запрошувати інших міністрів та експертів, а також утворювати комітети та робочі групи для виконання технічних завдань... До його повноважень належать розробка політики та стратегій у сфері кібербезпеки, формування технологічної дорожньої карти країни, запровадження стимулів та розвиток кадрового потенціалу. Засідання відбулося після створення Управління з питань кібербезпеки в січні 2025 року та ухвалення комплексного закону про кібербезпеку, який визначає національні стратегії та засновує раду, запроваджує покарання у вигляді позбавлення волі на строк до 12 років для осіб, які вчиняють кібератаки та отримують вигоду від викрадених даних, до 15 років за оприлюднення або продаж викрадених даних, а також штрафи для постачальників послуг, які не повідомляють про кібератаки або зловживання». *(Türkiye's cyber*

«За даними Адміністрації з питань кібербезпеки, минулого року державні органи повідомили про 726 інцидентів у сфері кібербезпеки, що дещо менше, ніж 755 випадків, зареєстрованих у попередньому році. Відповідно до чинних нормативних актів у сфері кібербезпеки, інциденти класифікуються за чотирма рівнями залежно від їхнього впливу на конфіденційність, цілісність та доступність, причому більшість зареєстрованих випадків віднесено до категорії низького рівня серйозності. Зокрема, 87,33% інцидентів були рівня 1, 9,78% — рівня 2 і 2,89% — рівня 3, тоді як інцидентів рівня 4 зафіксовано не було. Більшість атак (68,6%) становили несанкціоновані вторгнення, за ними йшли несправності обладнання, перебої в роботі сервісів та атаки на веб-сайти...

Адміністрація визначила кілька основних загроз кібербезпеці, з якими стикаються державні органи. До них належать: встановлення шкідливого програмного забезпечення на нещодавно придбані державні комп'ютери через підроблені месенджери; використання зловмисниками методів «bring-your-own-driver» для обходу засобів захисту та отримання несанкціонованого доступу; а також уразливості, що виникають через встановлення підрядниками з технічного обслуговування програмного забезпечення для віддаленого доступу на веб-сервери. Додаткові ризики пов'язані з уразливостями або неправильними налаштуваннями периферійних мережевих пристроїв, що може наражати системи на шкідливу діяльність...

Для протидії цим загрозам влада рекомендувала посилити контроль за встановленням програмного та апаратного забезпечення, а також додатків, проводити регулярні перевірки на наявність вразливостей, своєчасно встановлювати виправлення, впроваджувати брандмауери веб-додатків та оновлювати системи захисту кінцевих пристроїв. Державним установам також було рекомендовано посилити управління безпекою постачальників, зокрема контроль доступу, захист даних, повідомлення про інциденти та регулярні аудити кібербезпеки. Інші рекомендовані заходи включають використання білих списків для зовнішніх підключень, блокування непотрібних мережевих портів, підтримку оновленого прошивання на периферійних пристроях, впровадження систем фільтрації електронної пошти та пісочниці, обмеження дозволів на спільний доступ у хмарі та сканування завантажених файлів на наявність загроз...

Адміністрація також наголосила на важливості забезпечення надійних резервних копій, систем дублювання та засобів відновлення, а також проведення регулярних навчань із забезпечення безперебійної роботи для гарантування швидкого відновлення систем у надзвичайних ситуаціях. З метою підвищення стійкості Міністерство цифрових технологій заохочує використання зашифрованих розподілених резервних копій для критично важливої державної інфраструктури у декількох хмарних середовищах, щоб зменшити ризики, пов'язані з наявністю єдиних точок відмови». (*Shelley Shan. Agencies report 726 cybersecurity incidents*

«Національне агентство Індії з реагування на кіберзагрози — Індійська команда реагування на комп'ютерні надзвичайні ситуації (CERT-In) — опублікувало комплексний план під назвою «План щодо зменшення вразливості та захисту від експлуатації вразливостей у цифровій інфраструктурі за допомогою штучного інтелекту», в якому застерігає, що штучний інтелект кардинально та стрімко змінює ландшафт кіберзагроз, що вимагає термінових і структурних змін у підході організацій до кіберзахисту. У плані кіберзловживання за допомогою ШІ визначено як зростаючу та прискорювану загрозу для взаємопов'язаної цифрової інфраструктури, хмарних екосистем, операційних технологій та ланцюгів постачання програмного забезпечення, причому зловмисники дедалі частіше використовують ШІ для автоматизації розвідки, виявлення вразливостей, фішингу, створення шкідливого програмного забезпечення, розробки експлойтів та проведення масштабних атак, що значно скорочує час, необхідний для виявлення та використання слабких місць... Атаки з використанням штучного інтелекту стають дедалі більш автономними на різних етапах кібернетичного ланцюга атак, включаючи розвідку, експлуатацію вразливостей, горизонтальне переміщення та витік даних, тоді як поява автономних систем штучного інтелекту відкриває перспективу проведення повністю автоматизованих багатоетапних операцій у надзвичайно стислі терміни. Особливе занепокоєння викликає зростаюче використання штучного інтелекту для створення надзвичайно переконливого фішингового контенту, голосових та відеошахрайств на основі технології «діпфейк», синтетичних ідентичностей та персоналізованих кампаній соціального інжинірингу, які завдяки своєму реалізму та контекстуальній точності здатні обходити традиційні механізми виявлення, що базуються на обізнаності. У документі також міститься попередження про значне зниження технічних бар'єрів для входу на ринок, що дозволить навіть нефахівцям або напівкваліфікованим зловмисникам здійснювати масштабні складні атаки, тоді як організації, що впроваджують системи штучного інтелекту, стикаються зі зростаючими ризиками, зокрема з введенням шкідливого коду, маніпулюванням моделями, отруєнням навчальних даних, крадіжкою моделей штучного інтелекту та компрометацією конвеєрів оркестрування штучного інтелекту. Визначено, що життєво важливі сектори, зокрема урядовий, фінансовий, телекомунікаційний, медичний, енергетичний, транспортний, виробничий та сектор цифрової громадської інфраструктури, наражаються на підвищений ризик, потенційні наслідки якого включають порушення операційної діяльності, фінансове шахрайство, компрометацію конфіденційної інформації та ширші наслідки для національної безпеки... У відповідь на ці загрози CERT-In закликає організації рішуче відмовитися від періодичних оцінок та підходів до безпеки, орієнтованих на захист периметра та дотримання нормативних вимог, на користь безперервного управління ризиками, адаптивного захисту, операцій на основі аналітики та

практик кібербезпеки, спрямованих на забезпечення стійкості. У цьому плані рекомендується низка конкретних стратегічних принципів, зокрема: прийняття підходу «виходити з припущення про злом» для забезпечення швидкого виявлення, локалізації та відновлення; впровадження моделі безпеки «нульової довіри» шляхом постійної верифікації, доступу з мінімальними привілеями та мікросегментації; вбудовування безпеки в системи з самого початку за допомогою підходів «безпека за замовчуванням» та «безпека за задумом»; узгодження засобів захисту з тактиками супротивника шляхом інтеграції розвідданих про загрози та використання «червоної команди»; а також захист даних протягом усього їхнього життєвого циклу за допомогою класифікації, шифрування та управління доступом...» (*Anna Ribeiro. CERT-In warns AI-assisted adversaries amplifying lateral movement, exploitation, data exfiltration across critical systems // Industrial Cyber* (<https://industrialcyber.co/ai/cert-in-warns-ai-assisted-adversaries-amplifying-lateral-movement-exploitation-data-exfiltration-across-critical-systems/>). 27.05.2026).

Ізраїль, Туреччина та країни Близького сходу

«Нещодавно створена в Туреччині Рада з питань кібербезпеки проведе своє перше засідання у вівторок під головуванням президента Реджепа Таїпа Ердогана, на порядку денному якого стоїть національна дорожня карта з кібербезпеки. Обговорення будуть зосереджені на захисті критичної інфраструктури від кібератак та розвитку кадрового потенціалу у сфері кібербезпеки. До складу ради входять президент і віце-президент, ключові міністри (зокрема міністри юстиції, закордонних справ, внутрішніх справ, національної оборони, промисловості та технологій, а також транспорту та інфраструктури), високопосадовці з питань безпеки та розвідки, а також керівники відповідних органів оборони та кібербезпеки. Рада може запрошувати інших міністрів та експертів, а також утворювати комітети та робочі групи для виконання технічних завдань... До його повноважень належать розробка політики та стратегій у сфері кібербезпеки, формування технологічної дорожньої карти країни, запровадження стимулів та розвиток кадрового потенціалу. Засідання відбулося після створення Управління з питань кібербезпеки в січні 2025 року та ухвалення комплексного закону про кібербезпеку, який визначає національні стратегії та засновує раду, запроваджує покарання у вигляді позбавлення волі на строк до 12 років для осіб, які вчиняють кібератаки та отримують вигоду від викрадених даних, до 15 років за оприлюднення або продаж викрадених даних, а також штрафи для постачальників послуг, які не повідомляють про кібератаки або зловживання». (*Türkiye's cyber security board holds inaugural meeting // Daily Sabah* (<https://www.dailysabah.com/politics/turkiyes-cyber-security-board-holds-inaugural-meeting/news>). 04.05.2026).

«...ОАЕ запустили «UAE Cyber Factory» — ініціативу з кібербезпеки на базі штучного інтелекту, покликану захистити національний цифровий суверенітет країни від вражаючої кількості щоденних кібератак, яка сягає 800 000. Ця платформа, презентована Радою з кібербезпеки ОАЕ та компанією CRX Holdings на виставці «Make it in the Emirates», використовує штучний інтелект для суттєвого покращення виявлення загроз, прискорення часу реагування та зміцнення державних систем і критичної інфраструктури. Цей проект знаменує стратегічний зсув у бік створення суверенної, локальної екосистеми талантів та інновацій, що відображає більш широку тенденцію серед країн Перської затоки до зменшення залежності від іноземних технологій безпеки. У міру того, як глобальні загрози енергетичним мережам та фінансовим системам стають все більш автоматизованими та витонченими, ОАЕ позиціонують себе як центр передової кіберзахисту, орієнтованого на штучний інтелект, щоб випереджати дедалі складніші шкідливі програми та методи...» *(Mandi Kogosowski. UAE Launches AI-Powered Cyber Factory to Strengthen Digital Sovereignty // Arrowmedia Israel Ltd. (<https://www.israeldefense.co.il/en/node/68937>). 11.05.2026).*

«Оскільки штучний інтелект знижує бар'єри для здійснення масштабних складних кібератак, критична інфраструктура стає головним об'єктом атак, а здатність ОАЕ протистояти загрозам на основі штучного інтелекту розглядається як обнадійливий фактор і водночас як ознака посилення тиску. Голова урядового агентства з кібербезпеки ОАЕ д-р Мохамед Аль-Кувейти повідомляє, що зараз у країні фіксується близько 530 000 кіберінцидентів на день, що на 270 000 більше, ніж до останнього загострення ситуації, підкреслюючи, що традиційна оборона, зосереджена на периметрі, не може встигати за швидкими, адаптивними супротивниками, що використовують штучний інтелект... У високоцифрових, взаємопов'язаних економіках атаки на критичну національну інфраструктуру розглядаються як події, що стосуються громадської безпеки та національної безпеки, а не як ІТ-проблеми, що зміщує пріоритети з простого запобігання порушенням безпеки на розробку систем, покликаних обмежити збитки у разі їхнього виникнення. У статті стверджується, що багато середовищ ОТ у країнах Перської затоки все ще покладаються на застарілі моделі безпеки, які не відповідають сучасним загрозам, де зловмисники можуть проводити розвідку зі швидкістю машини, адаптувати обхідні заходи та постійно перевіряти захист. У ній пропагується стратегія «припущення про порушення», зосереджена на стійкості та локалізації: забезпечення видимості підключених активів ОТ та потоків даних у реальному часі, впровадження сегментації та підключення з мінімальними привілеями для запобігання побічному переміщенню, а також використання принципів Zero Trust для обмеження масштабів поширення будь-якого порушення... Оскільки безперебійність роботи має вирішальне значення, у звіті рекомендується проводити поетапну модернізацію з використанням архітектур накладення, які дозволяють забезпечити сегментацію без заміни застарілих систем та без перебоїв у роботі, а також закликається керівництво оцінювати успішність за показниками стійкості, такими як радіус ураження, час локалізації та доступність

послуг під час інцидентів. У зв'язку з прискоренням темпів цифрової трансформації в країнах Перської затоки головне завдання полягає в тому, щоб використовувати досвід ОАЕ як регіональний орієнтир і створювати інфраструктуру, призначену для локалізації порушень, збереження життєво важливих послуг та швидкого відновлення роботи». (*Sam Tayan. In the age of AI cyberattacks, prevention is no longer enough // Al Nisr Publishing LLC (<https://gulfnews.com/opinion/op-eds/in-the-age-of-ai-cyberattacks-prevention-is-no-longer-enough-1.500544318>). 18.05.2026*).

Країни Африки

«Швидко зростаюча цифрова економіка Нігерії наразі стикається з серйозною кризою у сфері кібербезпеки, яка характеризується понад 4 000 кібератак щотижня. Д-р Вінсент Олатунджі, національний комісар Комісії з захисту даних Нігерії (NDPC), нещодавно наголосив на тривожному масштабі цих загроз, зазначивши, що сама NDPC щотижня стикається з понад 1 500 спробами атак на власну мережу. Хоча такі сектори, як фінтех, електронна комерція та хмарні послуги, сприяють значному економічному зростанню, ця цифрова трансформація одночасно збільшила вразливість країни до фінансових втрат, витоків даних та шкоди репутації, викривши критичний пробіл у готовності країни виявляти загрози та реагувати на них...

Основною проблемою, на яку вказала NDPC, є надмірна залежність Нігерії від іноземної інфраструктури для зберігання даних: понад 90% даних, що генеруються в країні, наразі зберігаються за кордоном. Така залежність породжує серйозні проблеми у сфері національної безпеки, витрат та регуляторного контролю. Щоб відновити цифровий суверенітет, Олатунджі наголосив, що дані, які генеруються в Нігерії, повинні зберігатися та оброблятися на місцевому рівні. Комісія займає тверду позицію з цього питання, чітко роз'яснюючи, що зберігання даних є формою обробки даних відповідно до закону. Отже, центри обробки даних та всі організації, що працюють з даними, повинні дотримуватися суворих стандартів захисту або зіткнутися з серйозними наслідками, включаючи потенційні штрафи у розмірі до двох відсотків від їх валового доходу та притягнення до відповідальності керівників...

З метою забезпечення цифрового майбутнього країни NDPC виступає за стратегічний поворот, що передбачає збільшення інвестицій у системи кібербезпеки, людський капітал та надійні технічні засоби захисту від ризиків, пов'язаних із штучним інтелектом та Інтернетом речей. Оскільки, за прогнозами, до 2031 року ринок інфраструктури даних Нігерії перевищить 1 мільярд доларів, комісія підкреслює, що захист даних є необхідним не тільки для підтримання національної безпеки, але й як фундаментальна «валюта довіри», необхідна для підтримання міжнародної конкурентоспроможності, забезпечення дотримання нормативних вимог та сприяння довгостроковому сталому розвитку». (*Juliet Umeh. NDPC: 4,000 weekly cyberattacks push data localisation, stricter compliance //*

Vanguard Media Limited (<https://www.vanguardngr.com/2026/05/ndpc-4000-weekly-cyberattacks-push-data-localisation-stricter-compliance/>). 02.05.2026).

«Ініціатива Microsoft «Advancing Regional Cybersecurity» (ARC), започаткована у 2025 році, зосереджується на людських факторах та управлінських рішеннях, які визначають, чи здатна країна впоратися з серйозним кіберінцидентом — зокрема, хто керує процесом, як відбувається обмін інформацією, коли втручається уряд та як забезпечується функціонування життєво важливих служб і підтримка суспільної довіри. Першим конкретним результатом цієї ініціативи є «Звіт та набір інструментів щодо навчань ARC у Кенії», підготовлений за підсумками навчань, що відбулися в грудні 2025 року в Найробі та були розроблені спільно з Національним комітетом з координації боротьби з комп'ютерними та кіберзлочинами (NC4) та компанією RiskSight... Ці навчання були розроблені з метою перевірки на міцність лідерських якостей та міжвідомчого процесу прийняття рішень в умовах тиску, а не для оцінки технічних засобів; для цього використовувалися такі сценарії, як злом систем із застосуванням штучного інтелекту, атаки програм-вимагачів та порушення роботи інфраструктури. У ході навчань були виявлені прогалини в питаннях повноважень, надійних каналів зв'язку та спільних механізмів реагування. Створений на основі цього інструментарій перетворює ці уроки на практичний 12-місячний план дій для посилення національної готовності шляхом уточнення ролей керівництва під час інцидентів, встановлення моделей реагування та посібників, що відповідають стандартам, покращення оперативної готовності та шляхів ескалації між секторами та центрами операцій з безпеки, а також поглиблення надійного обміну інформацією між державним та приватним секторами за допомогою загальних правил обробки, безпечніших механізмів добросовісного повідомлення та регулярних спільних навчань. Хоча цей підхід розроблено з урахуванням швидкозростаючої цифрової економіки Кенії, відомої як «Силіконова Савана», та її дедалі більшої вразливості до кіберзагроз, його позиціонують як такий, що може бути застосований в інших країнах «Глобального Півдня», які стикаються з проблемою роздробленості власності на інфраструктуру та нерівномірного рівня кіберпотенціалу. Компанія Microsoft зазначає, що розширює діяльність ARC на інші регіони, зокрема започатковує новий напрям роботи в Мексиці». (*Kaja Ciglic. Strengthening cyber capacity in Kenya: A new toolkit with lessons for the region // Microsoft (<https://blogs.microsoft.com/on-the-issues/2026/05/04/strengthening-cyber-capacity-in-kenya-a-new-toolkit-with-lessons-for-the-region/>). 04.05.2026).*

«Наразі Сенегал стикається зі сплеском кібератак на державні установи, причому нещодавній злом системи Державного казначейства став третім серйозним інцидентом за менш ніж шість місяців. Це сталося після гучного злом податкової служби наприкінці 2025 року та масштабного викрадення даних у січні 2026 року в Міністерстві внутрішніх справ, де хакери, як стверджується, викрали 139 терабайтів даних, що охоплюють усе населення країни. Експерти припускають,

що зростаюча міжнародна популярність Сенегалу та нещодавно виявлені родовища нафти й газу зробили країну привабливою мішенню для кіберзлочинних угруповань, які прагнуть визнання. Ця тенденція відображає загальну ситуацію в Африці, де організації зараз стикаються в середньому з 2 940 атаками на тиждень — це найвищий показник у світі — що зумовлено швидкою цифровізацією та нерівномірним рівнем зрілості систем безпеки...

Окрім державних установ, континент стикається з поширеною кіберзлочинністю, яка зачіпає пересічних громадян, зокрема через онлайн-шахрайство, програми-вимагачі та нову загрозу — обман за допомогою «дідфейків», створених за допомогою штучного інтелекту. У відповідь на це міжнародні ініціативи, такі як операція Інтерполу «Серенгеті 2.0», почали боротися зі злочинними мережами, що у 2025 році призвело до понад 1 200 арештів та повернення майже 100 мільйонів доларів. Однак фахівці з безпеки стверджують, що справжня кіберстійкість вимагає не лише реактивних заходів. Вони закликають африканські уряди вийти за межі споживання іноземних технологій і натомість створити комплексну, суверенну «архітектуру кіберстійкості». Це включає створення сучасних правових рамок, масштабних програм навчання та регіональної співпраці для захисту критичної інфраструктури та забезпечення виявлення загроз у режимі реального часу за допомогою національних команд реагування на надзвичайні ситуації». (*Zeenat Hansrod. As Africa rapidly goes digital, it becomes a prime target for hackers // France Médias Monde (<https://www.rfi.fr/en/africa/20260515-as-africa-rapidly-goes-digital-it-becomes-a-prime-target-for-hackers>). 15.05.2026*).

Кіберстрахування

«Світовий ринок кіберстрахування перебуває на критичному роздоріжжі, стикаючись із різким зростанням попиту, спричиненим рекордним рівнем серйозності кіберінцидентів, особливо у США. З огляду на те, що середня вартість витоку даних в Америці у 2025 році сягне 10,2 млн доларів, виникла вражаюча «аномалія ціноутворення»: хоча оцінка збитків стрімко зростає, страхові премії знизилися приблизно на 30% порівняно з піковим рівнем 2022 року. Ця розбіжність відбувається на тлі значних змін на ринку, зокрема придбання Zurich Insurance Group за 11 млрд доларів компанії Beazley, інноватора в цій галузі. Цей крок розглядається як спроба скористатися сприятливою ситуацією на ринку для забезпечення висококласної кіберекспертизи, хоча експерти сумніваються, що це спричинить ширшу хвилю консолідації галузі...

Однією з головних проблем для страховиків залишається «ризик сукупності» — ймовірність масштабних одночасних атак, особливо в умовах загострення геополітичної напруженості, наприклад, у конфлікті між США та Іраном. Цей ризик ускладнюється тим, що важко провести межу між кіберзлочинністю та кібервійною, що ведеться за підтримки держави, оскільки остання, як правило, виключається зі стандартних полісів як «акт війни». Недавні інциденти, такі як

атака з використанням вірусу-віпера «Stryker», ще раз підкреслили необхідність чіткішого формулювання виключень, пов'язаних з війною...

Окрім технічних загроз, галузь також стикається з поширенням масових арбітражних розглядів та судових спорів із третіми сторонами, які як страховики, так і страхувальники тепер визнають глобальною проблемою, а не лише проблемою, що стосується США. Хоча в США рівень проникнення кіберстрахування наразі становить 40%, Велика Британія відстає, маючи лише 10%, що свідчить про те, що майбутнє зростання ринку, ймовірно, буде зумовлене новими державними нормами. Крім того, штучний інтелект є наступним важливим напрямком, що зрештою призведе до появи окремого страхування, пов'язаного з ШІ. Зрештою, ринок кіберстрахування намагається залишатися гнучким у швидко мінливому середовищі загроз, де десятиліттями усталені галузеві практики дедалі частіше стикаються з викликами, пов'язаними зі швидкістю сучасних цифрових ризиків». (*Deborah Ritchie. Cyber Insurance: Marginal No More // Global Finance Magazine* (<https://gfmag.com/insurance/cyber-insurance-marginal-no-more/>). 06.05.2026).

«Штучний інтелект кардинально змінює галузь кіберстрахування, суттєво збільшуючи як частоту, так і рівень складності кібератак, що змушує страховиків переглядати моделі ризиків і підвищувати страхові премії. Зараз кіберзлочинці використовують ШІ для автоматизації фішингових кампаній, створення переконливих діпфейків, злому паролів та швидкого виявлення вразливостей зі швидкістю та в масштабах, з якими традиційні засоби захисту часто не можуть зрівнятися. Адаптивний та непередбачуваний характер загроз, що базуються на ШІ, — таких як шкідливе програмне забезпечення, яке навчається на невдалих спробах та змінює свою поведінку в режимі реального часу, — значно ускладнює страховикам точну оцінку потенційних збитків, що призводить до підвищення страхових премій для компенсації цієї невизначеності...

Зростаюча залежність організацій від систем штучного інтелекту в сфері обслуговування клієнтів, аналізу даних та прийняття оперативних рішень також створила нові внутрішні вразливості. Наразі страхові компанії ретельно оцінюють систему управління штучним інтелектом, політику кібербезпеки, рівень підготовки персоналу та загальну зрілість системи безпеки компанії перед тим, як встановлювати страхові премії. На ціноутворення додатково впливає регуляторний тиск, оскільки все більш суворі закони щодо захисту даних та управління штучним інтелектом у всьому світі наражають підприємства, що не дотримуються вимог, на значні штрафи та юридичну відповідальність, особливо в таких регульованих секторах, як охорона здоров'я, банківська справа та фінанси...

У відповідь на це страхові компанії, що спеціалізуються на кіберстрахуванні, відходять від традиційних анкет і переходять до моніторингу в режимі реального часу, аналізу ризиків на основі штучного інтелекту та постійної оцінки безпеки. Компанії, які демонструють ефективні практики кібербезпеки, зокрема багатофакторну автентифікацію, регулярні оновлення, надійне управління

ризиками за допомогою штучного інтелекту та чіткі механізми управління, можуть розраховувати на нижчі страхові премії та вигідніші умови.

Підсумовуючи, можна сказати, що стрімка еволюція загроз, пов'язаних зі штучним інтелектом, змушує галузь кіберстрахування кардинально переглянути підходи до оцінки та ціноутворення ризиків, а також спонукає організації серйозніше інвестувати в кібербезпеку та відповідальне управління штучним інтелектом, щоб контролювати витрати та захищати себе у дедалі складнішому цифровому середовищі». (*Naveen Goud. How AI Cyber Threats are influencing Cyber Insurance Premium Costs // Cybersecurity Insiders (<https://www.cybersecurity-insiders.com/how-ai-cyber-threats-are-influencing-cyber-insurance-premium-costs/>). 22.05.2026*).

«Згідно з новим дослідженням компанії WFI Insurance, лише чверть австралійських фермерів розглядають кіберстрахування як необхідність у майбутньому, незважаючи на те, що близько 80% фермерських господарств вже використовують агротехнології. Цей показник значно нижчий за 70%, які серед підприємств інших галузей розглядають можливість укладення кіберстрахування, що свідчить про явний розрив між зростаючою цифровою залежністю сектору та рівнем управління кіберризиками...

У міру того як сільськогосподарські підприємства все частіше впроваджують підключену до мережі техніку, автоматизовані системи, інтелектуальні системи зрошення, роботизоване доїння, системи моніторингу зерна та інструменти на основі аналізу даних, їхня вразливість до кіберзагроз суттєво зросла. Кіберінциденти тепер можуть безпосередньо порушувати фізичні операції — наприклад, затоплювати посіви, захоплювати контроль над автоматизованими тракторами, викрадати цінний генетичний матеріал худоби або компрометувати системи зберігання зерна — що призводить до значних фінансових втрат, тривалих простоїв у критичні періоди, такі як збір врожаю, порушення ланцюгів постачання та потенційного впливу на продовольчу безпеку.

Генеральний директор WFI Дем'єн Галлахер охарактеризував кіберризик як «невидиму» загрозу для багатьох фермерів порівняно з традиційними ризиками на фермах, тоді як доктор Кайл Мулруні з Центру сільської кримінології Університету Нової Англії попередив, що розширення автоматизації та збору даних різко збільшило площу атаки. Незважаючи на те, що середня вартість кіберзлочинів для малих підприємств за останній рік зросла на 50% до 56 000 доларів, лише близько 20% австралійських МСП на даний момент мають кіберстрахування...

WFI зазначила, що продукти кіберстрахування еволюціонували і тепер поєднують фінансовий захист із засобами профілактики, постійним скануванням безпеки та цілодобовою підтримкою у разі інцидентів. Щоб зменшити ризики, страховик рекомендує використовувати надійні паролі та багатофакторну автентифікацію, зберігати резервні копії в офлайн-режимі, оновлювати всі пристрої та розумне обладнання, розділяти операційні та офісні мережі, навчати персонал та родичів розпізнавати шахрайство, розробляти простий план реагування на інциденти та ставитися до кіберризиків так само серйозно, як і до інших ризиків

фермерського господарства, шляхом належної підготовки та планування безперебійної діяльності». (*Mav Rodriguez. Only 1 in 4 Aussie farmers eye cyber cover as 'smart' farms become hacker targets // KM Business Information Australia Pty Ltd (<https://www.insurancebusinessmag.com/au/news/breaking-news/only-1-in-4-aussie-farmers-eye-cyber-cover-as-smart-farms-become-hacker-targets-576345.aspx>). 25.05.2026*).

«Рада з кібербезпеки ОАЕ наголосила на зростаючому значенні кіберстрахування на тлі стрімкого поширення цифрової трансформації та ускладнення кіберзагроз, спрямованих проти фізичних осіб та організацій. Обсяг ринку кіберстрахування в ОАЕ оцінюється приблизно в 70 мільйонів доларів США, що свідчить про підвищення обізнаності щодо управління цифровими ризиками в умовах постійного зростання залежності від технологічних рішень у різних секторах. Рада підкреслила, що кіберстрахування стало важливим інструментом для пом'якшення фінансових та операційних наслідків кіберінцидентів, таких як порушення систем безпеки, витік даних та перебої у роботі цифрових послуг. Покриття зазвичай включає розслідування інцидентів, відновлення даних, юридичну відповідальність та вимоги про відшкодування збитків, що допомагає організаціям швидше відновлюватися та мінімізувати фінансові втрати. Рада прогнозує, що в найближчі роки страхові премії значно зростуть через збільшення масштабів та складності кіберзагроз, особливо з огляду на те, що в атаках дедалі частіше використовуються передові технології, такі як штучний інтелект та соціальна інженерія... Наразі близько 80 відсотків установ та компаній в ОАЕ визнають кіберстрахування невід'ємною частиною своїх стратегій управління ризиками. Водночас Рада наголосила, що кіберстрахування має доповнювати, а не замінювати основні заходи з кібербезпеки в рамках комплексної системи захисту. Вона підкреслила важливість кіберстрахування в таких критично важливих секторах, як фінансові послуги, охорона здоров'я та енергетика, де кібератаки можуть порушити функціонування життєво важливих послуг або поставити під загрозу конфіденційні дані, що призведе до фінансових збитків та шкоди репутації. Крім того, кіберстрахування сприяє дотриманню нормативних стандартів, оскільки багато страховиків вимагають від організацій впровадження мінімальних заходів кібербезпеки перед наданням страхового покриття. У перспективі Рада очікує більшої інтеграції між страховими компаніями та фірмами з кібербезпеки, що поєднуватиме послуги з профілактики, страхування та реагування на інциденти. Очікується, що аналіз даних також відіграватиме дедалі важливішу роль в оцінці ризиків та ціноутворенні полісів, адаптованих до потреб організацій. Зрештою, Рада наголосила, що ефективна кібербезпека сьогодні виходить за межі технічних інструментів і включає можливості швидкого реагування, що мінімізують збитки, підтримують безперебійність бізнесу та зміцнюють довіру до цифрового середовища». (*Huda Ata. UAE cyber insurance market reaches \$70 million amid rising digital threats // Al Nisr Publishing LLC (<https://gulfnnews.com/uae/uae-cyber-insurance-market-reaches-70-million-amid-rising-digital-threats-1.500551611>). 24.05.2026*).

«Під час війни між Ізраїлем та Іраном у червні 2025 року удар балістичною ракетою поблизу Тель-Авівського університету завдав фізичної шкоди Інституту досліджень національної безпеки (INSS), проте в кіберпросторі вже тривала паралельна атака, яка тривала набагато довше. Згідно з розслідуванням газети «Гаарец», заснованим на понад 99 000 викрадених електронних листів, файлів та повідомлень WhatsApp, пов'язана з Іраном хакерська група Handala — яку США визнали прикриттям для Міністерства розвідки Ірану — проводила багаторічну кіберкампанію проти INSS, опублікувавши за останні місяці понад 100 000 викрадених документів. Операція розпочалася щонайменше ще у 2019 році і переросла у масштабну розвідувальну діяльність, яка не тільки збирала конфіденційні дані, але й, як стверджується, підтримувала операції з впливу, фішингові кампанії та навіть спроби замахів на ізраїльських діячів, зокрема високопоставлених чиновників INSS...

Хоча INSS формально є незалежним аналітичним центром, багато його дослідників — це колишні високопосадовці ізраїльських розвідувальних та оборонних відомств, а інститут підтримує тісні зв'язки з урядовими органами, що робить його надзвичайно цінною ціллю. Серед викрадених матеріалів — адміністративні дані, а також конфіденційна інформація, така як паролі до камер відеоспостереження, мереж Wi-Fi, облікових записів Zoom і навіть код доступу до будівлі, а також дані, що дозволяють ідентифікувати військовослужбовців, дипломатів та посадовців НАТО. Документи описують стійкий «ланцюг зараження», в якому іранські агенти видавали себе за співробітників, зламували електронні поштові акаунти, витікали матеріали до публікації як приманку та неодноразово атакували дослідників і видатних ізраїльтян фішинговими атаками. У деяких випадках зламані акаунти нібито використовувалися для заманювання чиновників за кордон у рамках ймовірних планів викрадення. До 2024 року кампанія переросла у фізичну площину, і ізраїльські власті висунули звинувачення проти місцевих агентів, яких звинувачували у стеженні за дослідником INSS, якого іранські куратори нібито намагалися вбити.

Витік інформації також свідчить про участь INSS у проектах з впливу та протидії впливу, зокрема у співпраці з ізраїльськими міністерствами та службами безпеки щодо моніторингу іранських мереж та глобальних кампаній впливу. Незважаючи на допомогу з боку приватних компаній з кібербезпеки та Національного кібердиректорату Ізраїлю, критики зазначають, що захисні заходи інституту були недостатніми, що поставило колишніх співробітників розвідки та дослідників у вразливе становище. Експерти, на яких посиляється Haaretz, описують цей випадок як доказ «очевидної прогалини в захисті», особливо щодо захисту приватних пристроїв та облікових записів колишніх високопосадовців, які не підпадають під офіційні рамки державної безпеки. Хоча INSS заявляє, що не зберігає секретних матеріалів і посилює свою кіберзахист, цей випадок підкреслює стратегічну вразливість напівофіційних інституцій, що працюють на стику досліджень та національної безпеки, а також те, як тривалі кібероперації можуть безпосередньо сприяти виникненню реальних загроз...» (*Omer Benjakob. Hack,*

Leak and Attack: How Iran Penetrated Israel's Top Security Think Tank // Haaretz Daily Newspaper Ltd. (<https://www.haaretz.com/israel-news/security-aviation/2026-05-04/ty-article-magazine/.premium/hack-leak-and-attack-how-iran-penetrated-israels-top-security-think-tank/0000019d-f2da-ded7-a99d-fedfb8260000>). 04.05.2026.

«Кількість кібератак у Сполучених Штатах зростає, що все частіше призводить до збою роботи критичної інфраструктури та служб державних і місцевих органів влади. Про це свідчать такі інциденти, як атака з використанням програм-вимагачів, яка змусила водоочисну станцію в місті Мінот (штат Північна Дакота) працювати в ручному режимі протягом 16 годин, а також неодноразові відключення систем у окрузі Вінона (штат Мінесота), що змусило губернатора задіяти Національну гвардію. Ці події свідчать про те, що зловмисники шукають слабкі місця в різних юрисдикціях, і хоча деякі штати почали реагувати на це посиленням координації та запровадженням більш суворих стандартів, багато хто відстає, що підкреслює необхідність прийняття штатами перевірених моделей... Штат Техас став одним із першопрохідців у цій сфері, запустивши в червні 2025 року загальнодержавний Центр кібербезпеки, покликаний централізувати управління вразливостями, підготовку кадрів та оперативне реагування на інциденти, а також налагодивши партнерські відносини з такими університетами, як Техаський університет у Сан-Антоніо, з метою формування кадрового резерву фахівців з кібербезпеки. У відповідь на дороговартісний витік даних, внаслідок якого були оприлюднені тисячі файлів, штат Невада у лютому 2026 року затвердив загальнодержавну політику класифікації даних, встановивши чіткі категорії для стандартизації підходів державних органів до захисту інформації та усунення розбіжностей у практиках... У березні 2026 року штат Міссісіпі створив Державний оперативний центр безпеки з метою координації безперервного моніторингу та реагування між відомствами, а також поєднав його з програмою підготовки фахівців за участю державних університетів та місцевих коледжів. У квітні 2026 року штат Західна Вірджинія ухвалив закон, який уповноважує його керівника з інформаційної безпеки (CISO) впроваджувати єдині загальнодержавні політики з кібербезпеки, що відповідають найкращим практикам, замінивши тим самим ситуативні підходи окремих відомств та зменшивши залежність від конкретних постачальників завдяки технологічно нейтральним стандартам. У квітні 2026 року штат Мен виніс на розгляд законопроект, який зобов'язує лікарні впровадити плани з кібербезпеки, що відповідають вимогам CISA, а також процедури звітності, резервного копіювання, навчання персоналу та забезпечення безперервності надання медичної допомоги, щоб запобігти перебоям у лікуванні пацієнтів під час відключень... Штат Нью-Йорк запровадив нові правила для об'єктів водоочищення, які передбачають проведення навчання, управління вразливістю, постійний моніторинг, контроль доступу та планування дій на випадок надзвичайних ситуацій. Ці заходи супроводжуються грантом у розмірі 2,5 мільйона доларів та програмою підтримки, покликаними допомогти комунальним підприємствам оцінити та модернізувати системи захисту. У сукупності ці приклади пропонують іншим штатам наступний алгоритм дій: встановити чіткі

стандарти, створити єдині оперативні структури, інвестувати у підготовку кадрів, а також поширити відповідні вимоги та підтримку на всю критичну інфраструктуру, обмінюючись при цьому ефективними підходами для зміцнення загальної національної стійкості». (*David Kertai. States Should Learn From Each Other to Close Cybersecurity Gaps // Information Technology & Innovation Foundation (<https://itif.org/publications/2026/05/04/states-should-learn-from-each-other-to-close-cybersecurity-gaps/>). 04.05.2026*).

«Компанія Rapid7 повідомляє, що пов'язана з іранською державою зловмисна група MuddyWater з початку 2026 року проводила тривалу хакерську кампанію під чужим прапором, спрямовану проти організацій у США та інших країнах, намагаючись видати ці вторгнення за атаки групи Chaos, що надає послуги з викрадення даних (RaaS). В ході операції використовувалися методи соціальної інженерії через Microsoft Teams для зв'язку зі співробітниками, ініціювання сеансів спільного доступу до екрану та обману жертв з метою введення ними облікових даних у локально створений текстовий файл, що дозволило зловмисникам зібрати логіни та обійти багатофакторну аутентифікацію... Компанія Rapid7 попереджає, що маскуванню державної операції під виглядом програм-вимагачів може ввести захисників в оману, змусивши їх розглядати інциденти як кіберзлочини з фінансовою мотивацією, що сповільнить процес встановлення відповідальності та ускладнить реагування, надаючи зловмиснику можливість переконливо заперечувати свою причетність. Кампанія, судячи з усього, спрямована на стратегічно важливі цілі, зокрема деякі урядові структури, і для забезпечення стійкості використовувала DWAgent разом із спеціальним трояном віддаленого доступу, ідентифікованим як Game.exe. Хоча Chaos — активний з 2025 року та відомий голосовим фішингом та підробкою ІТ-персонажів — з'явився після того, як правоохоронні органи зруйнували інфраструктуру програм-вимагачів BlackSuit/Royal, Rapid7 стверджує, що діяльність MuddyWater має ознаки, пов'язані з Міністерством розвідки та безпеки Ірану. Телеметрія вказує на цілі за межами США, зокрема на Близькому Сході та в Південній Азії, з ідентифікованими жертвами в таких місцях, як Йорданія та Австралія». (*David Jones. Iran-sponsored threat group behind false flag social engineering campaign // TechTarget, Inc. (<https://www.cybersecuritydive.com/news/iran-threat-group-false-flag-social-engineering/819454/>). 06.05.2026*).

«Геополітичні конфлікти стали основними індикаторами кіберризиків як для державних, так і для приватних організацій, оскільки сучасні напруження між національними державами дедалі частіше поширюються на кіберпростір. Коли зростає геополітична нестабільність — як це було помітно під час нещодавніх суперечок за участю США, Ізраїлю та Ірану — цивільні підприємства часто стикаються з паралельним сплеском зловмисної активності, зокрема з викраденням облікових даних, DDoS-атаками та розвідкою мережі. Ця динаміка не обмежується

жодним окремим регіоном; європейські інституції зіткнулися зі значними наслідками війни в Україні та операціями, пов'язаними з державою, такими як руйнівна атака 2022 року на уряд Албанії та нещодавнє націлювання на медичну технологічну компанію Stryker в Ірландії. Ці операції не є випадковими актами дезорганізації, а стратегічними інструментами, які використовують такі актори, як Росія, Китай та Іран, для демонстрації сили, збору розвідданих або здійснення відплати без вдавання до традиційної військової конфронтації...

Стратегічний характер цих загроз — які часто передбачають, що зловмисники протягом місяців або років зберігають прихований доступ до мереж, перш ніж активувати свої дії — перетворив кібербезпеку на один із головних пріоритетів управління. Особливо вразливими є організації в секторах критичної інфраструктури, таких як енергетика, телекомунікації та фінанси, але партнери ланцюга поставок та науково-дослідні установи також часто стають мішенями як непрямі точки входу. Відображаючи цю зміну, 84% компаній зараз залучають свого головного юрисконсульта до розробки стратегії кібербезпеки, оскільки кіберризики дедалі частіше перетинаються з прийняттям рішень у правовій, регуляторній та операційній сферах...

Щоб орієнтуватися в цій ситуації, керівництво та ради директорів повинні узгодити своє планування у сфері кібербезпеки з більш широкою оцінкою геополітичних ризиків. Нормативно-правові рамки, такі як Директива ЄС NIS2, ще більше закріплюють ці очікування, підвищуючи вимоги до нагляду та стійкості на рівні ради директорів. Посилюючи захист ідентичності, наприклад за допомогою багатофакторної автентифікації, та підтримуючи надійні процедури реагування на інциденти, організації можуть перейти від реактивної позиції до проактивного передбачення. Зрештою, інтеграція геополітичних знань у корпоративне управління дозволяє зацікавленим сторонам краще прогнозувати та мінімізувати загрози, перш ніж вони переростуть у значні операційні кризи». **(Robert Kang. Understanding the Cyber Security Fallout of Geopolitical Tensions // European Scientist (https://www.europeanscientist.com/en/features/understanding-the-cyber-security-fallout-of-geopolitical-tensions/). 11.05.2026).**

«Заступник генерального секретаря НАТО з питань кібербезпеки та цифрової трансформації Жан-Шарль Еллерман-Кінгомбе попередив, що кіберпотенціал відіграє сьогодні ключову роль у сучасній війні, а штучний інтелект різко скорочує час, який залишається у захисників на виявлення та усунення вразливостей. Виступаючи на конференції Defence24 Days у Варшаві, він описав кіберпростір як «критичний фактор» у наземних, морських та повітряних операціях, а не просто як окрему сферу, зазначивши, що кіберможливості можуть нейтралізувати інфраструктуру, на якій базуються кінетичні атаки, ще до їхнього здійснення. Він сказав, що сучасна війна буде фундаментально цифровізованою і що НАТО роками працювало над посиленням кіберзахисту та обміном інформацією, але виклик стає дедалі гострішим...

Еллерманн-Кінгомбе наголосив на уроках, отриманих в Україні, де енергетична інфраструктура зазнала атак як фізичного характеру, так і у вигляді

кібератак, та підкреслив, що енергосистеми, транспортні мережі та підводні кабелі мають вирішальне значення як для повсякденного життя громадян, так і для оборонного потенціалу НАТО. Оскільки значна частина цієї інфраструктури перебуває у приватній власності, він наголосив на важливості співпраці між урядом та промисловістю й повідомив, що НАТО створює інтегрований кіберцентр для об'єднання зусиль держав-членів та представників приватного сектору. Щодо зростаючої ролі штучного інтелекту він попередив, що нові інструменти можуть скоротити проміжок часу між виявленням вразливості та її використанням з тижнів до лічених годин, що збільшить тиск на захисників, які мусять переходити від виявлення до усунення вразливостей за лічені хвилини. Ці зауваження пролунали на тлі триваючої гібридної діяльності Росії, спрямованої проти східного флангу НАТО, зокрема кібератак, саботажу та кампаній дезінформації, які, як попередили Польща та інші країни, мають на меті перевірити рішучість Альянсу». (*Michał Maria Zdanowski. 'Minutes to patch': NATO warns AI is collapsing cyber defense timelines // TVP World (<https://tvpworld.com/93123552/cyber-is-at-the-center-of-modern-war-nato-chief-warns>). 07.05.2026*).

«Агентство внутрішньої безпеки Польщі успішно відбило кібератаки на п'ять водоочисних станцій, не дозволивши хакерам потенційно захопити контроль над промисловими системами та порушити водопостачання. Протягом останніх двох років агентство перехопило численні спроби саботажу, спрямовані проти критичної інфраструктури країни, зокрема проти її електромереж та транспортних мереж. Хоча участь Росії в конкретних атаках на водоочисні станції не була прямо підтверджена, Польща нещодавно зіткнулася зі сплеском кібератак з боку груп, пов'язаних з Москвою. Ці інциденти підкреслюють зростаючу глобальну вразливість підприємств водо- та енергопостачання, що є дзеркальним відображенням попередніх порушень інфраструктури у Сполучених Штатах — таких як атака на водоочисну станцію у Флориді в 2021 році — та збігається з нещодавніми попередженнями щодо хакерів, підтримуваних Іраном, які націлені на промислові системи управління по всьому світу». (*Cyberattacks on Polish critical infrastructure raise security concerns // Shafaq News (<https://shafaq.com/en/World/Cyberattacks-on-Polish-critical-infrastructure-raise-security-concerns>). 10.05.2026*).

«...Зусилля з протидії кібератакам на ОАЕ на тлі ескалації конфлікту за участю Ірану були ефективними і залишаються головним пріоритетом, заявив Омран Шараф, помічник міністра закордонних справ ОАЕ з питань передових наук і технологій, виступаючи на виставці AI+ Expo у Вашингтоні. Шараф заявив, що конфлікт ведеться не лише за допомогою ракет, безпілотників і літаків, але й за допомогою кібероперацій і загроз цифровій безпеці, з якими мають справлятися країни всього регіону. У звіті Microsoft про цифровий захист за 2025 рік було визначено, що Іран часто атакує Ізраїль, США, ОАЕ та Індію, а керівник відділу кібербезпеки ОАЕ Мохамед Аль-Кувейті нещодавно повідомив,

що кількість атак на цифрову інфраструктуру країни зросла втричі – з приблизно 200 000 до 600 000 – з початку війни... У відповідь на це ОАЕ активізували заходи з «кібергігієни», зокрема опублікували рекомендації від Центру управління надзвичайними ситуаціями, кризовими ситуаціями та катастрофами Абу-Дабі, в яких застерігають, що страх, розгубленість і чутки можуть призвести до поспішних рішень, що роблять людей більш вразливими до фішингових посилок та викрадення інформації. Шараф також наголосив на тому, що ОАЕ приділяють особливу увагу захисту своєї інфраструктури центрів обробки даних штучного інтелекту, яка постійно розширюється, шляхом планування заходів з управління кризовими ситуаціями, створення резервних систем та впровадження політик забезпечення безперебійної роботи. У ширшому контексті слід згадати неодноразові спроби, пов'язані з Іраном, скомпрометувати мережі США, а також попередження уряду США про атаки на промислові пристрої, які можуть загрожувати системам водопостачання, водовідведення та енергопостачання, а також нещодавній злом, відповідальність за який взяла на себе пов'язана з Іраном група Handala, що стосувався особистої електронної пошти директора ФБР...» *(Cody Combs. UAE cyber security priorities pay off amid Iran tensions, official says // International Media Investments (https://www.thenationalnews.com/future/technology/2026/05/10/uae-iran-hacking-cybersecurity/). 10.05.2026).*

«Група зловмисників, пов'язана з Китаєм, під назвою SHADOW-EARTH-053, здійснює операції з кібершпигунства проти урядових, оборонних об'єктів та об'єктів критичної інфраструктури в Азії та за її межами, використовуючи незахищені вразливості в Microsoft Exchange Server та Internet Information Services. Кампанія, яка триває щонайменше з грудня 2024 року, була спрямована проти щонайменше восьми країн, а жертви зосереджені в Південній, Східній та Південно-Східній Азії, включаючи урядові міністерства, оборонних підрядників, ІТ-консалтингові фірми та транспортні організації. Польща, член НАТО, також стала мішенню, що вказує на ширший стратегічний охоплення за межами Азіатсько-Тихоокеанського регіону...

Основний вектор атак цієї групи базується на ланцюжку вразливостей ProxyLogon — CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 та CVE-2021-27065 — які, незважаючи на те, що їм уже кілька років, залишаються ефективними проти організацій, що використовують незахищені оновленнями або застарілі версії Exchange. У кількох випадках зломщики встановлювали модулі управління Exchange, виявляли цінні поштові скриньки та експортували їхній вміст за допомогою спеціального інструменту через API веб-служб Exchange — техніку, яку раніше застосовувала китайська група Silk Typhoon. Дослідники Trend Micro також відзначили значне перекриття з пов'язаним набором вторгнень, SHADOW-EARTH-054, який, як видається, передував діяльності SHADOW-EARTH-053 на кілька місяців і має ідентичні хеші інструментів та тактики...

Основним використовуваним імплантом є ShadowPad — модульний бекдор, який історично пов'язують із APT41 і який використовують численні угруповання,

пов'язані з Китаєм. Варіант, розгорнутий у цьому випадку, не має розширених функцій обфускації, що свідчить про те, що група має доступ до старішого компілятора, а не до вихідного коду. Розгортання відбувається за послідовним триетапним механізмом: легітимний підписаний бінарний файл, вразливий до завантаження DLL з боку, шкідливий завантажувач DLL та зашифрований корисний вантаж ShadowPad, що зберігається у реєстрі Windows, а згодом видаляється з нього. Група зловживала підписаними виконуваними файлами від відомих постачальників, зокрема Samsung та Mainline Net Holdings, щоб приховати діяльність із завантаження з боку. Організаціям, що використовують інфраструктуру Exchange або IIS, підключену до Інтернету, настійно рекомендується негайно застосувати доступні виправлення, розгорнути правила запобігання вторгненням та брандмауер веб-додатків, впровадити моніторинг цілісності файлів у веб-каталогах, обмежити привілеї робочих процесів IIS, застосувати білі списки додатків та стежити за такими індикаторами, як запуск командної оболонки процесом веб-сервера та несподівані вихідні з'єднання». *(Tushar Subhra Dutta. China-Aligned SHADOW-EARTH-053 Exploits Exchange Servers to Deploy ShadowPad Malware // Cyber Security News (<https://cybersecuritynews.com/china-aligned-shadow-earth-053-exploits-exchange-servers/>). 05.05.2026).*

«Російська хакерська група «Sandworm», що діє за підтримки держави та відома також як APT44, переорієнтувала свою діяльність зі стандартних вторгнень в IT-мережі на компрометацію операційних технологій (OT) та промислових систем управління, які керують критично важливою фізичною інфраструктурою. На відміну від зловмисників, що використовують програмивимагачі з метою фінансової вигоди, ця військово-розвідувальна група ставить собі за мету дезорганізацію та саботаж. Замість використання новітніх експлойтів, Sandworm постійно досягає успіху, використовуючи добре задокументовані вразливості, які можна виправити — такі як EternalBlue та WannaCry, що існують вже кілька років — та використовуючи плацдарми, вже створені попередніми зловмисниками, щоб проникнути глибше в промислові середовища...

Аналіз, проведений компанією Nozomi Networks, показує, що ці вторгнення характеризуються скоріше «гучністю», ніж прихованістю. У досліджених випадках уражені системи генерували надійні сигнали тривоги в середньому протягом 43 днів до того, як Sandworm розпочав свою основну кампанію, що свідчить про те, що ці атаки в основному можна було запобігти. Група діє за централізовано організованим, «бюрократичним» ритмом — пік активності припадає на середу після обіду за московським часом — і виявляє небезпечну тенденцію до ескалації своєї діяльності, а не до відступу, після виявлення. Такі ескалації зазвичай передбачають більш агресивне націлювання на критично важливі активи, такі як інтерфейси «людина-машина» та польові контролери, що використовуються на електростанціях та виробничих об'єктах. Щоб протидіяти цій загрозі, експерти з безпеки закликають організації перейти від пасивного виявлення до швидкої ізоляції, наголошують на необхідності суворого сегментування мережі між IT- та

ОТ-системами та рекомендують розглядати рутинні сповіщення про безпеку як термінові стратегічні попередження, а не як фоновий шум. У звіті зроблено висновок, що, оскільки Sandworm покладається на використання давніх прогалин у безпеці та попередньо скомпрометованих середовищ, базові заходи з безпеки та проактивне зміцнення інфраструктури залишаються найефективнішими засобами для протидії їхнім операціям». **(Tushar Subhra Dutta. Sandworm Hackers Pivot From Compromised IT Systems Toward Critical OT Assets // Cyber Security News (<https://cybersecuritynews.com/sandworm-hackers-pivot-from-compromised-it-systems/>). 14.05.2026).**

«Нещодавню руйнівну кібератаку, спрямовану проти системи громадського транспорту Лос-Анджелеса, пов'язують з іранським урядом. Управління міського транспорту округу Лос-Анджелес (LA Metro) виявило злом у середині березня; це спричинило внутрішні операційні збої, але не вплинуло на роботу залізничного та автобусного сполучення. На початку квітня представники LA Metro повідомили, що перед відновленням роботи сотні серверів довелося перевірити на наявність ознак злому. Через кілька днів відповідальність за атаку взяла на себе група Ababil of Minab, яка позиціонує себе як проіранська хактивістська організація. Хакері нібито знищили сотні терабайтів даних та викрали понад 1 ТБ файлів, опублікувавши скріншоти та відео, щоб продемонструвати доступ до внутрішніх систем LA Metro, зокрема до основної платформи віртуалізації, веб-сервера Microsoft IIS, на якому розміщені як внутрішні, так і публічні ресурси, і навіть до оперативної технологічної системи, що використовується для моніторингу поїздів...

Згідно з даними компанії Dataminr, що спеціалізується на аналізі кіберзагроз, зловмисна група Ababil of Minab вважається новою організацією з обмеженою публічною присутністю та незначною кількістю підтверджених дій, що робить оцінку її можливостей та намірів передчасною. Проте ізраїльська компанія Gambit, що займається кіберзахистом, проаналізувала цю групу та виявила зв'язки з інфраструктурою, яку раніше використовували хакери, пов'язані з іранським урядом. Gambit заявила, що Ababil of Minab навряд чи є незалежною організацією, оскільки криміналістичні докази пов'язують її з інфраструктурою та діяльністю, пов'язаною з Black Shadow — групою, пов'язаною з Іраном, яку Національне кіберуправління Ізраїлю відносить до Міністерства розвідки та безпеки Ірану. Розслідування Gambit виявило, що Ababil of Minab здійснила атаки на цілі в США, Ізраїлі, Саудівській Аравії та Туреччині, що включали викрадення даних та, в деяких випадках, деструктивні дії. Серед жертв були ізраїльські медіаорганізації, вищий навчальний заклад, турецький страховий брокер та різні веб-сайти з таких секторів, як ресторанний бізнес, культура, цифрові послуги та новини». **(Eduard Kovacs. LA Metro Cyberattack Linked to Iranian State-Sponsored Hackers // SecurityWeek (<https://www.securityweek.com/la-metro-cyberattack-linked-to-iranian-state-sponsored-hackers/>). 27.05.2026).**

«У міру того як космічні системи стають дедалі більш комерційними та програмно-орієнтованими, кібербезпека перетворилася з вузькоспеціалізованої технічної проблеми на стратегічну необхідність, оскільки супутники тепер у більшій мірі залежать від комерційно розробленого обладнання, спільних програмних платформ, дистанційної переконфігурації та оновлень на орбіті — переваг, які водночас розширюють площину для кібератак. На тлі глобальних напружень, швидко розвиваючихся загроз та нових технологій, таких як квантові обчислення, що можуть підірвати сучасну криптографію, Європейське космічне агентство (ESA) поставило кібербезпеку в центр розвитку технологій, враховуючи ризики у космічному, наземному та комунікаційному сегментах протягом усього життєвого циклу місії... В рамках Програми загальної технологічної підтримки (GSTP) ESA прискорює реалізацію низки заходів у сфері кібербезпеки, зокрема дорожню карту на 2026–2028 роки «Продукти (кібер)безпеки для захисту космічних систем» та семінар 7 травня 2026 року, спрямовані на визначення пріоритетності питань безпеки, виявлення прогалин на ринку та формування галузевих консорціумів для перетворення «будівельних блоків кібербезпеки» на готові продукти, що підвищують безпеку місій, зменшують вплив на витрати та графіки та сприяють комерціалізації... Основними напрямками роботи семінару є забезпечення безпеки каналів зв'язку, виявлення вторгнень, а також методи захисту та відновлення, що відображає такі основні загрози, як потреби у постквантовій безпеці, зростаюча необхідність у безпечному дистанційному оновленні програмного забезпечення, а також завдання запобігання створенню системних вразливостей програмними компонентами — які часто походять від різних постачальників і працюють на готових системах — особливо у великих супутникових групах, де недоліки можуть поширюватися на багато космічних апаратів. GSTP також пропонує готові до впровадження рішення на найближчу перспективу, такі як співпраця з німецькою компанією OHB у сфері безпечних перепрограмованих супутникових обчислювальних систем із використанням постквантової криптографії та оновлень на орбіті; проект TANDI від Airbus, спрямований на безпечну ізоляцію та верифікацію численних додатків на спільних супутникових обчислювальних системах; а також ARCA SATLINK Encryptor від CYSEC — бібліотека шифрування для захисту каналів передачі даних між супутником і наземними станціями та управління криптографічними ключами протягом усього терміну експлуатації супутника. У сукупності ці зусилля ілюструють, як ESA втілює стратегію кібербезпеки в практичні технології для забезпечення майбутнього європейських космічних місій». (*Strengthening Space Cybersecurity through ESA's GSTP // European Space Agency (ESA) (https://www.esa.int/Enabling_Support/Space_Engineering_Technology/Shaping_the_Future/Strengthening_Space_Cybersecurity_through_ESA_s_GSTP). 06.05.2026*).

«Кіберфізична стійкість змушує операторів критичної інфраструктури відійти від підходу до безпеки, орієнтованого на захист периметра, і зосередитися на захисті цілісності промислових процесів, оскільки історичне розмежування між ІТ та ОТ значною мірою зникло у зв'язку з розширенням можливостей підключення та віддаленого доступу. У міру зникнення «повітряного проміжку» моделей, що базуються виключно на запобіжних заходах, вже недостатньо: зловмисники можуть проникнути в систему, переміщатися по ній, маніпулювати системами управління та спричиняти фізичні наслідки, перш ніж їх виявлять, і навіть через довгий час після інциденту зі Stuxnet багато промислових середовищ залишаються вразливими до атак... Це зумовило перехід до виявлення вторгнень у внутрішні операційні процеси за допомогою таких методів, як аналіз ризиків кіберпроцесів та моніторинг фізичних або технологічних аномалій, замість того, щоб покладатися переважно на мережеві індикатори. Дані галузі ілюструють цей тиск: близько 21% компаній щорічно стикаються з кібератаками на операційні технології (ОТ), 40% цих інцидентів призводять до перебоїв у роботі бізнесу, майже половина виявлених загроз виявляється протягом 24 годин, але видимість на рівні процесів залишається слабкою, віддалений доступ продовжує збільшувати вразливість, а 78% промислових пристроїв управління містять вразливості, які неможливо усунути... Архітектура також переглядається, оскільки конвергенція ІТ та ОТ виявляє застарілі проекти ОТ, розроблені з метою підвищення ефективності, а не безпеки, тоді як кількість атак на інфраструктуру промислового управління різко зросла (за даними KPMG, зростання становить 87% у порівнянні з минулим роком). Відновлення залишається серйозною проблемою: майже 20% організацій потребують більше місяця для відновлення роботи після інциденту, що підкреслює, що стійкість дедалі більше визначається тим, як швидко оператори можуть виявляти, локалізувати та відновлювати роботу без переривання основних процесів.

Експерти наголошують, що кіберфізична стійкість полягає у забезпеченні безпечного та надійного функціонування послуг навіть у разі порушення цілісності систем, що вимагає постійного моніторингу, сегментації, безпечного віддаленого доступу, аналітики в режимі реального часу та міждисциплінарної координації між підрозділами безпеки, інженерії та експлуатації. Вони попереджають, що багато організацій переоцінюють свою готовність, оскільки моніторять лише трафік Ethernet/IP, ігноруючи послідовні та аналогові сигнали ICS, які керують фізичними процесами, створюючи «сліпі зони», що дозволяють порушенням розвиватися, доки їхній вплив не стане очевидним — уроки, винесені з таких інцидентів, як атака на енергомережу України у 2015 році та інцидент на водоочисній станції в Олдсмарі. З огляду на постійну вразливість, пристрої, для яких неможливо встановити виправлення, ризики ланцюга постачання та прискорене виявлення вразливостей за допомогою штучного інтелекту, керівники виступають за формування менталітету, що базується на припущенні про злом: вбудовані резервні системи та засоби захисту від збою, детерміновані базові показники «нормальної» роботи, швидке виявлення аномалій, пов'язане з поведінкою процесів, відпрацьовані процедури управління інцидентами та надзвичайними ситуаціями, а також надійне планування відновлення після збою та забезпечення безперервності

роботи, перевірене під час навчань. Основна зміна полягає в тому, що захисту «систем» вже недостатньо; оператори повинні захищати фізичні процеси, які контролюють ці системи, та бути здатними швидко відновлювати надійну роботу у разі порушення безпеки...» (*Anna Ribeiro. Cyber-physical resilience reshaping industrial cybersecurity beyond perimeter defense to protect core processes // Industrial Cyber* (<https://industrialcyber.co/features/cyber-physical-resilience-reshaping-industrial-cybersecurity-beyond-perimeter-defense-to-protect-core-processes/>). 03.05.2026).

«Кібербезпека стала спільною відповідальністю всіх підрозділів організації, а для електроенергетичних компаній це питання є особливо важливим, оскільки саме мережева інфраструктура забезпечує стабільність та надійність енергосистеми. Керівники мереж енергетичних компаній поєднують операційні та безпекові функції: тоді як підрозділи з безпеки розробляють стратегію та політику, мережеві підрозділи відповідають за системи, які повинні протистояти реальним загрозам і відповідати вимогам NERC CIP, тому проактивний підхід є необхідною умовою для запобігання перебоям у постачанні електроенергії, дотримання нормативних вимог та забезпечення стійкості до атак досвідчених злоумисників... Основні рекомендації починаються з забезпечення повної видимості мережі — розуміння всіх комутаторів, маршрутизаторів, брандмауерів, бездротових і послідовних мостів, шлюзів та віртуальних інтерфейсів, включаючи непередбачені з'єднання, — що підкріплюється оглядами обладнання, точними схемами (що також вимагається стандартом NERC CIP-002-3), періодичними перевітками та, за можливості, комерційними засобами сканування. Ведення повного та актуального інвентарного списку активів є необхідністю як з точки зору дотримання вимог, так і з точки зору безпеки; він має містити ідентифікатори пристроїв, версії прошивки та ОС, модулі, інтерфейси та IP-адреси, місцезнаходження, ступінь критичності, стан підтримки та терміни закінчення терміну експлуатації... Встановлення виправлень вважається ключовим засобом захисту, незважаючи на операційні обмеження в корпоративних та промислових середовищах управління. При цьому рішення базуються на результатах регулярного або пасивного сканування, рекомендаціях постачальників та визначенні пріоритетів на основі ризиків (наприклад, з використанням оцінок CVSS), що забезпечує відповідність документації вимогам CIP. Стандартизовані конфігурації та шаблони для мережевих пристроїв знижують ризик неправильної конфігурації та підвищують узгодженість у веденні журналів, синхронізації часу, контролі доступу, SNMP, шифруванні та правилах іменування. Контроль доступу повинен виходити за межі паролів і включати доступ на основі ролей, MFA, де це можливо, безпечні канали віддаленого доступу та проміжні хости, принцип мінімальних привілеїв, гігієну облікових записів та моніторинг привілейованої діяльності, що підлягає аудиту. Ефективна кібербезпека також вимагає тісної інтеграції між управлінням мережею та кіберпрограмами — забезпечення роботи систем реєстрації та датчиків, участь у навчаннях, а також координація на ранніх етапах проектування, — де сегментація на чітко визначені зони та канали передачі

даних вважається одним із найдієвіших засобів контролю для обмеження горизонтального переміщення та локалізації інцидентів. Загалом, суть полягає в тому, що менеджери мереж не просто обслуговують інфраструктуру комунальних підприємств, а безпосередньо забезпечують надійність енергосистеми, а проактивна співпраця та практики «безпеки за замовчуванням» дозволяють втілити стратегію кібербезпеки в повсякденній діяльності». (*Alan Hirth. Cybersecurity is Now a Network Manager's Job—Here's How to Own It // Access Intelligence, LLC (<https://www.powermag.com/blog/cybersecurity-is-now-a-network-managers-job-heres-how-to-own-it/>). 06.05.2026*).

«Агентство з кібербезпеки та безпеки інфраструктури (CISA) запустило нову ініціативу під назвою CI Fortify, покликану забезпечити безперебійну роботу критичної інфраструктури під час масштабних кібератак навіть у разі відключення телекомунікаційних та інтернет-послуг. Ця ініціатива знаменує стратегічний перехід від односторонньої зосередженості на вигнанні вбудованих хакерів до більш багаторівневого підходу, орієнтованого на «ізоляцію та відновлення». У рамках цієї структури організаціям рекомендується відокремити свої операційні технології (OT) від більш широких мереж та розвинути здатність проактивно відключатися від залежності від сторонніх ресурсів під час кризи...

Переорієнтація на забезпечення стійкості та «офлайн»-операції значною мірою зумовлена постійною загрозою з боку державних суб'єктів, зокрема пов'язаною з Китаєм кампанією під назвою «Volt Typhoon». Оскільки ці суб'єкти проникли в інфраструктуру США щонайменше з 2019 року — часто викрадаючи облікові дані для полегшення повторного проникнення — експерти стверджують, що повне викорінення загрози вже не є реалістичною короткостроковою метою. Натомість CI Fortify виходить з того, що системи, можливо, вже скомпрометовані, і зосереджується на обмеженні «радіусу ураження», забезпечуючи можливість продовження роботи критично важливих служб в ізольованому стані. Виконуючий обов'язки директора CISA Нік Андерсен зазначив, що ця ініціатива також стосується тактик, які спостерігалися під час нещодавніх російських кібератак на мережі операційних технологій у Польщі...

Окрім геополітичної напруженості, розвиток штучного інтелекту додав цій програмі додаткової актуальності. Представники CISA висловили занепокоєння тим, що ШІ суттєво прискорює та збільшує масштаби кібератак, посиляючись на нещодавні повідомлення про хакерів, які використовують моделі ШІ для зломів муніципальних систем комунального господарства. Для реалізації цієї ініціативи CISA планує провести цільові галузеві оцінки, щоб допомогти організаціям удосконалити свої плани дій у надзвичайних ситуаціях та забезпечити належну сегментацію їхніх систем. Зрештою, мета CI Fortify полягає в тому, щоб навіть у разі руйнівних кібератак найважливіші служби країни могли витримати удар і швидко відновитися, перебуваючи в ізоляції». (*Jonathan Greig. New CISA initiative aims for critical infrastructure to operate offline during cyberattacks // Recorded Future News (<https://therecord.media/cisa-initiative-aims-for-critical-infrastructure-to-operate-during-cyberattacks>). 06.05.2026*).

«У 2025 році в Польщі відбувся 144-відсотковий сплеск кібератак на об'єкти критичної інфраструктури, який пов'язують із ескалацією кампанії «війни в сірій зоні», що веде російська розвідувальна служба ГРУ. Міністр цифрових справ Кшиштоф Гавковський охарактеризував ці операції як «першу хвилю» фізичної війни, наголосивши на майже катастрофічній спробі вивести з ладу національну електромережу безпосередньо перед Новим роком 2026 року. Хоча цю конкретну атаку було відбито, Гавковський зазначив, що її час був обраний з метою підірвати довіру громадськості до уряду та знищити почуття безпеки населення...»

Хоча Польща входить до п'ятірки країн світу з найвищим рівнем кіберзахисту — їй вдається блокувати 99,9% усіх вторгнень — через величезний обсяг активності ці 0,1%, що залишаються, все одно призводять до численних успіхів супротивника. У відповідь на це польське керівництво переходить до більш проактивної та наступальної позиції, наголошуючи на необхідності мати відповідні навички та персонал для «удару у відповідь» по супротивниках з метою забезпечення стримування...

Для підтримки цього стратегічного курсу Польща працює над створенням найбільших збройних сил у Європі, ставлячи за мету набрати 300 000 військовослужбовців та сформувати цивільний резерв, до якого увійдуть тисячі ІТ-фахівців. Однак довгострокові цілі є ще амбітнішими: уряд прагне збільшити кількість фахівців у сфері кібербезпеки до 1,5 мільйона до 2035 року. Незважаючи на цю концепцію, залишаються значні перешкоди, зокрема складність залучення висококласних фахівців до державного сектору, коли зарплати у приватному секторі часто вчетверо перевищують державні...» *(Stew Magnuson. JUST IN: Poland Engaged in Toe-to-Toe Cyber Warfare with Russians // National Defense Industrial Association* <https://www.nationaldefensemagazine.org/articles/2026/5/7/poland-engaged-in-toetotoe-cyber-warfare-with-russians>). 07.05.2026).

«З огляду на зростаючу складність та взаємопов'язаність сучасних авіаційних систем, прогнозується, що до 2030 року обсяг світового ринку кібербезпеки в авіації досягне 7,95 млрд доларів, зростаючи із середньорічним темпом зростання (CAGR) на рівні 8,6%. Таке стрімке зростання зумовлене насамперед переходом галузі на хмарні платформи, поширенням підключених до мережі літаків та нагальною потребою захищати дані пасажирів та операційну інфраструктуру за допомогою передових засобів виявлення загроз та аналітики в режимі реального часу...»

Щоб скористатися можливостями цього ринку, що активно розширюється, провідні корпорації в галузі авіакосмічної промисловості, оборони та технологій — зокрема Airbus, Lockheed Martin, IBM та Accenture — активно розширюють свої можливості за допомогою стратегічних поглинань та партнерських відносин. Наприклад, на початку 2023 року Accenture придбала бразильську компанію з кібербезпеки Morphus, щоб посилити свої пропозиції з кіберзахисту та управління

ризиками, розроблені спеціально для клієнтів з авіаційної галузі. Аналогічно, партнерські альянси виявляються вирішальними для інновацій, про що свідчить нещодавнє партнерство між ізраїльським фахівцем з кібербезпеки літаків Cyvation та Deloitte Canada. Ця співпраця поєднує глибокий консультативний досвід із інструментами проактивного моніторингу загроз, щоб допомогти авіакомпаніям орієнтуватися у мінливих кіберзагрозах та дотримуватися нових галузевих нормативних вимог...

З метою задоволення різноманітних і надзвичайно технічних потреб галузі ринок кібербезпеки в авіаційній сфері має складну сегментацію. За складовими він поділяється на конкретні рішення (такі як безпека мереж, кінцевих точок та даних) та послуги (включаючи консалтинг, реагування на інциденти та керувану безпеку). Крім того, ринок класифікує свої пропозиції за типом безпеки — охоплюючи безпеку мереж, бездротових мереж, хмарних середовищ та додатків — моделями розгортання та критичними сферами застосування, що варіюються від управління авіакомпаніями та вантажними перевезеннями до експлуатації аеропортів та управління повітряним рухом». (*Leading Firms Advancing Innovation and Growth in the Aviation Cyber Security Market* // *openPR* (<https://www.openpr.com/news/4503749/leading-firms-advancing-innovation-and-growth-in-the-aviation>). 06.05.2026).

«У новому звіті Королівського інституту міжнародних відносин (британський аналітичний центр, відомий у народі як «Chatham House») міститься застереження, що світова галузь цивільної ядерної енергетики «намагається наздогнати» інших у сфері кібербезпеки, відстаючи від таких критично важливих секторів, як фінанси та управління водними ресурсами. Хоча традиційна орієнтація галузі на надійну фізичну охорону та спеціальне програмне забезпечення з «повітряним розривом» колись давала відчуття безпеки, стрімка цифровізація ядерних об'єктів та впровадження готового комерційного програмного забезпечення створили цілу низку нових вразливостей. Серед них — застарілі системи, відсутність патчів безпеки та небезпечні методи роботи, такі як використання портативних пристроїв для зберігання даних. У звіті наводиться приклад кримінального засудження у 2024 році британського об'єкта «Sellafield» за порушення кібербезпеки як яскравий приклад того, як ризиковані практики можуть зберігатися за чинних режимів ліцензування...

Потенційні наслідки кібератаки на ядерний об'єкт виходять далеко за межі розплавлення реактора — що залишається малоімовірним завдяки багаторівневій системі безпеки — і включають викрадення інформації, пошкодження обладнання та значні перебої в енергопостачанні. Оскільки атомні електростанції забезпечують необхідну «базову» потужність і підтримують стабільність енергосистеми завдяки інерції системи, зупинка, спричинена кібератакою, може призвести до масштабних відключень електроенергії та порушити роботу життєво важливих служб, таких як охорона здоров'я. Ситуація з ризиками ще більше ускладнюється появою малих модульних реакторів (SMR); хоча вони розроблені з урахуванням сучасних вимог безпеки, їхня підвищена підключеність до Інтернету та залежність від складних

ланцюгів постачання будівельних матеріалів роблять їх привабливими цілями для кіберзлочинців, які шукають нагоди...

Щоб пом'якшити ці загрози, що постійно зростають, Chatham House рекомендує багаторівневий підхід, орієнтований на посилення міжнародної співпраці та підвищення прозорості. У звіті міститься заклик відмовитися від ізоляціоністської культури галузі та «зацикленості на сприйнятті», натомість сприяючи регулярному інституційному діалогу та партнерству між державним і приватним секторами з метою обміну передовим досвідом та даними про інциденти. На національному рівні уряди повинні посилити свою здатність забезпечувати дотримання стандартів кібербезпеки та ретельно планувати заходи реагування на інциденти. Зрештою, у міру розширення та диверсифікації ядерного сектору операторам та регуляторним органам необхідно терміново активізувати спільні зусилля, щоб кібербезпека стала фундаментальним елементом ядерної безпеки та національної стійкості». (*Nuclear Sector Must Step Up Cybersecurity // GlobalData Plc* (<https://www.nsenenergybusiness.com/analysis/playing-catch-upon-cyber-safety/>). 04.05.2026).

«Компанія Dragos попередила, що доступні на ринку інструменти генеративної штучної інтелекту прискорюють спроби проникнення в середовища операційних технологій на підприємствах водопостачання та інших операторів критичної інфраструктури. В аналізі, проведеному спільно з Gambit Security, Dragos описав кампанію вторгнень у 2025–2026 роках проти декількох мексиканських урядових організацій, зокрема муніципального підприємства водопостачання та водовідведення, що обслуговує регіон Монтеррея, де слідчі виявили докази того, що невідомий зловмисник використовував моделі Claude від Anthropic та GPT від OpenAI для розвідки, розробки інструментів, атак на облікові дані та горизонтального переміщення після компрометації корпоративних ІТ-систем...

Зловмисники використовували скрипти та засоби автоматизації, створені за допомогою штучного інтелекту, щоб виявити платформу SCADA та промисловий шлюз, підключені до операційного середовища комунального підприємства. За повідомленнями, система Claude визначила цю систему, пов'язану з технологічними мережами (OT), як ціль високої цінності та почала шукати шляхи доступу між ІТ-мережами та мережами водопостачання. Dragos зазначив, що хоча моделі не генерували нових технік атак на промислові системи управління, вони значно прискорили виконання відомих методів атак і допомогли зловмисникам швидко створити та вдосконалити інструментарій, включаючи фреймворк Python на 17 000 рядків для збору облікових даних, опитування Active Directory та латерального переміщення після компрометації. Спроба проникнення в ОТ-середовище комунального підприємства в кінцевому підсумку зазнала невдачі, і Dragos не виявив жодних доказів компрометації операційної системи, але стверджує, що цей інцидент демонструє, як ШІ може скоротити час від вторгнення в ІТ до атак на промислові системи... Dragos закликав комунальні підприємства посилити такі основоположні заходи, як сегментація мереж, надійна

аутентифікація, забезпечення прозорості операційних технологій (OT) та моніторинг трафіку «схід-захід», а також звернув увагу на такі рекомендації, як «П'ять критично важливих заходів контролю для кібербезпеки ICS» від SANS, як підготовку до все більш автоматизованих загроз для водопровідної інфраструктури». *(Cyberattackers used AI to map pathways into water utility OT systems, report says // WaterWorld (<https://www.waterworld.com/water-utility-management/news/55377018/cyberattackers-used-ai-to-map-pathways-into-water-utility-ot-systems-report-says>). 12.05.2026).*

«Нещодавній несанкціонований злом системи радіозв'язку Тайванської корпорації швидкісних залізниць (THSRC), що змусив чотири потяги здійснити аварійну зупинку, викрив критичні системні вразливості в національній інфраструктурі Тайваню. Хоча спочатку це виглядало як поодинокий промах студента, який перехопив, скопіював і підробив легітимні сигнали, щоб викликати аварійні сигнали тривоги, цей інцидент висвітлює глибоку інституційну самовпевненість та тривале погіршення стану систем кіберзахисту на рівні комунікацій... Експерти застерігають, що зосередження уваги виключно на веб-атаках або індивідуальній відповідальності не враховує серйозних операційних ризиків, пов'язаних зі старінням обладнання, застарілими механізмами аутентифікації та відсутністю засобів блокування аномалій у режимі реального часу. Якщо така важлива система, як THSRC, може бути так легко зламана, то інші життєво важливі сектори — такі як енергетичні мережі, диспетчерські служби та громадський транспорт — також можуть опинитися під загрозою. Відповідно, цей інцидент розглядається не лише як проблема кібербезпеки, а й як серйозне попередження щодо національної безпеки. Щоб усунути ці структурні недоліки, владі рекомендується впровадити комплексний міжвідомчий механізм аудиту, що включатиме регулярні стрес-тести та імітаційні атаки на всю критичну інфраструктуру... Крім того, системи зв'язку необхідно підняти до рівня управління національною безпекою із застосуванням єдиних стандартів шифрування, а політика державних закупівель має передбачати суворе дотримання вимог кібербезпеки, а не ставити на перше місце економію коштів. Зрештою, для забезпечення громадської безпеки необхідні проактивні системні реформи, оскільки покладання на реактивні, фрагментарні рішення та індивідуальну самодисципліну залишає країну в небезпечному становищі перед майбутніми, потенційно катастрофічними порушеннями безпеки». *(Chen Ching-yun. Taiwan's cyberdefenses flawed // The Taipei Times (<https://www.taipaitimes.com/News/editorials/archives/2026/05/16/2003857413>). 16.05.2026).*

«Хімічні підприємства вже давно покладаються на усталені методи забезпечення безпеки технологічних процесів — визначення сценаріїв відмов, тестування рівнів захисту та перевірку безпеки процесів — проте зростаюча цифровізація породжує нову категорію ризиків, яку традиційні моделі хімічної

небезпеки часто не враховують. Мережеві системи управління та системи технічної безпеки можуть бути змінені внаслідок кібервтручання, віддалених змін конфігурації або порушення зв'язку без очевидних фізичних ознак, а це означає, що хіміки та інженери повинні враховувати не тільки внутрішню безпеку хімічних процесів, але й цілісність та доступність цифрових систем, які їх контролюють та керують ними. Це зміщує акцент в оцінці ризиків з виключно відхилень у процесах на оцінку надійності рівнів захисту, коли вони залежать від спільних мереж, віддаленого доступу або логіки, керованої програмним забезпеченням...

Необхідність інтеграції кібербезпеки у функціональну безпеку відображена у стандарті IEC 61511, видання 2, який запровадив вимогу щодо оцінки ризиків безпеки для систем інструментального забезпечення безпеки, а також у більш широкому стандарті IEC 62443 щодо захисту систем промислової автоматизації та управління. Проте багато підприємств ставляться до цих вимог як до формальних пунктів для відмітки або взагалі їх ігнорують. Традиційні аналізи HAZOP та аналізи рівнів захисту зазвичай стосуються механічних несправностей, таких як втрата сигналу датчика, що перешкоджає вимкненню, але часто не враховують цифрові режими відмови, такі як затримка або блокування сигналів вимкнення, несанкціоновані зміни параметрів або втрата синхронізації між резервними системами. Практична оцінка безпеки SIS починається з визначення меж критичних функцій безпеки та їх цифрових з'єднань, відображення залежностей, оцінки сценаріїв, в яких цілісність або доступність можуть бути порушені, а потім вибору та інтеграції засобів контролю кібербезпеки в процеси управління змінами...

Польові спостереження виявляють повторювані слабкі місця на промислових об'єктах, зокрема недостатнє розділення мереж безпеки та управління технологічними процесами, спільне використання облікових даних, застарілі системи, які обслуговуються, але не захищені належним чином, постійно активний віддалений доступ, а також процедури резервного копіювання та відновлення, які рідко перевіряються. Оскільки цифрові архітектури часто розвиваються поступово, приховані залежності можуть пов'язувати декілька рівнів захисту через спільні канали, невидимі на традиційних технологічних схемах, що створює ризик того, що один злом може одночасно вплинути на кілька засобів захисту. Щоб вирішити цю проблему, підприємствам слід розширити аналіз ризиків, включивши до нього сценарії перебоїв у роботі мережі та втрати цілісності, розробити процедури контрольованого відключення на випадок, коли середовищу управління не можна довіряти, та проводити навчання з реагування на інциденти. Практичні заходи включають надійну сегментацію мережі, більш жорстке управління віддаленим доступом, офіційний контроль над змінами цифрової конфігурації та тестування, яке перевіряє не тільки апаратне забезпечення, але й цілісність даних, логіки та комунікацій у реальних умовах експлуатації, при цьому хіміки тісно співпрацюють з командами з кібербезпеки та систем управління, щоб гарантувати безпеку перевірених процесів на підключених заводах». (*Denrich Sananda. Opinion: Why chemistry's cybersecurity risk models need updating // American Chemical Society (<https://cen.acs.org/articles/104/web/2026/05/cybersecurity-risk-hazard-digital-intrusion-safety-protection.html>). 15.05.2026*).

«Останні звіти з кібербезпеки виявили тривожну тенденцію: хакери зламують пристрої для моніторингу та зчитування даних про паливні резервуари на автозаправних станціях по всій території Сполучених Штатів. Ці підземні сенсорні системи, які відіграють ключову роль у відстеженні запасів палива та виявленні можливих витоків, дедалі частіше стають мішенню зловмисників через використання застарілих мереж та слабкі налаштування безпеки. Використовуючи ці вразливості, зловмисники можуть отримати несанкціонований доступ до конфіденційних операційних даних або маніпулювати показниками запасів палива, що може призвести до хаосу в ланцюгу постачання, збоїв у роботі систем та значних фінансових втрат... У відповідь на ці ризики та загальне зростання кількості кібератак на об'єкти критичної інфраструктури регуляторні органи та компанії з кібербезпеки закликають до термінового оновлення технологічної інфраструктури галузі. Відповідно, багато операторів електростанцій почали посилювати свої системи кіберзахисту, впроваджуючи сучасні методи шифрування та посилюючи контроль за пристроями, підключеними до їхніх внутрішніх мереж, з метою захисту життєво важливих енергетичних послуг та запобігання майбутнім порушенням безпеки...» (*Medhat Elsheikh. A cyberattack hits fuel tank readers at US gas stations // Voice Of Emirates (<https://www.voiceofemirates.com/en/news/2026/05/16/a-cyberattack-hits-fuel-tank-readers-at-us-gas-stations/>). 17.05.2026*).

«Цифрові загрози поширюються зі швидкістю поїзда, і залізниці реагують на них за допомогою спеціалізованих підходів до кібербезпеки, розроблених для систем, які повинні залишатися працездатними в умовах постійного руху. У міру того як поїзди стають дедалі більш підключеними до мережі — об'єднуючи бортові комп'ютери з приколіїним обладнанням, диспетчерськими центрами та пасажирським Wi-Fi — галузь стикається з новими ризиками, які вже не можна розглядати як звичайні ІТ-проблеми. За словами Едді Тезе, віце-президента з цифрових технологій та кібербезпеки компанії Alstom, те, що пасажирів сприймають як звичайну подорож, є щоденною «фінішною прямою» для тих, хто відповідає за безпечну та безперебійну роботу залізниці. Кіберінцидент на залізниці може порушити роботу цілих економік, але, на відміну від офісних систем, поїзд не можна просто перезавантажити посеред подорожі...

Кібербезпека залізничного транспорту є окремою дисципліною, оскільки вона покликана захищати високошвидкісний «офісний будинок на колесах», який перетинає кордони, проїжджає тунелі, перемикається між мережами та створює сильні електромагнітні перешкоди, при цьому використовуючи застарілі протоколи сигналізації, що з'явилися ще до появи Інтернету. Рішення починається з апаратного розділення за допомогою «двосторонніх дверей» для даних: інформація може витікати для моніторингу та технічного обслуговування, але ніщо не може проникати назад із менш захищених мереж, таких як пасажирський Wi-Fi. Це поєднується з кібербезпекою, притаманною залізничному транспорту, яка враховує фізичні обмеження, нульову толерантність до затримок у системах безпеки та

неможливість переривання обслуговування. Замість реагування на інциденти, акцент змістився з простого дотримання нормативних вимог на забезпечення довгострокової безперебійної роботи — надійного та безпечного перевезення пасажирів протягом десятиліть...

Зрештою, ефективна кібербезпека залізничного транспорту має залишатися непомітною. Пасажири без зайвих роздумів сідають у потяги та виходять з них, покладаючись на те, що надійний і постійно вдосконалюваний захист — розроблений з самого початку та підтримуваний протягом десятиліть — забезпечує безпечну та надійну роботу системи». (*Why rail cybersecurity requires a different security model // ALSTOM SA (<https://www.alstom.com/stories/why-rail-cybersecurity-requires-different-security-model>). 26.05.2026*).

Кіберзахист закладів охорони здоров'я

«Кібератаки на дві лікарні в північній частині Делі в червні 2025 року призвели до виведення з ладу цифрових баз даних пацієнтів, а атака програм-вимагачів у вересні 2025 року на британську компанію Kido International, що надає послуги в галузі дошкільної освіти, призвела до витоку конфіденційних даних про близько 8 000 дітей та співробітників, що ілюструє реальні ризики, з якими стикаються вразливі сектори. Згідно з доповіддю «Глобальний прогноз у сфері кібербезпеки на 2026 рік» Світового економічного форуму, кібернерівність продовжує зростати, при цьому брак кваліфікованих кадрів є другою за значимістю проблемою, а 51% неурядових організацій (NGO) повідомляють про недостатність ресурсів... Сфера охорони здоров'я, освіта та NGO є головними цілями, оскільки зловмисники використовують терміновість, моральний тиск та неможливість тривалого простою, щоб застосовувати програми-вимагачі, фішинг та вимагання даних проти секторів, які не мають фінансових, технічних та інституційних можливостей для забезпечення базової кібербезпеки. У сфері охорони здоров'я ФБР зафіксувало у 2024 році більше інцидентів, ніж у будь-якому іншому секторі критичної інфраструктури; 92% організацій охорони здоров'я зазнали принаймні однієї кібератаки у 2025 році, а середня вартість порушення безпеки становила 7,42 млн доларів; сектор покладається на взаємопов'язані системи життєзабезпечення, медичні картки пацієнтів та медичні пристрої, багато з яких підключені до Інтернету без належного захисту — нещодавній аналіз виявив понад 2,25 мільйона пристроїв Інтернет медичних речей (IoMT), причому 96% установ використовують пристрої з відомими вразливостями, які експлуатуються зловмисниками... Щоб усунути ці прогалини, компанія Mandiant (що належить Google) пропонує безкоштовні абонентські послуги з реагування на інциденти відповідним сільським лікарням у США в рамках ініціативи Google Initiatives for Rural Health; програма Cyber4Healthcare від CyberPeace Institute надає безоплатні послуги з реагування на інциденти та аналізу загроз по всьому світу; а клініки, пов'язані з Berkeley Research Group, підвищують рівень безпеки за допомогою досліджень, клінічних партнерств та передових практик, причому виявлення аномалій на основі штучного інтелекту

допомагає на ранній стадії виявляти підозрілі спроби доступу та небезпечні конфігурації. У сфері освіти школи та університети керують відкритими цифровими середовищами, застарілими ІТ-системами, великими обсягами конфіденційних даних, різноманітними користувачами з різним рівнем обізнаності та залежністю від хмарних платформ і концепції «Принеси свій пристрій» (BYOD), що робить їх вразливими до програм-вимагачів та фішингу, включаючи атаки на основі QR-кодів в електронних листах та формах...

Після інциденту з витоком даних у 2021 році Університет штату Орегон створив Навчальний центр з питань безпеки, який використовує інструменти штучного інтелекту для автоматизації моніторингу та залучення студентів-аналітиків, тоді як компанія Microsoft започаткувала навчання з урахуванням рольових функцій для керівників, викладачів, студентів, батьків та ІТ-фахівців відповідно до рекомендацій CISA; а робочий посібник Національного альянсу з кібербезпеки «Тоді й зараз: як захистити себе в Інтернеті» спрямований на людей похилого віку з метою підвищення їхньої впевненості у використанні цифрових технологій та стійкості до кіберзагроз... NGO, які часто працюють у середовищах з високим рівнем ризику та політичною чутливістю, маючи обмежені бюджети та розгалужені мережі, стикаються з атаками, що наражають бенефіціарів на ризики для безпеки та конфіденційності та порушують надання гуманітарних послуг; NetHope надає спільні послуги з кібербезпеки, аналітику щодо загроз та підтримку у розбудові потенціалу; Центр гуманітарної кібербезпеки Інституту CyberPeace пропонує безоплатну допомогу у реагуванні на інциденти, проведення експертизи та відновлення; Лабораторія Lenovo «AI for Social Impact Lab» (разом з Tech To The Rescue) надає обраним NGO інструменти штучного інтелекту та навчання; а Центр обміну інформацією та аналізу NGO сприяє обміну інформацією про загрози між колегами та наданню індивідуально підібраних ресурсів. Ефективна кібербезпека в цих секторах вимагає спільних дій, що поєднують людей, процеси та технології; штучний інтелект може розширити можливості перевантажених команд у сферах запобігання, виявлення, реагування та розвитку кадрів, але для подолання зростаючої нерівності необхідна спільна відданість урядів, постачальників технологій, великих установ та громадянського суспільства, щоб розглядати кібербезпеку як фундаментальне суспільне благо та забезпечити доступ до засобів захисту на основі штучного інтелекту для найбільш вразливих верств населення».

(Jason Ruger, Chiara Barbeschi. Target-rich, cyber-poor: How to strengthen cybersecurity and build resilience in vulnerable sectors // World Economic Forum (<https://www.weforum.org/stories/2026/05/target-rich-cyber-poor-how-to-strengthen-cybersecurity-and-build-resilience-in-vulnerable-sectors/>). 07.05.2026).

«Через п'ять років після того, як Управління служб охорони здоров'я (HSE) зазнало найбільшої кібератаки в історії Ірландії, експерти з безпеки попереджають: хоча захисні механізми організації значно покращилися, загрози стали набагато витонченішими. Інцидент 2021 року, організований російською групою Conti за допомогою простого фішингового листа, спричинив руйнівне відключення всієї системи, що серйозно позначилося на вразливих

пацієнтах, зокрема хворих на рак, які втратили доступ до важливих діагностичних обстежень та планів лікування. У відповідь на атаку HSE переглянула свою стратегію кібербезпеки; головний спеціаліст з інформаційної безпеки Ніл Маллен зазначає, що спеціалізована команда з безпеки розширилася з менш ніж десяти співробітників до 70, висловлюючи впевненість, що організація тепер набагато стійкіша та здатна відновлюватися після подібних інцидентів набагато швидше, ніж раніше...

Однак чиновники та експерти з кібербезпеки наголошують, що зловмисники розвиваються не менш стрімко. Сучасні кіберзлочинці — це вже не просто поодинокі хакери, що сидять у підвалах; вони діють як високопрофесійні організації, що мають власні кадрові відділи, системи преміювання та стратегічні цілі. Цей професіоналізм ще більше підсилюється завдяки застосуванню штучного інтелекту, що дозволяє зловмисникам створювати гіперперсоналізовані, ретельно підібрані фішингові листи, які дедалі важче відрізнити від справжніх повідомлень. Незважаючи на підвищену обізнаність HSE та посилені системи, такі експерти, як консультант-онколог професор Шеймус О'Рейлі та фахівець з кібербезпеки Ронан Мерфі, попереджають, що ризик залишається гострим. Поки HSE продовжує вирішувати довгострокові наслідки для пацієнтів, дані яких були скомпрометовані під час злом у 2021 році, залишається загальна думка, що, хоча захисні системи Ірландії вдосконалилися, невпинні інновації цих злочинних угруповань, що використовують штучний інтелект, гарантують, що рівень загрози продовжує зростати». (*Edel McAllister. Cyber attacks more advanced five years on from HSE breach // Ireland's National Public Service Media (https://www.rte.ie/news/ireland/2026/0514/1573383-cyber-attacks-hse/). 14.05.2026*).

«Наприкінці минулого року «Manage My Health» (ММН) — місцевий онлайн-портал (Нова Зеландія), який медичні заклади використовують для обміну інформацією з пацієнтами, — зазнав хакерської атаки та став об'єктом вимагання викупу. Хакерська група Kazu викрала медичні записи майже 100 000 пацієнтів, опублікувала зразки даних в Інтернеті та погрожувала оприлюднити всі дані, якщо не буде сплачено 60 000 доларів США (105 000 доларів)... Три звіти, опубліковані сьогодні на замовлення Health NZ, Міністерства охорони здоров'я та Управління комісара з питань конфіденційності, виявляють серйозні проблеми, пов'язані з недоліками безпеки, відсутністю незалежного нагляду та надмірною залежністю від власних запевнень ММН. Результати розслідування, як повідомляє NZ Herald, підкреслюють, що технічні заходи безпеки ММН на момент порушення були недостатніми, оскільки бракувало систем виявлення незвичайного доступу до даних, які могли б пом'якшити наслідки атаки. Крім того, виникли питання щодо загальної архітектури безпеки та практик управління ризиками. З організаційної точки зору, до складу проектної групи, відповідальної за залучення ММН, не входили фахівці з питань конфіденційності чи безпеки, і вона не провела незалежних перевірок, покладаючись на запевнення ММН, що призвело до недостатньої поінформованості осіб, які приймають рішення, про ризики. Комісар з питань конфіденційності Майкл Вебстер скористався нагодою, щоб закликати до

структурних реформ, зокрема до створення централізованого процесу перевірки для забезпечення відповідності порталів охорони здоров'я стандартам безпеки та внесення змін до Закону про конфіденційність, щоб притягнути до відповідальності сторонніх постачальників у разі невиконання ними вимог безпеки... У звітах компаній «Deloitte» та «CyberCX» також наголошувалося, що рівень цифрової безпеки в секторі охорони здоров'я був нерівномірним і часто недостатнім, що супроводжувалося надмірною залежністю від послуг сторонніх постачальників та неготовністю ММН до подібних інцидентів. Міністерство охорони здоров'я прийняло всі рекомендації, запровадивши такі заходи, як незалежні перевірки безпеки постачальників, більш суворі стандарти обробки даних та комплексний перегляд цифрових систем охорони здоров'я. Фінансовий директор Health NZ Беван Маккензі визнав, що пацієнтів підвели, і вибачився за порушення, яке призвело до призупинення передачі інформації з Нортленда на портал. ММН заявило, що атака була злочинним актом із використанням викрадених облікових даних і що жодних додаткових даних, крім початкової вибірки, публічно не оприлюднювалося. Відтоді на платформі запроваджено обов'язкову багатофакторну автентифікацію, покращено моніторинг у реальному часі, посилено контроль доступу та збільшено кількість незалежних тестувань безпеки. Очікується, що на другому етапі розслідування буде вивчено більш широкі наслідки порушення, включаючи політику зберігання даних, дотримання вимог щодо повідомлення та його непропорційний вплив на маорі Нортленда, який, як було підтверджено, був значним». (*Henry Oliver. Damning health data breach reports released // The Spinoff (<https://thespinoff.co.nz/the-bulletin/27-05-2026/damning-health-data-breach-reports-released>). 27.05.2026*).

Захист персональних даних та соціальні мережі

«Британське Управління комісара з питань інформації (ICO) наклало штраф у розмірі 963 900 фунтів стерлінгів на материнську компанію South Staffordshire Water у зв'язку з серйозним порушенням безпеки, внаслідок якого були викрадені персональні дані понад 633 000 осіб. Інцидент стався у вересні 2020 року, коли співробітник став жертвою фішингового листа, що дозволило зловмисникам встановити шкідливе програмне забезпечення, яке залишалося невиявленим протягом 20 місяців, поки внутрішні проблеми з продуктивністю не спонукали до розслідування у липні 2022 року. Згодом зловмисники викрали 4,1 терабайта даних — включаючи імена, банківські реквізити, паролі та конфіденційну інформацію щодо інвалідності — які були опубліковані в даркнеті...

У ході розслідування ICO було виявлено системні недоліки в системі безпеки, зокрема використання застарілого програмного забезпечення, такого як Windows Server 2003, слабкий контроль адміністративного доступу та недостатній моніторинг, який охоплював лише 5% ІТ-середовища компанії. Регулюючий орган

розкритикував компанію за відсутність проактивних заходів безпеки, зазначивши, що покладатися на проблеми з продуктивністю або записку з вимогою викупу для виявлення порушення є неприйнятним для організації, яка управляє критичною національною інфраструктурою. Хоча ICO спочатку планував накласти більш високий штраф, його розмір було зменшено на 40% після того, як компанія визнала свою відповідальність і погодилася врегулювати справу без оскарження». **(Sinisa Markovic. Poor security left hackers inside water company network for nearly two years // Help Net Security (<https://www.helpnetsecurity.com/2026/05/11/ico-south-staffordshire-cyberattack-fine/>). 11.05.2026).**

«За даними дослідника GitGuardian Гійома Валадона, CISA протягом приблизно шести місяців залишила відкритим публічний репозиторій GitHub під назвою «Private-CISA», що містив близько 844 МБ надзвичайно конфіденційних даних, зокрема паролі у вигляді звичайного тексту, приватні ключі, токени та файли конфігурації з промовистими назвами, такими як «external-secret-repo-creds.yaml» та «AWS-Workspace-Firefox-Passwords.csv». Валадон зазначив, що витік містив облікові дані та артефакти, які могли б відкрити широкі можливості для зломів, такі як доступ до внутрішнього JFrog Artifactory CISA, ключів реєстру Azure, облікових даних AWS, конфігурації та маніфести Kubernetes, файли додатків ArgoCD, інфраструктурний код Terraform, особисті токени доступу GitHub та сертифікати Entra ID SAML, а також те, що він описав як «каталог небезпечних практик», включаючи резервні копії, зафіксовані в Git, та інструкції щодо вимкнення сканування секретів GitHub... 14 травня компанія GitGuardian повідомила про репозиторій до CISA, і його було видалено наступного дня після того, як Валадон звернувся до кількох інстанцій, зокрема поінформувавши журналіста Браяна Кребса, оскільки на початковий звіт CERT/CC надійшло лише автоматичне підтвердження. CISA заявила, що проводить розслідування, і стверджує, що наразі немає ознак того, що оприлюднені дані були скомпрометовані, тоді як Валадон зазначив, що не може підтвердити, чи хтось інший отримав доступ до секретних даних першим, і що репозиторій, судячи з усього, не був розгалужений, а остаточна відповідь належить GitHub. Цей інцидент є особливо незручним, враховуючи роль CISA як провідного агентства з кіберзахисту уряду США, а Валадон також підкреслив наявність «змішаної ідентичності» — комітів, пов'язаних як з електронною адресою підрядника CISA, так і з особистою адресою Yahoo та особистим обліковим записом на GitHub — що, на його думку, є поширеним джерелом важко виявляємих витоків, які мають серйозні наслідки». **(Jessica Lyons. America's top cyber-defense agency left a GitHub repo open with passwords, keys, tokens – and incredibly obvious filenames // Situation Publishing (<https://www.theregister.com/security/2026/05/19/americas-top-cyber-defense-agency-left-a-github-repo-open-with-passwords-keys-tokens-and-incredibly-obvious-filenames/5242915>). 19.05.2026).**

«Масштабний кіберзлом у клубі «Аjax» (Амстердам) підкреслив значні ризики, з якими стикаються спортивні організації через величезні обсяги персональних та операційних даних, що зберігаються у них. 27 травня 2026 року голландська поліція заарештувала в місті Бурен 35-річного чоловіка за неодноразове використання незахищеної веб-уразливості в системах клубу. Хоча «Аjax» спочатку повідомив про витік електронних адрес кількох сотень осіб та обмежених даних, пов'язаних із заборонами на відвідування стадіону, подальші повідомлення RTL свідчать про те, що, ймовірно, було скомпрометовано особисту інформацію понад 300 000 зареєстрованих уболівальників та понад 42 000 записів про абонементи. Найбільше занепокоєння викликала здатність зловмисника змінювати записи про заборони на відвідування стадіону та передавати квитки, поєднуючи витік комерційних даних із прямими наслідками для громадської безпеки та контролю натовпу під час живих заходів...

Цей інцидент вписується у тривожну тенденцію, що спостерігається у європейському футболі: нещодавно подібні порушення були зафіксовані у клубах «Болонья», «Парі Сен-Жермен» та «Манчестер Юнайтед», а також у Королівській голландській футбольній асоціації та Французькій футбольній федерації. Спортивні клуби регулярно керують надзвичайно чутливими базами даних уболівальників, медичними записами, системами продажу квитків, інтелектуальною власністю та комерційними контрактами, проте часто працюють з ІТ-бюджетами та практиками безпеки, які не відповідають їхньому фактичному профілю ризику. Випадок з «Аjax», де вразливість залишалася не виправленою достатньо довго, щоб її можна було використати кілька разів, підкреслює серйозні прогалини в управлінні виправленнями та оцінці ризиків, пов'язаних із сторонніми організаціями...

Що стосується програм корпоративної безпеки та управління ризиками, пов'язаними зі сторонніми організаціями, цей випадок порушення безпеки дає два чітких сигнали: системи, що взаємодіють із клієнтами та користувачами і містять великі обсяги персональних даних або контролюють фізичний доступ, повинні підлягати такому ж суворому графіку встановлення оновлень, як і основні фінансові системи; крім того, реєстри ризиків мають краще відображати межу між цифровими комерційними платформами та фізичною операційною безпекою, яка стає дедалі розмитішою. Розслідування триває, і компанія Ajax зобов'язується повідомити постраждалих осіб, щойно буде підтверджено повний масштаб витоку даних». (*Holger Schulze. Ajax Cyber Breach Exposed 300,000 Fan Records and Stadium-Ban Controls // Cybersecurity Insiders (<https://www.cybersecurity-insiders.com/ajax-cyber-breach-fan-records-stadium-ban-controls/>). 27.05.2026*).

«Рада з питань кібербезпеки уряду ОАЕ опублікувала попередження про зростання ризиків крадіжки цифрової ідентичності, наголосивши, що кожна третя людина може бути вразливою до таких злочинів через поширену практику обміну особистими даними на цифрових платформах та в соціальних мережах. У практичному посібнику щодо захисту цифрової ідентичності Рада підкреслила, що цифрова ідентичність є одним із найцінніших активів як для фізичних осіб, так і для організацій, оскільки містить конфіденційну

інформацію, таку як особисті дані, фінансові операції та медичні записи, які необхідно належним чином захищати. Розвиток штучного інтелекту, Інтернету речей (IoT) та хмарних додатків зробив цифрові ідентичності більш привабливими цілями для кіберзлочинців, які використовують вразливості для підробки особи, шахрайства або продажу на чорному ринку. Захист цифрової ідентичності розглядається як необхідність для забезпечення конфіденційності, запобігання шахрайству та підтримки безперебійного функціонування цифрових послуг без фінансових втрат... Рада зазначила, що кількість кібератак, спрямованих на цифрові ідентичності, у першому півріччі зросла на 32% через все більшу залежність від цифрових послуг. Вона визначила багатофакторну автентифікацію (MFA) як один із найефективніших засобів захисту, здатний запобігти понад 99% атак, пов'язаних із викраденням ідентичності. Ризики виходять за межі крадіжки даних і можуть призвести до шахрайства з використанням викраденої ідентичності, фінансових збитків, шкоди репутації та професійних невдач. Тому користувачам настійно рекомендується уникати передачі конфіденційної інформації, використовувати надійні та унікальні паролі, увімкнути MFA та залишатися пильними. Рада наголосила, що захист цифрової ідентичності залежить не лише від технологій, а й від обізнаності та відповідальної поведінки, попередивши, що компрометація ідентичностей може призвести до серйозних наслідків, таких як фінансове шахрайство, фішинг та масштабні кіберзагрози. Вона порадила громадськості захищати облікові записи, уникати підозрілих посилань, регулярно оновлювати системи та використовувати надійні браузері. Підкреслюючи ризики, пов'язані з соціальними мережами, Рада повідомила, що 40% користувачів соціальних мереж в ОАЕ стикалися з хакерськими атаками після того, як поділилися особистими даними, та наголосила, що 97% кібератак пов'язані зі слабкими паролями, підкресливши важливість використання надійних облікових даних та безпечних цифрових практик як основних засобів захисту від кіберзагроз». (*Abdulla Rasheed. UAE Cybersecurity Council warns of rising digital identity theft risks // Al Nisr Publishing LLC (<https://gulfnews.com/uae/people/uae-cybersecurity-council-warns-of-rising-digital-identity-theft-risks-1.500519565>). 26.05.2026*).

Масштабні витоки персональних даних

«Згідно з аналізом Have I Been Pwned, група зловмисників ShinyHunters викрала особисті дані понад 119 000 осіб після злому сервісу Vimeo у квітні. Vimeo — публічна платформа для розміщення відео, що налічує понад 300 мільйонів зареєстрованих користувачів, — повідомила, що несанкціонований доступ до даних клієнтів та користувачів став наслідком злому в Anodot, сторонньому постачальнику послуг з виявлення аномалій у даних. Компанія заявила, що скомпрометовані бази даних містили переважно технічні дані, назви відео та метадані, а в деяких випадках — електронні адреси клієнтів, але не містили відеоконтенту, облікових даних для входу або інформації про платіжні картки.

Vimeo заявила, що інцидент не спричинив перебоїв у роботі сервісу, що облікові дані Anodot було вимкнено, інтеграцію було видалено, залучено сторонніх експертів з безпеки та повідомлено правоохоронні органи...

Після того як Vimeo відмовився виконати вимоги здирників, група ShinyHunters опублікувала на своєму сайті в даркнеті архів викрадених даних обсягом 106 ГБ, заявивши, що злом відбувся через компрометацію екземплярів Snowflake та BigQuery за допомогою токенів Anodot. Сервіс Have I Been Pwned повідомив, що серед викрадених даних були адреси електронної пошти, а в деяких випадках — імена 119 200 осіб. Раніше група заявляла, що атакувала десятки компаній, використовуючи подібні слабкі місця в системах аутентифікації сторонніх розробників, і відома своїми кампаніями вішингу, спрямованими на компрометацію корпоративних облікових записів з єдиним входом для отримання доступу до підключених SaaS-платформ. Протягом останніх тижнів ShinyHunters також заявила про злами, що зачепили такі великі організації, як Європейська комісія, Rockstar Games, McGraw Hill, Medtronic, Carnival, Zara, 7-Eleven та Udemu...» (*Sergiu Gatlan. Vimeo data breach exposes personal information of 119,000 people // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/vimeo-data-breach-exposes-personal-information-of-119-000-people/). 05.05.2026).*

«Через десять років після того, як у 2015 році внаслідок витоку даних з Управління кадрового менеджменту (OPM) були оприлюднені особисті дані понад 22 мільйонів діючих та колишніх федеральних службовців, осіб, які подавали заявки на отримання допуску до секретної інформації, та членів їхніх сімей, термін дії послуг федерального уряду з захисту жертв від крадіжки особистих даних добігає кінця. Особи, зареєстровані в програмі MyIDCare, створеній після витоку даних для надання послуг з моніторингу кредитів, сканування даркнету, страхування та відновлення, отримують повідомлення про те, що їхня страховка закінчиться через 10 років з дати реєстрації, а повідомлення продовжуватимуться до кінця фінансового року. Спочатку OPM пропонувало три роки захисту з покриттям до 1 мільйона доларів, але пізніше Конгрес затвердив 10 років і до 5 мільйонів доларів. Агентство уклало контракти на суму понад 750 мільйонів доларів з компанією ID Experts (нині IDX) для управління програмою...

Управління з питань персоналу (OPM) заявило, що розглядало можливість продовження дії страхового покриття, але дійшло висновку, що це не буде відповідальним використанням коштів платників податків, посиляючись на високу вартість програми та відносно невелику кількість заяв, поданих останнім часом. Раніше Управління з питань урядової відповідальності критикувало OPM за надмірні витрати на страхове покриття, яке воно назвало, ймовірно, непотрібним. У рамках угоди про врегулювання колективного позову жертвам, які довели наявність фінансових труднощів, було виділено 63 мільйони доларів, але в підсумку було розподілено лише 4,8 мільйона доларів, а решта коштів була повернута до казни... Завершення програми викликало неоднозначну реакцію: деякі постраждалі особи стверджують, що уряд повинен надавати довгостроковий

або довічний захист, враховуючи чутливість викрадених даних та ймовірність того, що вони залишаються в руках іноземців, тоді як інші визнають проблеми, пов'язані з витратами, і заявляють, що люди повинні брати на себе відповідальність за моніторинг власного кредитного рейтингу. Деякі законодавці, зокрема сенатор Марк Уорнер, продовжують виступати за продовження дії програми, попереджаючи, що жертви можуть стикатися з ризиками протягом усього життя внаслідок одного з найсерйозніших федеральних кіберзлочинів в історії». **(Eric Katz and David DiMolfetta. 10 years after OPM data breach, identity protection benefits for affected feds start to expire // Government Media Executive Group LLC. (<https://www.govexec.com/management/2026/05/10-years-after-opm-breach-identity-protection-services-affected-feds-expire/413336/>). 05.05.2026).**

«Компанія Carnival Corp, один із найбільших операторів круїзних лайнерів, повідомила про кіберінцидент, що призвів до витоку персональних даних. У заяві, опублікованій вночі 27 травня 2026 року, компанія повідомила, що атака сталася 14 квітня 2026 року, коли зловмисник отримав доступ до облікового запису співробітника за допомогою методів соціальної інженерії. Зловмисник отримав доступ до обмеженої частини ІТ-системи Carnival, хоча конкретні деталі щодо області, до якої було отримано доступ, не розголошувалися. Компанія оперативно відреагувала, заблокувавши несанкціоновану діяльність та залучивши зовнішніх експертів з безпеки для посилення захисту та проведення ретельного розслідування. У ході цього процесу Carnival встановила, що зловмисник незаконно отримав доступ до певної особистої інформації, зокрема імен, адрес, електронних адрес, номерів телефонів, дат народження та номерів державних посвідчень, таких як паспорти та водійські посвідчення... Компанія Carnival повідомила про інцидент усіх постраждалих та опублікувала офіційні заяви для осіб, контактні дані яких є застарілими або недостатніми. Компанія також заявила, що посилила заходи безпеки та запропонувала постраждалим послугу моніторингу кредитної історії. Незважаючи на ці зусилля, Carnival не вказала загальну кількість постраждалих осіб і не оприлюднила деталей щодо зловмисника або конкретного характеру атаки. Компанія наголосила на своєму незмінному прагненні вдосконалювати системи ІТ-безпеки та захисту даних, щоб випереджати нові загрози». (Daniel Croft. Carnival Cruise Line confirms cyber incident that compromised personal data // Momentum Media (<https://www.cyberdaily.au/security/13661-carnival-cruise-line-confirms-cyber-incident-that-compromised-personal-data>). 28.05.2026).

Кібербезпека Інтернету речей. Штучний інтелект

«Нове дослідження Британського інституту безпеки штучного інтелекту (AI Security Institute) свідчить, що модель GPT-5.5 від OpenAI (кодова назва

«Spud») тепер не поступається Mythos Preview від Anthropic за рівнем розвинених кіберможливостей, скоротивши перевагу Mythos, яка, як очікувалося, мала бути значною. Під час тестування GPT-5.5 успішно завершила складну 32-крокову симульовану кібератаку на корпорацію у двох із десяти прогонів, порівняно з трьома із десяти для Mythos; до появи Mythos жодна модель штучного інтелекту ніколи не завершувала цей тест. GPT-5.5 також перевершила Mythos у кількох завданнях типу «захоплення прапора», що вимірюють виявлення вразливостей, реверс-інжиніринг та експлуатацію веб-додатків. Коли Mythos був запущений, компанія Anthropic припустила, що конкуренти відстають на 6–18 місяців у подібних кіберпоказниках, але нові результати ставлять під сумнів цей графік і викликають питання щодо того, скільки часу урядів та операторів критичної інфраструктури залишилося на зміцнення захисту...

Доступ до цих розширених можливостей залишається суворо обмеженим. Компанія Anthropic надала доступ до Mythos лише близько 40 організаціям, зокрема учасникам партнерської програми Project Glasswing, тоді як OpenAI надає версії GPT-5.4 та GPT-5.5 з більш ліберальними обмеженнями лише перевіреним фахівцям із кібербезпеки в рамках своєї програми Trusted Access, дотримуючись суворіших обмежень щодо публічних версій. Як повідомляється, Білий дім закликав Anthropic не розширювати доступ до Mythos через міркування національної безпеки, навіть попри те, що OpenAI співпрацює з федеральним, штатним, місцевим урядами США та урядами союзників, щоб забезпечити контрольований доступ з метою кібербезпеки». *(Sam Sabin. OpenAI isn't far behind Mythos' hacking powers // Axios Media Inc. (<https://www.axios.com/2026/05/05/openai-anthropic-mythos-cyber-testing>). 05.05.2026).*

«Дослідники у сфері безпеки продемонстрували, що один зламаний гуманоїдний робот Unitree може автоматично заражати інші сумісні пристрої в радіусі дії Bluetooth, створюючи саморозповсюджувальну бот-мережу роботів. Експлоїт, названий «UniPwn», націлений на нову лінійку продуктів Unitree і використовує жорстко запрограмовані ключі шифрування, спільні для всіх пристроїв. Після зараження робот сканує сусідні пристрої через Bluetooth Low Energy, заражає їх без втручання людини та запускає експоненціальне поширення, оскільки кожен новозаражений пристрій починає сканувати та атакувати інші — фактично перетворюючи флоти на заразні мережі...

Ризики виходять за межі цифрових збитків. Дослідники продемонстрували, що зламані роботи можна дистанційно керувати, зокрема змушувати їх виконувати фізичні рухи, такі як удари по людині, а також захоплювати їх за допомогою введення голосових команд. Окрім потенційної фізичної шкоди, заражені роботи можуть виконувати функції засобів спостереження, регулярно передаючи відео-, аудіо- та сенсорні дані на віддалені сервери... Незважаючи на відповідальне розкриття інформації та публічні демонстрації вразливостей у 2025 році, дослідники стверджують, що компанія Unitree не вжила суттєвих заходів для усунення недоліків, залишивши розгорнуті роботи на заводах, у лікарнях та на

складах незахищеними. Оскільки ця вразливість може поширюватися як черв'як, один зламаний пристрій може заразити весь парк за лічені години, що викликає серйозні занепокоєння щодо безпеки дедалі більш автономних мережових робототехнічних систем». *(Al Landes. When Robots Start Hacking Each Other: The Disastrous Threat No One Saw Coming // Gadget Review (<https://www.gadgetreview.com/when-robots-start-hacking-each-other-the-disastrous-threat-no-one-saw-coming>). 05.05.2026).*

«У 2026 році ситуація у сфері кібербезпеки характеризується критичним парадоксом: штучний інтелект одночасно надає зловмисникам безпрецедентні можливості та швидкість, а захисникам — інструменти для переосмислення операцій з забезпечення безпеки. Ця конвергенція відбувається на тлі постійного дефіциту кваліфікованих кадрів в організаціях та загрози з боку квантових обчислень, які обіцяють зламати сучасні криптографічні стандарти. Кіберзлочинці, використовуючи технології корпоративного рівня, перейшли до довгострокової стратегії: вони проникають у системи та залишаються в прихованому режимі, щоб завдати максимальної шкоди... Щоб протистояти цим новим загрозам, керівники служб безпеки повинні перейти від реактивної стратегії, орієнтованої на інструменти, до проактивного, інтегрованого підходу, в основі якого лежать постійне управління виявленням загроз, уніфікований огляд ризиків та впровадження механізмів виявлення дідфейків у саму основу своїх систем безпеки. Ця еволюція вимагає не лише впровадження нових технологій, а й фундаментального вирішення системного дефіциту кваліфікованих кадрів шляхом покращення співпраці між науковими колами та промисловістю, використання агентного штучного інтелекту для автоматизації рутинних завдань та стратегічної підготовки до постквантового майбутнього шляхом розробки криптоагільних архітектур...» *(Sheetal Mehta. Four key areas in cybersecurity that need fresh thinking and actionable steps in 2026 // Future US, Inc. (<https://www.techradar.com/pro/four-key-areas-in-cybersecurity-that-need-fresh-thinking-and-actionable-steps-in-2026>). 06.05.2026).*

«Нове дослідження професора Майкла Лоунса з Університету Геріот-Ватт попереджає, що інтеграція генеративної ШІ в системи машинного навчання може спричинити значні ризики, незважаючи на потенційне підвищення ефективності та зниження витрат. У статті, опублікованій у журналі Patterns, Лоунс стверджує, що використання генеративної ШІ для проектування, побудови, навчання або експлуатації робочих процесів машинного навчання може збільшити вразливість до кібератак, витоків даних, упередженості щодо недостатньо представлених груп та інших непередбачених негативних наслідків. Він застерігає, що хоча інструменти генеративного ШІ — зокрема великі мовні моделі (LLM) — дедалі частіше інтегруються в процеси машинного навчання, їхні обмеження та непередбачуваність вимагають ретельного аналізу, особливо в секторах з високими ризиками, таких як охорона здоров'я та фінанси...»

У дослідженні визначено чотири основні напрямки застосування генеративної ШІ: як компонент у ланцюжках машинного навчання, для проектування та кодування систем, для генерації синтетичних навчальних даних та для аналізу результатів. Кожен такий випадок використання несе в собі ризики, особливо коли в одній системі використовується кілька великих мовних моделей (LLM) або коли «агентні» моделі самостійно взаємодіють із зовнішніми інструментами. Основною проблемою є те, що LLM можуть «марити», робити помилки та працювати непрозоро, що ускладнює забезпечення надійності, прозорості та дотримання законодавчих вимог. Лоунс радить розробникам уникати зайвої складності та ретельно балансувати між інноваціями та ризиками, наголошуючи, що те, що генеративна ШІ може бути інтегрована в системи машинного навчання, не означає, що це потрібно робити — особливо там, де рішення безпосередньо впливають на життя та добробут людей». **(Lewis Robertson. Study warns cost-cutting use of generative AI could increase cyber-attack risks // Science X (<https://phys.org/news/2026-04-generative-ai-cyber.html>). 03.05.2026).**

«...Штучний інтелект здатний докорінно змінити сферу кібербезпеки, замінивши традиційну складність цієї галузі на більш доступні системи, що працюють на основі природної мови. Протягом десятиліть професіоналізм у сфері кібербезпеки залежав від володіння численними пропрієтарними інструментами, інтерфейсами та технічними мовами, що призвело до появи вузькоспеціалізованого «священства», яке, у свою чергу, сприяло виникненню сьогоденішнього гострого дефіциту кадрів. Організації часто керують десятками інструментів безпеки від багатьох постачальників, і внаслідок цього складність стала значним оперативним тягарем та бар'єром для входу на ринок. ШІ, зокрема великі мовні моделі та агентні системи, стає абстрактним шаром, що дозволяє аналітикам та адміністраторам описувати цілі простою мовою, тоді як система перетворює ці запити на технічні дії, зміщуючи фокус з синтаксису інструментів на розуміння загроз та стратегії...

Існує три основні демократизуючі наслідки цієї зміни: інтерфейси на основі природної мови значно скорочують час, необхідний для освоєння цієї галузі; вбудовані експертні знання в галузі ШІ надають невеликим організаціям доступ до можливостей, які раніше були доступні лише великим спеціалізованим командам; а консолідація платформ на базі ШІ зменшує обсяг розрізнених знань, необхідних для управління операціями з безпеки. У сукупності ці зміни можуть розширити коло учасників у сфері кібербезпеки та допомогти вирішити проблему глобального дефіциту кваліфікованих кадрів. Однак є застереження, що ШІ створює нові ризики, зокрема використання тих самих технологій зловмисниками, надмірну залежність від невеликої кількості платформ на базі ШІ та небезпеку, пов'язану з погано керованими агентами ШІ, що мають широкі привілеї. ШІ не усуне складності кібербезпеки, а лише перемістить їх, дозволивши фахівцям-людям більше зосередитися на оцінці, ризиках та прийнятті рішень, одночасно роблячи цю галузь більш доступною та стійкою». **(Vishal Salvi. How AI could open up cybersecurity to a wider workforce // World Economic Forum**

(<https://www.weforum.org/stories/2026/05/how-ai-could-open-up-cybersecurity-to-a-wider-workforce/>). 05.05.2026).

«Презентація компанії Anthropic проекту Claude Mythos викликала бурхливу реакцію в галузі кібербезпеки, підкріпивши думку про те, що штучний інтелект змінює правила гри, але насправді він насамперед прискорює роботу системи, яка й так вже не працює належним чином. Традиційне припущення про те, що захисники мають достатньо часу між виявленням уразливості та її експлуатацією, більше не відповідає дійсності: те, що раніше займало роки, тепер може відбутися за лічені години, внаслідок чого основна проблема переноситься з виявлення недоліків на прийняття рішення про те, що саме потрібно виправити, та вчасне застосування виправлень... У плані захисту штучний інтелект може виявляти величезну кількість вразливостей, але все ще не може визначити, які з них дійсно можна використати, через що команди з безпеки перевантажені накопиченими завданнями та проблемами з визначенням пріоритетів, тоді як зловмисники мають простішу мету — їм достатньо лише одного дієвого шляху, і вони використовують штучний інтелект для тестування варіантів зі швидкістю машини. Цей дисбаланс посилюється застарілими практиками безпеки, такими як щорічні тести на проникнення, повільні цикли випуску виправлень та ретроспективна звітність, які ґрунтуються на хибному припущенні, що час на боці захисника, навіть коли поверхня атаки розширюється через хмарні сервіси, інтеграції, застарілі системи та слабкі компоненти постачальників...

Отже, інцидент з Mythos висвітлює більш загальну проблему вразливості: багато організацій не до кінця розуміють, що саме є вразливим і як це можна використати. Для вирішення цієї проблеми необхідний перехід від реактивної безпеки до безперервної оцінки ризиків, що ґрунтується на прозорості, перевірці можливостей зловживання та оперативності, з урахуванням того, що сучасні загрози переросли можливості суто людського реагування. Кібербезпека дедалі більше перетворюється на змагання «ШІ проти ШІ», де захисники мусять використовувати ШІ для постійного тестування власних систем та визначення пріоритетності реальних ризиків, але людське судження залишається незамінним, оскільки ШІ бракує контексту для визначення того, що є найважливішим. Таким чином, поле бою зміщується від того, хто першим знайде вразливості, до того, хто швидше прийме кращі рішення, перетворюючи інформацію, виявлену ШІ, на дії, перш ніж зловмисники зможуть нею скористатися». (*Jorge Monteiro. Cybersecurity has a speed problem // TechDay (<https://securitybrief.co.uk/story/cybersecurity-has-a-speed-problem>)*). 07.05.2026).

«Штучний інтелект стрімко змінює сферу кібербезпеки, але твердження про те, що він замінить фахівців з безпеки або зробить постачальників послуг непотрібними, є здебільшого перебільшенням, оскільки сучасні середовища безпеки — що охоплюють розширювані хмарні інфраструктури, захист

конфіденційних даних, системи ідентифікації та дедалі витонченіші атаки — як і раніше потребують людського судження та експертних знань. Натомість ІІІ стає мультиплікатором сили, що зменшує навантаження та складність роботи команд з безпеки, допомагаючи аналітикам працювати швидше та зосередитися на найважливіших загрозах. Асистенти на базі ІІІ можуть спростити повсякденні операції, забезпечуючи взаємодію з платформами безпеки природною мовою, що дозволяє користувачам швидко досліджувати конфігурації, поведінку політик та аномалії, не перебираючи панелі інструментів, журнали або складні інструменти запитів...

Штучний інтелект також покращує виявлення загроз та захист даних, відходячи від жорстких підходів, заснованих на правилах, на користь контекстного аналізу, покращуючи виявлення та класифікацію даних у гібридних середовищах, зменшуючи кількість помилкових спрацьовувань та використовуючи базові моделі поведінки для більш раннього виявлення аномальної активності, такої як внутрішні загрози або скомпрометовані облікові дані. У сфері управління ідентифікацією та доступом штучний інтелект може виступати в ролі оперативного «другого пілота», надаючи аналітичні висновки, рекомендуючи вдосконалення політик та автоматизуючи повторювані завдання в рамках механізмів управління, допомагаючи командам справлятися зі зростаючою складністю, а не замінюючи їх... Водночас широке впровадження штучного інтелекту створює нові ризики для безпеки — такі як введення підказки, маніпулювання моделями та витік даних — що робить надзвичайно важливим забезпечення безпеки програм, моделей та навчальних даних штучного інтелекту протягом усього життєвого циклу ІІІ. Загалом, головний висновок полягає в тому, що майбутнє кібербезпеки — це не протистояння людей і машин, а поєднання людського досвіду та знань із можливостями штучного інтелекту». (*Philippe Vallée. AI in cybersecurity: How intelligent tools are strengthening security teams // Thales* (<https://www.thalesgroup.com/en/news-centre/insights/cybersecurity/ai-cybersecurity-how-intelligent-tools-are-strengthening>). 05.05.2026).

«Стрімкий розвиток штучного інтелекту допоміг британським малим підприємствам покращити маркетинг, обслуговування клієнтів, автоматизацію та аналіз даних, але він також супроводжувався зростанням кількості та складності кібератак, які зачепили навіть таких великих ритейлерів, як Marks & Spencer, The Co-op та Pandora, і посилили занепокоєння серед засновників малих та середніх підприємств. Незважаючи на це, опитування Moneysupermarket показало, що лише 10% малих та середніх підприємств проводять для своїх співробітників навчання з питань безпеки штучного інтелекту, що свідчить про розширення розриву між впровадженням штучного інтелекту та його безпечним використанням... За даними уряду, за минулий рік кіберзлочини або атаки торкнулися 43% підприємств — близько 612 000 компаній — причому аналогічно високі показники спостерігаються серед мікро- та малих підприємств, тоді як у звіті Bridewell «Кібербезпека в секторі критичної інфраструктури (CNI) — 2026» зазначено, що фішинг та компрометація

корпоративної електронної пошти є найпоширенішими загрозами, причому в середньому на одну організацію припадає 11 таких атак на рік. Фінансові ризики є серйозними: дослідження Samsung показує, що кожна п'ята МСП може припинити діяльність протягом трьох місяців після порушення, а атаки можуть коштувати близько 100 000 фунтів стерлінгів на рік у вигляді втрачених доходів та штрафів... Нестача навчальних ресурсів зумовлена обмеженим часом, бюджетом та кількістю спеціалістів, а ситуацію погіршує дефіцит кваліфікованих кадрів у сфері кібербезпеки, який наприкінці 2025 року зріс на 8% порівняно з попереднім роком, через що багато власників не мають чітких рекомендацій щодо безпечного впровадження штучного інтелекту. Для підвищення стійкості МСП рекомендується вживати таких простих заходів, як використання надійних унікальних паролів, увімкнення багатофакторної автентифікації, оновлення програмного забезпечення, проведення коротких регулярних навчальних заходів для зменшення людських помилок, встановлення чітких політик щодо дозволених інструментів ІІІ та даних, якими можна ділитися, а також впровадження доступних засобів захисту, таких як захист кінцевих точок, безпечні хмарні сервіси, автоматичне резервне копіювання та практичний план відновлення». *(Emily Clark. SMEs fall short on AI cybersecurity training despite rising risks // Marketing VF Ltd. (<https://startups.co.uk/news/ai-cybersecurity-training/>). 05.05.2026).*

«Інфраструктура інтелектуальних технологій, така як «розумні міста» та «розумні енергомережі», тісно інтегрує фізичні системи з цифровими пристроями, однак така взаємопов'язаність створює серйозні виклики у сфері кібербезпеки, оскільки багато мережевих «вузлів» (датчики, інвертори, інтелектуальні лічильники та інші пристрої Інтернету речей) часто не захищені, не мають надійних засобів захисту та не стандартизовані між різними виробниками. Зростаюча кількість підключених пристроїв розширює площину атаки, а хмарні архітектури можуть посилити наслідки компрометації, дозволяючи зловмиснику використовувати один слабкий вузол як шлюз до більш широких систем, що потенційно може призвести до витоку конфіденційних даних клієнтів або надати контроль над критичною інфраструктурою. Мережі «розумних міст» стикаються з такими загрозами, як атаки «людина посередині», крадіжка даних, захоплення пристроїв, DDoS та постійна відмова в обслуговуванні (PDoS), тоді як штучний інтелект може ще більше збільшити ризик, знижуючи технічні бар'єри для зловмисників, прискорюючи виявлення вразливостей та уможливлюючи створення адаптивного шкідливого програмного забезпечення на основі штучного інтелекту, яке ухиляється від виявлення та націлене на цінні активи...

Захист «розумних» міст вимагає врахування трьох взаємопов'язаних рівнів — апаратного забезпечення, програмного забезпечення та людського фактора — у мільйонах пристроїв, розгорнутих у громадських і часто фізично доступних місцях. Ключові засоби захисту включають безпечний та зашифрований обмін даними, аутентифікацію на основі сертифікатів, надійне управління доступом, зашифровані резервні копії, оперативне встановлення виправлень та скоординоване розгортання

оновлень, фізичну стійкість до несанкціонованого втручання, а також сегментацію мережі, що дозволяє локалізувати атаки без порушення роботи всіх сервісів. Все частіше використовуються засоби контролю на передньому плані, такі як брандмауери з глибокою перевіркою пакетів, архітектура «нульової довіри», виявлення вторгнень, фільтрування трафіку та хмарні засоби захисту від DDoS-атак, але ефективна безпека також залежить від поведінки людей, зокрема від уникнення використання стандартних паролів та застосування двофакторної автентифікації...

Інтелектуальні енергомережі несуть особливо серйозні та складні для управління ризику, оскільки їхня робота значною мірою залежить від даних інтелектуальних лічильників та підключених систем управління, а будь-які збої можуть безпосередньо вплинути на надійність електропостачання. Інтелектуальні лічильники можуть бути використані для крадіжки електроенергії та фальсифікації показань, що погіршує прогнозування навантаження, а їх відкрите розміщення поблизу зарядних станцій для електромобілів розширює шляхи атак. Інші вразливі компоненти включають датчики Інтернету речей (IoT), системи SCADA та сонячні інвертори, особливо з огляду на те, що застаріле обладнання модернізується з додаванням можливостей підключення без повного дотримання стандартів IT-безпеки; рутинні заходи, такі як перезавантаження або встановлення виправлень, можуть бути складними, оскільки прості можуть перервати електропостачання. Хоча такі стандарти, як DLMS/COSEM, визначають вимоги до шифрування та автентифікації, реальна безпека залежить від надійної реалізації, перевірки та захисту ключів, що може виявитися складним завданням з огляду на обмеження щодо вартості пристроїв. Загалом, для забезпечення безпеки інтелектуальної інфраструктури необхідні підходи, що передбачають вбудовану безпеку, посилення сертифікації та стандартизації, скоординовані зусилля урядів і виробників, а також постійні інвестиції, з урахуванням того, що в майбутньому безпека «розумних міст» може перетворитися на протистояння «ШІ проти ШІ» між зловмисниками та захисниками». (*Liam Critchley. As infrastructure becomes smarter, so does cybersecurity // Electronics Weekly (<https://www.electronicsworld.com/news/as-infrastructure-becomes-smarter-so-does-cybersecurity-2026-05/>). 08.05.2026*).

«У новому звіті Custom Market Insights прогнозується стрімке зростання світового ринку кібербезпеки «розумних» енергомереж у зв'язку з тим, що енергетичні компанії переходять на цифрові технології в енергетичній інфраструктурі та стикаються зі зростаючими кіберризиками й регуляторним тиском. Обсяг ринку оцінюється приблизно в 5,68 млрд доларів у 2025 році, за прогнозами, у 2026 році він досягне 7,19 млрд доларів, а до 2035 року, як очікується, зросте приблизно до 67,02 млрд доларів, що означає середньорічний темп зростання (CAGR) близько 28,2% у період з 2026 по 2035 рік. Зростання зумовлене широким впровадженням інтелектуальних лічильників, автоматизованих підстанцій, розподілених енергоресурсів та сучасних платформ управління енергомережами, що підвищує ефективність і надійність, але також розширює можливості підключення та площу атаки. У відповідь на це енергетичні компанії

інвестують у системи виявлення вторгнень у мережу, захист кінцевих точок, безпечні протоколи зв'язку, управління ідентифікацією та моніторинг загроз у реальному часі, тоді як уряди та регуляторні органи запроваджують більш суворі вимоги до кібербезпеки для захисту національних енергомереж... Розвитку ринку також сприяють досягнення в галузі штучного інтелекту, машинного навчання, аналітики загроз у режимі реального часу та хмарних платформ безпеки, які допомагають виявляти аномалії, запобігати вторгненням і прискорювати реагування, а також зростаюча складність, пов'язана з більш тісною інтеграцією відновлюваних джерел енергії, електромобілів та розподілених енергетичних систем». ***(Global Smart Grid Cybersecurity Market Size/Share Worth USD 67.02 Billion by 2035 at a 28.2% CAGR: Custom Market Insights // yahoo!finance (<https://uk.finance.yahoo.com/news/latest-global-smart-grid-cybersecurity-213000019.html>). 06.05.2026).***

«Штучний інтелект кардинально змінює сферу кібербезпеки в навчальних закладах, виступаючи як потужним засобом захисту, так і ефективним зброєю для зловмисників, що ставить питання про те, чи переважають його переваги недоліки. З точки зору захисту ШІ підвищує рівень безпеки завдяки швидкому аналізу величезних обсягів даних для виявлення аномалій — таких як підозрілі спроби входу в систему — які люди можуть пропустити, а також забезпечує автоматизований цілодобовий моніторинг і реагування, що є особливо цінним для ІТ-команд, які відчувають нестачу кадрів. І навпаки, кіберзлочинці використовують ШІ для створення дуже переконливих, без помилок фішингових повідомлень та для автоматизації виявлення слабких паролів і прогалин у мережі... Крім того, впровадження засобів безпеки на основі штучного інтелекту вимагає ретельного моніторингу мережевої активності, поведінки під час входу в систему та використання систем, що викликає серйозні занепокоєння щодо конфіденційності; навчальні заклади повинні гарантувати відповідність цих систем нормативним вимогам, щоб дані учнів та співробітників не потрапляли до рук публічних моделей штучного інтелекту. Оскільки штучний інтелект не є безвідмовним і іноді може створювати помилкове відчуття безпеки, не слід покладатися на нього як на універсальне рішення. Натомість школам потрібна збалансована стратегія, яка поєднує інструменти ШІ з надійними базовими практиками: всебічне навчання персоналу виявленню фішингу, багатофакторна автентифікація, регулярні оновлення програмного забезпечення та використання надійних паролів або менеджерів паролів. Нарешті, щоб пом'якшити фінансові наслідки неминучих витоків даних або інцидентів із програмним забезпеченням-вимагачем, школи повинні підкріпити свої захисні заходи кіберстрахуванням як запобіжним засобом». ***(Does AI threaten or strengthen cybersecurity in schools? // EdTech Innovation Hub (<https://www.edtechinnovationhub.com/news/does-ai-threaten-or-strengthen-cybersecurity-in-schools>). 04.05.2026).***

«У звіті Всесвітнього економічного форуму (WEF), підготовленому спільно з KPMG під назвою «Підсилення захисників: штучний інтелект для кібербезпеки», стверджується, що штучний інтелект стає основним чинником сучасної кіберзахисту, але приносить користь лише за умови його стратегічного впровадження, суворого управління та постійного контролю з боку людини. Спираючись на приклади партнерських організацій, у звіті керівникам та керівникам служб інформаційної безпеки (CISO) рекомендується закріпити впровадження штучного інтелекту в корпоративній стратегії та бажаних бізнес-результатах — таких як операційна стійкість, дотримання нормативних вимог, довіра клієнтів та економічна ефективність — а потім оцінити готовність у всіх процесах, даних, інфраструктурі, навичках та управлінні, перевірити рішення за допомогою структурованих пілотних проектів із чіткими критеріями успіху та обережно масштабувати, постійно контролюючи, вдосконалюючи та керуючи відхиленням моделі... У звіті зазначається, що 77% організацій вже використовують ШІ у сфері кібербезпеки, причому лідирують великі підприємства завдяки більшому фінансуванню, кваліфікованим кадрам та зрілості даних, тоді як менші організації, урядові структури та неурядові організації відстають. За умови правильного впровадження ШІ може зменшити навантаження на команди з безпеки та підвищити ефективність їхньої роботи: 88% команд повідомляють про економію часу та збільшення можливостей для проактивного захисту, а широке використання ШІ пов'язують зі скороченням термінів виявлення порушень приблизно на 80 днів та зменшенням середніх витрат, пов'язаних із порушеннями, на 1,9 млн доларів. ШІ також допомагає вирішувати структурні проблеми, такі як обсяг і складність атак, нестача кваліфікованих кадрів, втома від сповіщень і вигорання, розширення площі атаки та приховані вразливості, а також зростаючі регуляторні вимоги в рамках таких режимів, як DORA та NIS2, шляхом прискорення виявлення, реагування, звітування та документування...

Водночас зловмисники використовують ШІ для дій зі швидкістю машин — автоматизуючи розвідку, створюючи шкідливе програмне забезпечення, знаходячи вразливості в коді та уникаючи виявлення — тому завдання оборони переходить від простої автоматизації завдань до вдосконалення процесу прийняття рішень та визначення пріоритетності ризиків у великих масштабах. У звіті застерігають від надмірної залежності від автоматизації, яка може створювати «сліпі зони» та підривати людський досвід, і наголошують на необхідності тестування сценаріїв збою та збереження стійкості у разі компрометації або недоступності систем ШІ. У ньому підкреслюється, що агентний ШІ може надати захисникам швидкість та автономію, але також розширює площину атаки, вносить непередбачуваність (включно з галюцинаціями та маніпуляціями) і може випередити нагляд, що вимагає нових захисних бар'єрів, структур підзвітності та моделей управління, адаптованих до автономних агентів... Загалом, WEF доходить висновку, що штучний інтелект може істотно посилити кібербезпеку за умови поєднання його з високоякісними даними, кваліфікованими командами, інтегрованою інфраструктурою та підтримкою керівництва, але його впровадження має відбуватися поетапно, з орієнтацією на вимірювані результати та постійним переглядом ризиків і заходів контролю у міру розвитку технологій та еволюції

загроз». (*Anna Ribeiro. WEF maps path to AI-driven cybersecurity, calls for structured deployment, continuous monitoring, human control // Industrial Cyber* (<https://industrialcyber.co/ai/wef-maps-path-to-ai-driven-cybersecurity-calls-for-structured-deployment-continuous-monitoring-human-control/>). 06.05.2026).

«У вигаданому сценарії на Substack під назвою «Глобальна криза інтелекту 2028 року», опублікованій у лютому компанією Citrini Research, висловлювалася думка, що стрімке впровадження штучного інтелекту може спричинити масові звільнення «білих комірців», дефляційну спіраль і навіть системний економічний колапс; хоча багато експертів відкинули цей сценарій як нереалістичний або політично вмотивований, такі діячі, як генеральний директор Anthropic Даріо Амодеї, продовжують попереджати про наближення масштабного скорочення робочих місць... Відображаючи загальну тривогу, лютневе опитування Resume Builder показало, що 57% працівників «чіпляються за роботу», 70% бояться, що їх замінять штучним інтелектом, а 63% хвилюються щодо можливих звільнень протягом найближчих шести місяців. У дискусії стверджується, що організації повинні бути обережними і не впроваджувати ШІ таким чином, щоб це погіршувало якість роботи та моральний стан співробітників. Наводиться негативний приклад з The Plain Dealer, де статті, написані ШІ — незважаючи на редагування — піддавалися критиці за слабкі запобіжні заходи, такі як перевірка фактів та послідовне редагування, а також за те, що вони давали гірші результати для читачів... Водночас дедалі ширше визнається, що перепідготовка кадрів є нагальною потребою: зокрема, фахівці з кібербезпеки та ІТ повинні навчитися використовувати інструменти штучного інтелекту для збереження своєї ефективності, наприклад, шляхом навчання аналітиків SOC методам пошуку загроз із застосуванням ШІ, які можуть виявитися ефективнішими, ніж ручний аналіз журналів. Висновки дебатів у Джонс-Хопкінсі щодо ШІ та робочих місць підкреслили, що майбутній успіх залежить від зміцнення унікальних людських переваг — судження, емпатії, критичного мислення, гнучкості та етичної свідомості — при одночасному освоєнні інструментів ШІ та застосуванні їх до незахищених груп та менших організацій. Що стосується саме кібербезпеки, у статті підкреслюється роль цієї галузі у нагляді та «контролі» за агентами та додатками на базі штучного інтелекту, у мінімізації нових ризиків, пов'язаних із ШІ (зокрема, несанкціонованої поведінки агентів та сценаріїв внутрішніх загроз), а також у наданні допомоги організаціям у поєднанні старих і нових операційних моделей за допомогою оновлених механізмів управління персоналом, процесами та технологіями. Головний висновок полягає в тому, що ШІ не вирішить такі проблеми, як бідність чи кібербезпека, автоматично; це зможуть зробити лише люди, які відповідально та вміло використовують ШІ». (*Daniel J. Lohrmann. How to Upskill for Cybersecurity and Stay Ahead in the Age of AI // e.Republic LLC* (<https://www.govtech.com/security/how-to-upskill-for-cybersecurity-and-stay-ahead-in-the-age-of-ai>). 05.2026).

«Генеральний директор Trend-Setters Consulting Сем Шар (Sam Shar) висловив занепокоєння тим, що консалтингові компанії надто стрімко прискорюють впровадження штучного інтелекту в корпоративному секторі, що підвищує ризики для кібербезпеки та потенційно може спричинити нову хвилю інцидентів у сфері безпеки. Виступаючи на тлі загального зростання кіберзагроз — Check Point Research повідомляє, що кількість щотижневих кіберінцидентів подвоїлася в період з 2021 по 2025 рік, а IBM виявила, що 97% організацій стикалися з інцидентами безпеки, пов'язаними зі штучним інтелектом — Шар стверджував, що комерційні стимули спонукають консультантів рекомендувати велику кількість проєктів зі штучного інтелекту, незалежно від того, чи готові клієнти до їх впровадження з операційної точки зору та з точки зору безпеки. Опитування в галузі підтверджують ці побоювання: BCG виявила, що 61% генеральних директорів заявили, що їхні ради директорів поспішають із трансформацією ІІІ, а KPMG виявила, що лише 20% організацій, які експериментують із ІІІ, відчувають впевненість у управлінні пов'язаними з цим ризиками...

Головна теза Шара полягає в тому, що консалтингові фірми стали ключовим каналом збуту для провідних постачальників ІІІ, а домовленості між розробниками технологій та консалтинговими компаніями можуть спотворювати процес прийняття рішень, оскільки в них перевага надається обсягу проєктів, а не їхній якості, безпеці та реальній бізнес-цінності. Коли організації модернізують існуючі технологічні стеки за допомогою систем ІІІ, а співробітники залишаються недостатньо навченими щодо пов'язаних з цим ризиків, створюються нові поверхні атаки, і організації залишаються незахищеними. Він описав ситуацію як «неминучу катастрофу в сфері кібербезпеки» і назвав те, що він охарактеризував як менталітет «золотої лихоманки», поширений у деяких частинах галузі.

Щоб вирішити цю проблему, Шар закликав консалтингові компанії обмежити кількість одночасних проєктів зі штучного інтелекту, які вони реалізують для окремих клієнтів, приділяти більше часу роботі безпосередньо в організаціях клієнтів після впровадження для моніторингу систем та виявлення слабких місць, а також надавати пріоритет навчанню співробітників як фундаментальній складовій впровадження. Він визнав, що такий підхід передбачає згоду на повільніше зростання доходів у найближчій перспективі, але наголосив, що це необхідно для того, щоб проєкти зі штучного інтелекту приносили реальну користь безпечно та з дотриманням усіх вимог. Його коментарі заслуговують на увагу частково тому, що вони походять із самої консалтингової галузі, а не від регуляторних органів чи постачальників послуг з кібербезпеки, і ставлять питання про те, чи буде галузь виступати в ролі продавців трансформації, чи відповідальних «воротарів», готових уповільнити впровадження, коли клієнти до цього не готові». *(Sofiah Nichole Salivio. Consultancies urged to slow AI push amid cyber risk // TechDay (<https://securitybrief.co.uk/story/consultancies-urged-to-slow-ai-push-amid-cyber-risk>). 11.05.2026).*

«Штучний інтелект кардинально змінив ландшафт кібербезпеки, але спочатку перевага від цих змін була на боці зловмисників. Згідно з доповідями компаній Anthropic та Osterman Research, кіберзлочинці все частіше використовують великі мовні моделі та агентів штучного інтелекту для автоматизації до 80% своїх атак, що дозволяє навіть некваліфікованим особам здійснювати складні операції з вимагання даних, використовувати програми-вимагачі та створювати шкідливе програмне забезпечення без написання коду. Натомість захисники, як і раніше, стикаються з серйозними перешкодами через хронічний брак ресурсів та величезний обсяг сповіщень. Команди Центрів операцій з безпеки (SOC) наразі витрачають приблизно 75% свого часу на ручні, реактивні завдання, такі як сортування та розслідування сповіщень — процес, який може займати понад 15 хвилин на одне сповіщення під час зіставлення даних із різних джерел. Цей дисбаланс призвів до зростання «боргу безпеки» та небезпечного «часу перебування» зловмисників у системі...

Однак із появою штучного інтелекту, здатного імітувати людське мислення та експертні знання в галузі кібербезпеки, відбувається кардинальна зміна. Такі технології, як Dropzone AI, тепер здатні автоматизувати сортування, оцінку та дедуплікацію сповіщень, отримуючи дані в режимі реального часу з усього стеку безпеки організації. Функціонуючи як «армія аналітиків першого рівня», що працює цілодобово, ці агенти можуть проводити попереднє розслідування кожного сповіщення, відфільтровуючи помилкові спрацьовування та передаючи лише справжні загрози людським аналітикам. Хоча людське судження залишається необхідним для стратегічної співпраці та прийняття рішень на високому рівні, агенти ШІ полегшують тягар повторюваної рутинної роботи. Ця еволюція перетворює виявлення загроз із трудомісткого ручного процесу на масштабовану автоматизовану систему, роблячи захист на основі ШІ критичною необхідністю, а не розкішшю в сучасній боротьбі за цифрову безпеку». *(Edward Wu. AI Agents Are the Next Paradigm Shift in Cyber Defense // GeekWire, LLC (<https://www.geekwire.com/sponsor-post/ai-agents-are-the-next-paradigm-shift-in-cyber-defense/>). 11.05.2026).*

«Пентагон досягає значного підвищення ефективності завдяки впровадженню нових інструментів агентного штучного інтелекту, які дозволяють стиснути тижні роботи до лічених годин, хоча ці самі технології стрімко змінюють загальний ландшафт кібербезпеки. Заступник міністра оборони Еміль Майкл підкреслив успіх платформи GenAI.mil від міністерства — яка тепер використовує Gemini від Google поряд з рішеннями інших постачальників, щоб уникнути надмірної залежності — в автоматизації рутинних завдань. У рамках агресивних заходів із захисту критичної інфраструктури Пентагон навіть тестує «Mythos» — модель виявлення вразливостей від компанії Anthropic, незважаючи на те, що ця компанія офіційно визнана загрозою національній безпеці. Майкл виправдав цю фазу оцінки, наголосивши на нагальній потребі виявляти та усувати вразливості як у державних мережах, так і в об'єктах

приватного сектору, таких як лікарні, до того, як супротивники зможуть ними скористатися...

Однак, оскільки автоматичне виправлення вбудованих в ІІІ вразливостей стає галузевим стандартом, експерти з кібербезпеки застерігають, що цього буде недостатньо для запобігання майбутнім загрозам. Джексон Рід із компанії Barding Defense попереджає, що агентський ІІІ незабаром надасть звичайним кіберзлочинцям можливості діяти нарівні з витонченими суб'єктами, що мають державну підтримку. Замість того, щоб зосереджуватися виключно на швидких виплатах викупу за програмне забезпечення-вимагач, злочинці використовуватимуть ІІІ для реалізації складних тактик, таких як побічне переміщення в мережі, довгострокове шпигунство та промисловий інсайдерський трейдинг. Оскільки сучасні моделі ІІІ часто не в змозі виявити ці просунуті, приховані маневри, Рід наразі співпрацює з пов'язаною з військовими структурами компанією Breakpoint Labs над розробкою нової платформи ІІІ, спеціально призначеної для виявлення та протидії безпрецедентним кібератакам, що здійснюються за допомогою агентних інструментів». (*Patrick Tucker. Pentagon leaders love agentic AI. But it's giving cyber criminals nation-state-like powers // Government Media Executive Group LLC* (<https://www.defenseone.com/threats/2026/05/pentagon-leaders-love-agentic-ai-its-giving-cyber-criminals-nation-state-powers/413379/>). 06.05.2026).

«Штучний інтелект кардинально змінив ландшафт загроз у сфері кібербезпеки, ставши одночасно важливим засобом захисту та потужною зброєю в руках зловмисників. У рамках рубрики «Solution Spotlight» видання Solutions Review експерти з компаній DayBlink Consulting та Radware розповіли, як інструменти, що раніше вимагали спеціалізованих знань, злочинних мереж та спеціально побудованої інфраструктури, тепер є загальнодоступними на таких платформах, як GitHub, пропонуються у вигляді недорогих сервісів за передплатою та здатні генерувати сотні тисяч запитів-атак на секунду з одного мобільного пристрою. Одним із прикладів, наведених дослідниками, є фреймворк на базі GitHub, що поєднує 56 методів атак в єдиний скрипт, який виконує одночасні багатовекторні атаки, містить готові обхідні шляхи для поширених засобів захисту та оновлюється у міру адаптації постачальників послуг безпеки, фактично функціонуючи як жива наступальна платформа. Незважаючи на широке визнання того, що ІІІ є необхідним для безпеки, лише близько чверті організацій мають налагоджене ефективне управління ІІІ, що залишає значну прогалину, яку зловмисники активно використовують...

DDoS-атаки демонструють, як штучний інтелект прискорює зростання масштабів та інтенсивності існуючих загроз. Нинішні пікові атаки вже досягають 7,3 терабайта на секунду, і експерти очікують, що рекорди будуть побиватися кілька разів на рік, оскільки агенти ІІІ починають автономно координувати інфраструктуру атак та адаптуватися до засобів захисту в режимі реального часу. Для підприємств, які стикаються з мільйонними витратами на прості щохвилини, ані відключення від мережі, ані грубе обмеження швидкості не є прийнятними, що

робить моделювання поведінки — розуміння того, як виглядає легітимний трафік, щоб можна було точно ідентифікувати аномальні запити — єдиним практичним шляхом. Дві конкретні категорії загроз заслуговують на особливу увагу: інструменти для розпізнавання CAPTCHA на базі штучного інтелекту, які досягають 100% точності швидше, ніж будь-яка людина, і доступні як недорогі послуги за передплатою; та боти для обходу OTP, які використовують технологію голосового штучного інтелекту, щоб дзвонити жертвам, видавати себе за банківські системи безпеки та обманом змушувати їх продиктувати коди автентифікації, обходячи двофакторну автентифікацію за допомогою надзвичайно переконливого соціального інжинірингу...

Для протидії цим загрозам компанія Radware пропонує захисний підхід, що базується на чотирьох основних принципах: впровадження засобів захисту на основі штучного інтелекту, здатних протистояти можливостям зловмисників; створення поведінкових моделей на основі стабільних патернів легітимного трафіку для виявлення нових загроз; інтеграція платформ безпеки на рівні мережі, додатків та захисту від DDoS-атак для усунення прогалин, які залишають ізольовані системи захисту; а також забезпечення єдиного захисту в локальних середовищах, приватних та публічних хмарних середовищах, оскільки зловмисники обиратимуть за ціль найменш захищені точки. Експерти також наголосили, що будь-яка оборонна архітектура, яка спирається на інструменти, що не змінювалися протягом трьох років, ймовірно, є недостатньою для сучасного середовища, і що плани реагування на інциденти повинні бути підготовлені до того, як відбудеться атака, а не імпровізовані під час неї». (*William Jepma. AI Is Now Both the Weapon and the Shield in Cybersecurity // Solutions Review* (<https://solutionsreview.com/endpoint-security/ai-is-now-both-the-weapon-and-the-shield-in-cybersecurity/>). 11.05.2026).

«Хоча цифрова економіка залишається важливим двигуном економічного зростання, останні досягнення в галузі штучного інтелекту привели до появи системних вразливостей, які загрожують цілісності всього цифрового середовища. Традиційні заходи кібербезпеки, що базуються на криптографічних «замках» для захисту систем, стають дедалі менш ефективними, оскільки ШІ обходить ці засоби захисту, виявляючи альтернативні точки входу, що робить стандартні засоби захисту недостатніми. Розробка «Claude Mythos» від Anthropic — набору великих мовних моделей, здатних виявляти слабкі місця в безпеці та пропонувати способи їх усунення — наочно демонструє цю нову парадигму. Хоча Anthropic діяла відповідально, поділившись цими можливостями лише з основними технологічними партнерами, а не з широкою громадськістю, неминучість відтворення такої технології зловмисниками означає, що критична інфраструктура, від фінансових послуг до охорони здоров'я, стикається з безпрецедентними ризиками...

Отже, покладатися лише на регулювання не допоможе вирішити цю проблему; натомість галузь потребує кардинальних змін у підході до розробки програмного забезпечення. Надалі розробники повинні надавати пріоритет створенню

програмного забезпечення, «стійкого до ШІ», та впроваджувати численні незалежні рівні кіберзахисту для мінімізації вразливостей. Цей перехід, який фактично вимагає нового структурного підходу до сектору кібербезпеки, є надзвичайно важливим для того, щоб випереджати загрози, пов'язані з ШІ, та забезпечити довгострокову стабільність глобальної цифрової архітектури. Проактивне перепроектування, а не реактивне виправлення, є єдиним життєздатним шляхом уперед у цій новій технологічній реальності». (*Sheldon H. Jacobson. Opinion: Modern Cybersecurity Systems Unprepared for AI // e.Republic LLC (<https://www.govtech.com/opinion/opinion-modern-cybersecurity-systems-unprepared-for-ai>). 11.05.2026*).

«У звіті Всесвітнього економічного форуму (WEF) «Штучний інтелект і кібербезпека: розширення можливостей захисників», опублікованому в травні, який було підготовлено спільно з KPMG на основі даних, наданих понад 84 організаціями з 15 галузей, зроблено висновок, що штучний інтелект стрімко трансформує сферу кібербезпеки, посилюючи захист і водночас прискорюючи розвиток загроз. Згідно з результатами дослідження, 94% керівників у сфері кібербезпеки вважають штучний інтелект найвпливовішим фактором у цій галузі, а 77% організацій уже використовують його у своїх кіберопераціях. У звіті описується гонка на швидкість, в якій ШІ допомагає захисникам покращити виявлення загроз та реагування на них, але також дає змогу злочинцям автоматизувати обман, створювати шкідливе програмне забезпечення та масштабувати атаки швидше, ніж це можуть впоратися традиційні засоби контролю... Організації, які широко використовують штучний інтелект, можуть скоротити витрати, пов'язані з порушеннями безпеки, на суму до 1,9 млн доларів та зменшити тривалість циклу реагування на інциденти приблизно на 80 днів. Серед прикладів — компанія Accenture, яка скоротила час аналізу понад 100 000 веб-сайтів, що мають вихід в Інтернет, з 15 хвилин до менше ніж однієї хвилини, платформа IBM ATOM, яка автоматизує понад 850 годин роботи аналітиків на місяць і скорочує час розслідування на 37%, та KPMG, яка повідомляє про 25-відсоткове підвищення ефективності аналізу загроз. Підкреслюючи ці переваги, у звіті наголошується, що вплив штучного інтелекту залежить від ефективного управління, чітких стратегій впровадження та людського нагляду, і стверджується, що він повинен доповнювати, а не замінювати людський досвід. У рамках ініціативи WEF «Cyber Frontiers: AI & Cyber», започаткованої у 2024 році, дослідження закликає лідерів бізнесу та уряду розглядати ШІ як основний засіб безпеки та інвестувати у навички та системи, необхідні для роботи зі швидкістю машин». (*Rejoice Okechukwu. AI strengthens organisations' cybersecurity, says WEF report // Peoples Gazette™ Limited (<https://gazettengr.com/ai-strengthens-organisations-cybersecurity-says-wef-report/>). 04.05.2026*).

«Всебічне дослідження, проведене вченими з університетів Кембриджа, Единбурга та Стратклайда, поставило під сумнів поширену думку про те, що

генеративна ШІ відкриває нову еру «надпотужних» хакерів. Аналізуючи 97,895 тем на форумах, присвячених кіберзлочинності, дослідження під назвою «Stand-Alone Complex or Vibercrime?» (Самостійний комплекс чи Vibercrime?) показує, що фактичне використання ШІ для здійснення складних хакерських атак залишається надзвичайно низьким. Натомість переважна більшість злочинної діяльності, що базується на ШІ, зосереджена на «нижньому рівні харчового ланцюга» і спрямована на малоприбуткові, але масові шахрайські схеми, такі як SEO-спам, романтичні афери та масове створення зображень-діпфейків без згоди моделей...

Дослідники з'ясували, що значна частина ажіотажу навколо інструментів «темного ШІ», таких як WormGPT і FraudGPT, була зумовлена скоріше маркетинговими ходами, а не технічними можливостями. Багато з цих сервісів були лише необмеженими версіями загальнодоступних моделей, які працювали неефективно або швидко втрачали актуальність через дію ефективних заходів безпеки. Хоча «джейлбрейк» загальноприйнятих моделей є частою темою на цих форумах, у дослідженні зазначається, що такі експлойти стає дедалі складніше підтримувати, і вони часто витримують лише кілька днів, перш ніж їх виправляють. Крім того, дані показали, що навіть у підпільній спільноті існує значний скептицизм щодо «веб-хакінгу». Багато кіберзлочинців висловили занепокоєння, що надмірна залежність від кодування за допомогою ШІ призводить до створення незахищеного програмного забезпечення та швидкого погіршення їхніх власних технічних навичок...

Зрештою, дослідження показує, що найвагоміший вплив штучного інтелекту на екосистему кіберзлочинності полягає не в самій технології, а в її впливі на ринок праці. Дослідники застерігають, що різке зростання занепокоєння щодо скорочень та економічного спаду в легальному технологічному секторі може змусити висококваліфікованих розробників шукати роботу в підпільних спільнотах. Саме цей потенційний приплив професійних кадрів у сферу кіберзлочинності, а не автоматизація хакерських інструментів, є найсерйознішою довгостроковою загрозою, виявленою в ході дослідження». *(Jose Antonio Lanz. Cybercrime Might Be the One Job AI Isn't Taking, Study Suggests // Decrypt Media, Inc. (<https://decrypt.co/366855/cybercrime-hacking-ai-study>). 05.05.2026).*

«Популярність інструментів кодування на основі «віб», які дозволяють користувачам без технічних знань створювати веб-додатки за допомогою штучного інтелекту, стрімко зростає, проте компанія з кібербезпеки RedAccess попереджає, що багато таких додатків можуть бути вразливими. У дослідженні, опублікованому в журналі Wired, команда під керівництвом Дора Цві проаналізувала близько 5 000 веб-додатків, створених за допомогою Lovable, Replit, Base44 та Netlify, і виявила, що багато з них практично не мали аутентифікації чи захисту, іноді дозволяючи будь-кому, хто мав правильний URL-адресу, отримати доступ до додатка та його даних, або вимагаючи лише простих дій, таких як введення будь-якої адреси електронної пошти. RedAccess заявила, що приблизно 40% додатків розкривали конфіденційну інформацію, наводячи такі приклади, як графіки роботи персоналу лікарень, що містять особисті дані лікарів, презентації

стратегії виходу компанії на ринок, а також дані про продажі та фінансові звіти різних фірм... Дослідники зазначили, що демократизація розробки додатків призводить до того, що багатьом розробникам бракує знань у сфері безпеки, і ці інструменти можуть не забезпечувати безпечні налаштування за замовчуванням, якщо їх спеціально не налаштувати. Декілька компаній заперечили або поставили під сумнів ці висновки: представник Wix/Base44 заявив, що RedAccess не надав URL-адреси, необхідні для розслідування, і що деякі з нібито вразливих додатків були навмисно налаштовані як загальнодоступні або, судячи з усього, були тестовими сайтами; у свою чергу, компанія Lovable також зазначила, що у звіті бракує технічних деталей для перевірки цих тверджень, але додала, що вивчає це питання». (*Will McCurdy. Vibe Coding Is Causing 'Thousands' of Data Security Vulnerabilities // Ziff Davis, LLC. (<https://uk.pcmag.com/ai/164858/vibe-coding-is-causing-thousands-of-data-security-vulnerabilities-says>). 09.05.2026*).

«Google готується публічно розповісти про свої давно обговорювані плани щодо об'єднання Android та ChromeOS у нову операційну систему для ноутбуків, яка, за повідомленнями, має кодову назву «Aluminum» і на брифінгах позиціонується не стільки як традиційна ОС, скільки як «інтелектуальна система», побудована на базі Gemini. Нова концепція «Googlebook» працює на Android і представляє гібридний інтерфейс, що поєднує традиційні елементи ноутбука з елементами, характерними для телефонів, включаючи верхню панель стану та нижню панель навігації з помітною точкою входу в пошук Google/Gemini, а додатки постачаються переважно через Google Play Store... Google позиціонує глибоку інтеграцію телефону та ноутбука як ключову функцію: окрім синхронізації сповіщень, користувачі можуть відкривати додатки на різних пристроях та переглядати вміст пам'яті підключеного телефону з ноутбука, а деякі додатки можна «транслявати» з телефону на екран Googlebook, хоча деталі та окремі випадки, такі як використання в автономному режимі, залишаються незрозумілими. Хоча очікується повна підтримка браузера Chrome, значна частина програмного забезпечення, здається, зосереджена на додатках Android, адаптованих для більших екранів, а головною відмінністю платформи є повсюдна інтеграція Gemini, включаючи редагування та створення фотографій за допомогою штучного інтелекту, організацію інформації між додатками, створення віджетів та поведінку асистента, що запускається за контекстом і може активуватися рухом курсора... На момент запуску Google не планує самостійно випускати ноутбуки, а натомість співпрацюватиме з провідними виробниками, такими як HP, Dell, Asus, Acer та Lenovo; вихід пристроїв очікується «цієї осені», хоча ціни та технічні характеристики поки що не розкриваються. Водночас Google натякає на більш преміальне позиціонування, ніж у типових бюджетних Chromebook, та демонструє елемент дизайну під назвою «Glowbar». Кажуть, що ChromeOS і Chromebook продовжуватимуть існувати, включаючи підтримку деяких моделей до 10 років, але незрозуміло, чи будуть існуючі Chromebook оновлені до нової платформи, а ширше питання полягає в тому, чи сприймуть споживачі ноутбуки, орієнтовані на штучний інтелект, які, як стверджують

критики, пропонують обмежені переваги порівняно з традиційними системами Windows, macOS або Linux, потенційно зменшуючи гнучкість». (*Michael Crider. Googlebooks aren't just Android laptops. They're a Trojan horse for Gemini // FoundryCo, Inc. (<https://www.pcworld.com/article/3136774/googlebooks-arent-just-android-laptops-theyre-a-trojan-horse-for-gemini.html>). 12.05.2026*).

«Рішення компанії Anthropic від 7 квітня призупинити публічний випуск своєї моделі Claude Mythos Preview, посиляючись на її надзвичайно потужні можливості в галузі комп'ютерної безпеки, посилило дискусію щодо того, наскільки швидко «передовий» ШІ може бути використаний як зброя для кібератак, а також для оборони. В рамках проекту Glasswing модель Mythos була надана провідним технологічним та фінансовим установам США, щоб вони могли виявляти та усувати вразливості «нульового дня», і компанія Anthropic заявляє, що модель вже виявила тисячі вразливостей високого рівня серйозності в основних операційних системах та браузерях... Проте експерти застерігають, що це звужує вікно можливостей для країн і секторів, які все ще використовують застарілі системи — зокрема, для критичної національної інфраструктури Великої Британії, де урядові перевірки виявляють значну частку застарілих технологій у центральних урядових відомствах, фондах Національної служби охорони здоров'я (NHS) та поліцейських підрозділах — оскільки навіть великі організації тривалий час не виправляють багато виявлених вразливостей. Аналітики також очікують, що аналогічні можливості «класу Mythos» з'являться у інших розробників, зокрема в Китаї, що викликає занепокоєння щодо того, що хакерські угруповання, пов'язані з державою, отримають швидші можливості виявлення та використання вразливостей «нульового дня», а також щодо ширшої залежності від компаній, що працюють у сфері штучного інтелекту, які змушені самостійно контролювати свої найнебезпечніші моделі в умовах конкурентного тиску...

У Великій Британії підприємства та банки досі ведуть переговори з компанією Anthropic щодо доступу до її ресурсів, тоді як деякі організації шукають способи відтворити подібні можливості тестування за допомогою постачальників послуг з кібербезпеки, щоб перевірити ефективність захисних заходів та виправлень до того, як більш досконалі моделі виявлять невідомі вразливості. Окремо фахівці з безпеки застерігають, що саме стрімке впровадження систем штучного інтелекту в компаніях може створити нові шляхи для атак — особливо якщо чат-боти чи агенти підключені до конфіденційних внутрішніх систем — відкриваючи можливості для соціальної інженерії або витоку даних... Наразі заходи уряду Великої Британії включають публічні рекомендації, в яких організаціям настійно рекомендується відпрацьовувати алгоритми реагування на критичні інциденти, запрошення до технологічних компаній щодо спільної розробки штучного інтелекту в рамках національних зусиль з кіберзахисту, а також прогрес у розробці законопроекту про кібербезпеку та стійкість, який покладатиме на постачальників керованих послуг більш суворі регуляторні обов'язки та вимоги щодо звітності, хоча експерти наголошують, що саме наявність ресурсів для забезпечення дотримання законодавства визначатиме, чи матиме воно реальний вплив.

Спостерігачі відзначають, що відносини Великої Британії з компаніями, що займаються штучним інтелектом, та незалежна оцінка Mythos, проведена Інститутом безпеки штучного інтелекту, є позитивними, але загальна картина полягає в тому, що це технологія подвійного призначення, яка може або зміцнити розробку за принципом «безпека за рахунок дизайну», або прискорити наступальні операції — залежно від того, хто першим отримає та застосує ці можливості». **(Noah Vickers. Mythos And AI Hacking: A High-Stakes Cybersecurity Arms Race // Political Holdings Limited (<https://www.politicshome.com/news/article/mythos-ai-hacking-highstakes-cybersecurity-arms-race>). 22.05.2026).**

«Компанія EY вилучила з веб-сайту звіт про кібербезпеку, опублікований її канадським підрозділом, після того як дослідники виявили численні вигадані посилання, неточні статистичні дані та ознаки контенту, створеного штучним інтелектом, що викликало занепокоєння щодо все ширшого використання генеративного штучного інтелекту у сфері професійних послуг. Звіт під назвою «Точки атаки: виявлення кіберзагроз та шахрайства в системах лояльності» був видалений з веб-сайту EY Canada після того, як дослідницька група GPTZero проаналізувала його та виявила, що понад 70 відсотків цитат були сфабрикованими, недійсними або неправильно посилалися на джерела. За словами дослідників, документ містив типові помилки великих мовних моделей, включаючи фальшиві статистичні дані, неправильні посилання та внутрішні суперечності. Посилання, які нібито ведуть до таких джерел, як Forbes, McKinsey, Gartner, TechCrunch та Wired, або вели на неіснуючі веб-сторінки, або не підтверджували твердження, викладені у звіті...»

Серед найпомітніших проблем було неодноразове використання оцінки у 200 мільярдів доларів як для глобального ринку бонусних балів, так і для вартості невикористаних бонусних балів без надання пояснень. GPTZero виявило, що одна з цих цифр була приписана неіснуючому звіту McKinsey, хоча, ймовірно, походила з маловідомого блогу про фінтех. Дослідники попередили, що неточні звіти, підготовлені авторитетними компаніями, можуть ввести в оману майбутні дослідження та «отруїти джерело», поширюючи недостовірну інформацію через платформи з великою аудиторією...

Компанія EY заявила, що серйозно ставиться до точності своїх публікацій, видалила звіт та розпочала перевірку процедури його затвердження, наголосивши, що цей звіт не мав жодного стосунку до роботи з клієнтами. Цей інцидент відображає більш широку тенденцію до помилок, пов'язаних з ШІ, у сфері професійних послуг, слідом за подібними випадками, що стосувалися Deloitte та юридичної фірми Sullivan & Cromwell, яким обом довелося вирішувати питання щодо вигаданих або неправильних посилань у професійних документах. Незважаючи на ці суперечки, великі консалтингові фірми продовжують розширювати використання технологій ШІ, причому EY повідомляє про значне зростання доходів, пов'язаних із ШІ, та тисячі співробітників, які працюють над проектами, зосередженими на ШІ». **(Jonathan Easton. EY withdraws AI-generated cybersecurity report after fabricated citations found // National Technology News**

(NTN)

(https://nationaltechnology.co.uk/EY_Withdraws_AI_Generated_Cybersecurity_Report.php). 21.05.2026).

«Штучний інтелект стрімко змінює галузь кібербезпеки, але експерти вважають, що він, швидше за все, трансформує традиційні компанії з кібербезпеки, а не повністю їх витіснить. Системи безпеки на базі штучного інтелекту стали надзвичайно ефективними у виявленні підозрілої активності, ідентифікації шкідливого програмного забезпечення та реагуванні на загрози в режимі реального часу завдяки аналізу величезних обсягів даних набагато швидше, ніж традиційні інструменти, що покладаються на заздалегідь визначені правила та людський моніторинг. У міру того, як організації все частіше впроваджують платформи на базі штучного інтелекту для автоматизації таких завдань, як виявлення загроз, оцінка вразливостей, фільтрування спаму та реагування на інциденти, з'явилися побоювання, що традиційні постачальники послуг з кібербезпеки можуть втратити свою актуальність...

Однак ситуація у сфері кібербезпеки стає дедалі складнішою, а не простішою, оскільки кіберзлочинці також використовують штучний інтелект для розробки витончених атак, зокрема фішингових кампаній, створених за допомогою ШІ, автоматизованих хакерських інструментів та адаптивного шкідливого програмного забезпечення, здатного обходити традиційні засоби захисту. Це зумовлює постійну потребу у фахівцях з кібербезпеки, які можуть оцінювати ризики, проводити розслідування, розробляти стратегії захисту та реагувати на цілеспрямовані атаки, з якими системи штучного інтелекту не можуть впоратися самостійно. Технології ШІ також мають свої обмеження, зокрема помилкові спрацьовування, неповні дані та нездатність надійно розпізнавати унікальні або мінливі схеми атак без контролю з боку людини...

Як наслідок, компанії, що займаються кібербезпекою, все частіше інтегрують штучний інтелект та машинне навчання у свої послуги, щоб залишатися конкурентоспроможними. Фірми, які не зможуть пристосуватися, можуть зіткнутися з труднощами, тоді як ті, що успішно поєднують передові інструменти штучного інтелекту з людським досвідом, як очікується, будуть процвітати. Аналітики галузі прогнозують, що майбутнє кібербезпеки залежатиме від співпраці між інтелектуальними системами та кваліфікованими фахівцями, причому ШІ буде виконувати повторювані завдання, що вимагають обробки великих обсягів даних, а люди зосередяться на стратегічних рішеннях, етиці, дотриманні нормативних вимог та аналізі складних загроз. ШІ не знищує компанії, що займаються кібербезпекою, а навпаки — прискорює трансформацію галузі та спонукає компанії до інновацій і створення більш досконалих засобів захисту в дедалі складнішому цифровому середовищі». (Naveen Goud. *Will AI driven Security Applications wipe businesses of Cybersecurity firms* // *Cybersecurity Insiders* (<https://www.cybersecurity-insiders.com/will-ai-driven-security-applications-wipe-businesses-of-cybersecurity-firms/>). 25.05.2026).

«Передові моделі штучного інтелекту з кіберпотенціалом, такі як Mythos від Anthropic та GPT-5.5-Cyber від OpenAI, становлять важливу точку перелому для корпоративної безпеки, оскільки вони здатні на більше, ніж традиційні сканери: вони можуть аналізувати багатоетапні шляхи атак, оцінювати ймовірність їх реалізації та генерувати робочі процеси з безпеки, що підвищує як оборонний потенціал, так і ризик атак, збільшуючи швидкість зловмисників та знижуючи рівень кваліфікації, необхідний для здійснення складних вторгнень. Zscaler повідомляє, що ключовим питанням для організацій є те, чи зможуть захисники освоїти ці моделі швидше, ніж супротивники, і описує внутрішню систему оцінки, побудовану навколо трьох тестових наборів, що віддзеркалюють реальні сценарії: тестування «чорного ящика» за принципом «думай як зловмисник» без внутрішніх знань, перевірка артефактів та репозиторіїв коду й бінарних файлів для виявлення проблем до їх використання в атаках, а також тестування «сірого/білого ящика», яке використовує частковий або повний системний контекст, такий як моделі загроз та архітектура, для отримання найбільш практичних результатів. Кожен запуск відбувався за структурованим алгоритмом: від картування поверхні атаки до активного тестування, динамічної валідації, дедуплікації, сортування, реєстрації, виправлення та повторної валідації, щоб виміряти не лише обсяг виявлених проблем, а й те, які з них витримали валідацію та наскільки ефективними були шляхи їх усунення...

Тестування, проведене компанією Zscaler, показало, що головною перевагою цих моделей є глибина міркування — особливо ітеративний аналіз та ланцюгове виявлення вразливостей — завдяки чому вони об'єднують слабкі місця з низьким рівнем серйозності, помилки в налаштуваннях та стани привілеїв у правдоподібні багатоетапні шляхи компрометації. Це часто дозволяє отримати наочні докази концептуальної експлуатації, покращити визначення пріоритетів, пришвидшити підтримку розслідувань, вдосконалити методику виявлення та надати рекомендації щодо усунення вразливостей. За результатами порівняльних тестів, Zscaler стверджує, що передові моделі виявили приблизно вдвічі більше знахідок високого рівня серйозності за приблизно половину часу порівняно зі старими інструментами та пентестуванням, з вищим співвідношенням сигнал/шум після валідації. Компанія застерігає, що контекст є важливим, але складним: надання хорошого архітектурного контексту покращує точність, тоді як використання в моделі попередніх шаблонів проблем може спричинити закріплення та зменшити виявлення нових проблем; навпаки, занадто мало контексту може завищити рівень серйозності через неправильне тлумачення залежностей. Найефективніше використання було досягнуто завдяки керованим експертами, орієнтованим на цілі робочим процесам, вбудованим у повторювані механізми, а не широким, нецільовим підказкам, причому координація та управління моделлю виступали як справжній мультиплікатор сили...

Для підготовки компанія Zscaler рекомендує зменшити доступну площу атаки шляхом розміщення додатків за системою доступу «Zero Trust», покращити видимість активів та вразливостей (включно з активами III), використовувати обманні методи для виявлення та локалізації зловмисників, що використовують

багатошляхові атаки, послідовно застосовувати сегментацію «Zero Trust» для обмеження горизонтального переміщення, розглядати виробничі системи ІІІ як площини атаки з використанням методів «червоної команди» та захисних механізмів проти введення команд через консоль та дрейфу, а також надавати пріоритет усуненню вразливостей за допомогою управління вразливостями на основі ІІІ. Загалом, передова ІІІ переходить від ролі помічника до оперативної можливості, і що організації отримають перевагу, поєднуючи ці моделі з потужною архітектурою, надійним контекстом та дисциплінованим виконанням, щоб виявляти та усувати вразливості, які можна експлуатувати, швидше, ніж зловмисники зможуть ними скористатися». (*Cyber defense in the era of frontier AI: Insights from Mythos and GPT 5.5 Cyber // FoundryCo, Inc.* (<https://www.cio.com/article/4177927/cyber-defense-in-the-era-of-frontier-ai-insights-from-mythos-and-gpt-5-5-cyber.html>). 27.05.2026).

«Двадцять років тому галузь кібербезпеки зосереджувалася переважно на антивірусному програмному забезпеченні та брандмауерах, і тоді ще майже не усвідомлювали, що існує величезна кількість підключених пристроїв, якими можна маніпулювати без використання традиційних облікових даних. Хоча протокол HTTPS було запроваджено ще в 1990-х роках, широке застосування шифрування даних під час передачі все ще не було поширеним. Сьогодні кібербезпека перетворилася на стратегічний пріоритет для організацій, а керівники вищого рівня та ради директорів усвідомлюють, що безпека та безперервність бізнесу є нерозривними поняттями. Хакерів минулого замінили лідери галузі, які зараз керують командами з кібербезпеки, що відображає значний зсув, спричинений технологічним прогресом.

Розвиток технологій — зокрема хмарних обчислень, мобільних пристроїв, Інтернету речей (IoT) та штучного інтелекту — трансформував інфраструктуру та площини атаки. На початку 2000-х років відбувся підйом хмарних сервісів, таких як Salesforce та Amazon Web Services, які обіцяли операційну ефективність та економію коштів. Мобільні технології також швидко розвивалися: смартфони, такі як BlackBerry, iPhone та пристрої на базі Android, уможливили дистанційну роботу та збільшили обсяг даних, що виходять за межі корпоративного контролю. Поява Інтернету речей ще більше розширила площину атак, зробивши захист ідентичності та даних важливішим, ніж будь-коли...

Ця технологічна еволюція стимулювала постійні інновації в галузі кібербезпеки: стартапи бралися за вирішення нових завдань, а існуючі компанії інтегрували функції безпеки у свої платформи. Аналітика загроз стала більш досконалою, перейшовши від неформального обміну інформацією до комплексних, комерційних платформ, таких як Recorded Future. Незважаючи на ці зміни, основні принципи залишилися незмінними: захист інфраструктури, оновлення систем та навчання користувачів безпечним методам роботи. Водночас інструменти безпеки також перейшли від апаратних пристроїв до програмних рішень, що відображає загальну тенденцію до цифрової трансформації. За прогнозами, глобальні витрати на кібербезпеку у 2026 році сягнуть майже 240 млрд доларів, причому приблизно

половина цих коштів буде виділена на програмне забезпечення для безпеки, що є значним зростанням порівняно з лише 8,7 млрд доларів у 2006 році...

Залежність галузі від програмного забезпечення ще більше зросла під впливом переходу до хмарних середовищ, де апаратне забезпечення часто віртуалізується. Сучасні платформи безпеки зараз роблять акцент на інтегрованих, платформоорієнтованих підходах, таких як SASE, «нульова довіра» та розширене виявлення та реагування (XDR). Цей зсув зумовлений постійним переходом від локальних систем до хмарних архітектур, причому хмарні засоби безпеки, такі як управління станом системи та брокери доступу, стають центральними елементами стратегій захисту.

Загалом, хоча технології та інструменти зазнали кардинальних змін, основні принципи кібербезпеки — захист систем, оновлення засобів захисту та навчання користувачів — залишаються незмінними. Галузь продовжує стрімко розвиватися, а штучний інтелект та інші нові технології обіцяють сформувати наступну хвилю інновацій у сфері кібербезпеки». (*Fahmida Y. Rashid. Cybersecurity Evolution: How We Went From Perimeter Defense to AI-Native Security // TechTarget, Inc. (<https://www.darkreading.com/cybersecurity-operations/cybersecurity-evolution-perimeter-defense-to-ai-native-security>). 27.05.2026*).

Штучний інтелект, як інструмент боротьби із кіберзлочинністю

«Впровадження сучасних інструментів, таких як CLI-Anything, кардинально змінило принцип роботи агентів штучного інтелекту, що займаються програмуванням, але водночас виявило нову серйозну загрозу кібербезпеці, відому як «отруєння на рівні агента». Хоча ці інструменти безперешкодно перетворюють вихідний код на структуровані інтерфейси командного рядка для агентів ШІ, вони покладаються на новий «рівень інтеграції агентів», що складається з файлів конфігурації та наборів інструкцій природною мовою, таких як файли SKILL.md. Традиційна інфраструктура безпеки, включаючи статичне тестування безпеки додатків (SAST) та аналіз складу програмного забезпечення (SCA), повністю ігнорує цей рівень. Оскільки ці застарілі інструменти були розроблені для сканування синтаксису коду та версій залежностей, а не семантичного змісту текстових інструкцій, зловмисні директиви, вбудовані в визначення навичок ШІ, легко обходять існуючі протоколи безпеки...

Зловмисники активно використовують цю структурну вразливість, приховуючи шкідливі операційні вказівки у, на перший погляд, нешкідливій документації, прикладах коду або інструкціях з налаштування. Коли розробник підключає агент штучного інтелекту до скомпрометованого репозиторію, агент завантажує заражене визначення набору навичок і виконує приховані команди. Оскільки агент працює, використовуючи легітимні облікові дані розробника на плоскій площині авторизації, зловмисні дії — такі як витік даних або збір облікових даних — виглядають як авторизовані виклики API, повністю обходячи стандартний моніторинг виявлення та реагування на кінцеві точки. Бар'єр для виконання цих атак є небезпечно низьким, оскільки зловмисні навички не

викликають стандартних сповіщень про вразливість і ніколи не з'являються у специфікаціях програмного забезпечення...

Ця загроза вже активно реалізується у виробничих середовищах. Нещодавні аудити та дослідження, такі як звіт Snyk «ToxicSkills» та кампанія ClawHavoc, виявили тисячі шкідливих AI-скілів, які проникають на ринки відкритого програмного забезпечення з тривожно високим відсотком успіху. Зловмисники успішно використовують такі техніки, як Document-Driven Implicit Payload Execution, щоб уникнути виявлення, що призводить до несанкціонованої інсталяції агентів та компрометації залежностей. Оскільки сучасна екосистема безпеки розвивається повільніше, ніж зловмисники, експерти попереджають, що ця вразливість нагадує ранні, вкрай незахищені часи безпеки контейнерів.

Щоб протидіяти цьому «сліпому пляму», яке стрімко розширюється, керівники служб безпеки повинні негайно оновити свої стратегії захисту з урахуванням рівня інтеграції агентів. Організаціям настійно рекомендується провести інвентаризацію всіх інструментів-посередників для III-агентів у своїх середовищах та розглядати джерела III-навичок як ненадійні виконувані файли, що вимагають суворого аудиту та внесення до списку дозволених ресурсів. Крім того, команди повинні обмежити привілеї виконання агентів III, впровадити надійну спостережуваність під час виконання та розгорнути нещодавно розроблені спеціалізовані сканери, такі як Skill Scanner від Cisco або mcp-scan від Snyk, які спеціально призначені для аналізу поведінкових намірів файлів інструкцій агентів, перш ніж вони завдадуть шкоди всій системі». *(Louis Columbus. One command turns any open-source repo into an AI agent backdoor. OpenClaw proved no supply-chain scanner has a detection category for it // VentureBeat (<https://venturebeat.com/security/one-command-open-source-repo-ai-agent-backdoor-openclaw-supply-chain-scanner>). 05.05.2026).*

«Компанія Anthropic нещодавно запустила Mythos Preview — потужну модель штучного інтелекту, яка виявила тисячі вразливостей у основних операційних системах та веб-браузерах. Однак доступ до цього надзвичайно важливого захисного інструменту наразі обмежений приблизно 40 технологічними компаніями, що виключає більшість центральних банків, урядів та дрібніших організацій по всьому світу. Така ексклюзивність становить серйозну глобальну загрозу, оскільки кількість кібератак із використанням III у 2025 році зросла на 89%. Зловмисники, зокрема хакери, що діють за підтримки держави, з таких країн, як Північна Корея та Іран, зараз використовують III для реверс-інжинірингу патчів безпеки та перетворення експлойтів на зброю за лічені хвилини, а не роки. Відповідно, експерти попереджають про наближення «AI bugocalypse» — ситуації, коли некваліфіковані злочинці та іноземні супротивники зможуть легко та дешево атакувати глобальну інфраструктуру...»

Обмежений доступ до передових захисних моделей, таких як Mythos, створює небезпечний глобальний дисбаланс. У той час як фінансово забезпечені організації та широко використовуване американське програмне забезпечення можуть отримувати оперативні виправлення, менші підприємства, країни, що розвиваються, та пропріетарні системи залишаються вкрай вразливими. Оскільки

кібербезпека є глибоко взаємопов'язаною, порушення безпеки в незахищених місцевих підприємствах, лікарнях або муніципальних органах влади неминуче поширюватимуться по глобальних ланцюгах постачання, впливаючи на економіку в цілому. Цю кризу посилює масовий світовий дефіцит фахівців з кібербезпеки, що означає, що організації більше не можуть просто виправляти вразливості, які генеруються штучним інтелектом. Натомість експерти наголошують, що компанії повинні кардинально переписати програмне забезпечення, припустити, що компрометація систем відбудеться, та створити надійну операційну стійкість... Хоча компанія Anthropic попередила, що ці передові наступальні можливості незабаром поширяться серед зловмисних суб'єктів, Білий дім нещодавно заблокував плани щодо розширення доступу до Mythos для більшої кількості організацій. Зрештою, лідери галузі наголошують, що захист глобальної кіберінфраструктури вимагає безпрецедентної співпраці між розробниками, урядами та дослідниками, аргументуючи це тим, що ставлення до сучасних інструментів кібербезпеки як до ексклюзивної розкоші матиме катастрофічні наслідки для всього світу». **(Rina Chandran. The global cybersecurity gap deepens as AI-powered attacks surge // Rest of World (<https://restofworld.org/2026/ai-cybersecurity-anthropic-mythos/>). 05.05.2026).**

«Компанія Cisco Systems домовилася про придбання ізраїльського стартапу з кібербезпеки Astrix Security в рамках угоди, вартість якої, за повідомленнями, становить від 300 до 400 мільйонів доларів, з метою посилення захисту від нових ризиків, пов'язаних із стрімким поширенням автономних агентів штучного інтелекту. Заснована в 2021 році колишніми ветеранами підрозділу 8200 Ізраїльських сил оборони Алоном Джексоном та Іданом Гуром, компанія Astrix, що базується в Тель-Авіві, зосереджується на захисті «нелюдських ідентичностей», таких як API-ключі, облікові записи служб та токени OAuth, які все частіше використовуються для роботи агентів штучного інтелекту та взаємодії між машинами всередині корпоративних систем. Компанія стверджує, що ці облікові дані є широко поширеними, швидко зростають і часто погано управляються, що створює значну і здебільшого невидиму прогалину в безпеці...

Платформа Astrix відстежує роботу агентів штучного інтелекту в корпоративних мережах, контролює облікові дані та інструменти, які вони використовують для доступу до конфіденційних даних, а також виявляє аномальну або зловмисну поведінку в режимі реального часу. Оскільки організації інтегрують агентні системи штучного інтелекту в робочі процеси для автоматизації прийняття рішень та виконання складних завдань, компанія Cisco розглядає ці автономні системи як площину атаки, що стрімко розширюється. Cisco планує інтегрувати технології Astrix у свій загальний портфель рішень з безпеки, зокрема для вдосконалення аналітики ідентифікації та можливостей моделі «нульової довіри». Astrix, у якій працює близько 120 осіб і яка залучила понад 85 мільйонів доларів від інвесторів, зокрема Menlo Ventures та Bessemer Venture Partners, розглядає це придбання як спосіб подолати розрив, що зростає між швидко розвиваючимися

можливостями ШІ та готовністю підприємств до їхнього захисту...» (*Sharon Wrobel. US tech giant Cisco buys Israeli AI cyber startup to protect digital workforce // The Times of Israel* (<https://www.timesofisrael.com/us-tech-giant-cisco-buys-israeli-ai-cyber-startup-to-protect-digital-workforce/>). 05.05.2026).

«Компанія Mozilla випустила велике оновлення Firefox після усунення 271 уразливості безпеки, виявлених за допомогою експериментальної системи штучного інтелекту «Mythos» від Anthropic. Ця вдосконалена модель була застосована для масштабного сканування коду Firefox, виявляючи слабкі місця набагато швидше, ніж традиційні перевірки безпеки, що проводяться людьми, які можуть тривати місяці або роки. Керівництво Mozilla зазначило, що інструменти штучного інтелекту зараз наближаються до можливостей провідних дослідників у галузі безпеки, що знаменує зміну в підході до тестування та захисту програмного забезпечення, де штучний інтелект відіграє дедалі важливішу роль у виявленні вразливостей...

Однак у Mozilla також застерегли, що ті самі потужні інструменти штучного інтелекту, які використовуються для посилення захисту, можуть бути використані зловмисниками для швидшого виявлення та експлуатації вразливостей. Хоча штучний інтелект, можливо, не змінить сферу кібербезпеки за одну ніч, очікується, що він спричинить бурхливий період, під час якого як захисники, так і хакери отримають розширені можливості, що підвищить актуальність оперативного виправлення вразливостей. Існують також побоювання щодо нерівного доступу до таких передових систем, оскільки великі організації можуть мати кращі можливості для використання інструментів безпеки на основі ШІ, що потенційно ставить менших розробників та проекти з відкритим кодом у невигідне становище в плані протидії новим загрозам...» (*Daisy Edwards. Firefox just fixed 271 vulnerabilities found by AI and the warning is worth paying attention to // SB Media Holding Limited* (<https://tech.supercarblondie.com/firefox-fixed-271-vulnerabilities-ai-warning/>). 04.05.2026).

«Компанія Microsoft представила MDASH — систему виявлення вразливостей на основі штучного інтелекту, розроблену її командою Autonomous Code Security та групою Windows Attack Research and Protection. Ця система виявила 16 раніше невідомих вразливостей Windows, зокрема чотири критичні вразливості, що дозволяють віддалено виконати код, які були виправлені у випуску оновлень «Patch Tuesday» 12 травня... Ці критичні уразливості зачіпали широко розповсюджені корпоративні компоненти, зокрема: неавтентифіковану уразливість типу «use-after-free» у стеку IPv4 Windows, доступну через спеціально сформовані пакети з використанням опції Strict Source та Record Route (CVE-2026-33827); уразливість типу «double-free» на етапі до автентифікації у службі IKEEXT, що впливає на RRAS VPN, DirectAccess та Always-On VPN (CVE-2026-33824), а також дві додаткові критичні уразливості в Netlogon та клієнті DNS Windows, кожна з яких отримала оцінку CVSS 9,8; решта 12 «важливих»

уразливостей охоплювали відмову в обслуговуванні, підвищення привілеїв, розкриття інформації та обхід функцій безпеки в таких компонентах, як `tcip.sys`, `http.sys`, `ikeext.dll` та `telnet.exe`. За словами Microsoft, MDASH координує роботу понад 100 спеціалізованих агентів штучного інтелекту, що використовують різноманітні передові та оптимізовані моделі, для сканування коду, перевірки результатів та генерації відтворюваних вхідних даних перед передачею результатів інженерам-людям. Система розроблена таким чином, щоб бути в основному незалежною від конкретних моделей, тому базові моделі можна замінювати без необхідності перебудови конвеєра. Платформа увійде в стадію закритого попереднього перегляду для корпоративних клієнтів наступного місяця, з'явившись на тлі посиленого занепокоєння тим, що ШІ робить атаки швидшими та масштабнішими і посилює гонку з виявлення вразливостей «ШІ проти ШІ», особливо з огляду на те, що Microsoft також бере участь в ініціативах з оцінки моделей, таких як Mythos від Anthropic... Компанія Microsoft підкріпила свої твердження результатами тестів, які показали, що MDASH виявив усі 21 навмисно вбудованих уразливостей у внутрішньому тестовому драйвері без помилкових спрацьовувань, відновив більшість історичних випадків на старих знімках коду та набрав 88,45% у загальнодоступному тесті на відтворення уразливостей CyberGym. Водночас аналітики застерегли, що результати тестів не означають автоматично стійкості підприємства, якщо організації не мають також ефективних механізмів управління та дисципліни усунення уразливостей, щоб реагувати на виявлені системою проблеми». (*Gyana Swain. Microsoft's new AI system finds 16 Windows flaws, including four critical RCEs // FoundryCo, Inc. (<https://www.csoonline.com/article/4170785/microsofts-new-ai-system-finds-16-windows-flaws-including-four-critical-rces.html>). 13.05.2026*).

Штучний інтелект, як зброя кіберзлочинців

«Нове дослідження Единбурзького університету свідчить про те, що кіберзлочинцям не вдається повноцінно інтегрувати штучний інтелект у свою діяльність. У попередній версії дослідження, в якому проаналізовано понад 100 мільйонів дописів з підпільних злочинних форумів, зібраних за допомогою бази даних CrimeBB, дослідники використовували як ручний аналіз, так і велику мовну модель, щоб оцінити, як хакери обговорюють та застосовують інструменти ШІ. Хоча багато кіберзлочинців виявляли зацікавленість у навчанні використанню ШІ, дослідження не виявило суттєвих доказів того, що ці інструменти покращили їхню здатність зламувати системи, розробляти шкідливе програмне забезпечення або вдосконалювати шахрайські схеми. У дискусіях на форумах інструменти ШІ часто описують як не надто корисні, особливо для завдань, пов'язаних із кодуванням, де помічники, як правило, приносять користь вже досвідченим програмістам, а не надають початківцям істотної переваги...

Наразі головний практичний вплив ШІ, здається, обмежується легко автоматизованими діями, такими як створення ботів у соціальних мережах, прості

романтичні афери, шахрайство з оптимізацією пошукових систем та створення фейкових веб-сайтів для отримання доходу від реклами. Навіть досвідчені хакери здебільшого використовують загальнодоступні продукти ШІ, такі як Codex від OpenAI або Claude від Anthropic, для виконання рутинних допоміжних завдань, наприклад, відповідей на питання з програмування чи створення шпаргалок, замість того, щоб покладатися на спеціалізовані «злочинні» моделі ШІ, такі як WormGPT. Багато дописів на форумах зосереджуються на спробах обійти захисні механізми основних систем ШІ, але користувачі повідомляють про труднощі з подоланням цих захистів. Як результат, деякі звертаються до старіших моделей з відкритим кодом, які легше зламати, але вони менш функціональні та вимагають більше ресурсів. Загалом, результати дослідження свідчать про те, що вбудовані в провідні системи ШІ заходи безпеки наразі обмежують їхню ефективність як інструментів для кіберзлочинності». *(Anna Desmarais. Cybercriminals gave AI a go — and came away disappointed, study finds // Euronews (<https://www.euronews.com/next/2026/05/05/cybercriminals-gave-ai-a-go-and-came-away-disappointed-study-finds>). 05.05.2026).*

«Група Google з аналізу загроз (Google Threat Intelligence Group) повідомила про перший підтверджений випадок використання кіберзлочинцями експлойта «нульового дня», який, як вважається, було розроблено за допомогою штучного інтелекту, що свідчить про значне посилення кіберзагроз, пов'язаних із застосуванням ШІ. Експлойти «нульового дня» вважаються одними з найсерйозніших вразливостей безпеки, оскільки вони невідомі захисникам і на момент експлуатації для них немає доступних виправлень. Google повідомила постраждалу організацію перед оприлюдненням своїх висновків, що дозволило випустити виправлення. Хоча дослідники дійшли висновку, що модель Claude Mythos від Anthropic, найімовірніше, не була залучена до цього інциденту, він підкреслює, що використання ШІ для виявлення та використання вразливостей програмного забезпечення вже не є теоретичним...»

Джон Халтквіст, головний аналітик Google Threat Intelligence Group, попередив, що на кожну виявлену уразливість «нульового дня», пов'язану зі штучним інтелектом, припадає, ймовірно, набагато більше невиявлених, і що зловмисники вже використовують ШІ для підвищення швидкості, масштабів та витонченості своїх атак. У тому ж звіті зафіксовано, що пов'язані з Росією угруповання використовують ШІ для атак на українські мережі за допомогою шкідливого програмного забезпечення, а північнокорейська державна хакерська група APT45 застосовує ШІ для вдосконалення та розширення своїх кібероперацій. У попередніх повідомленнях також зазначалося, що у листопаді хакери, підтримувані Пекіном, вперше використали ШІ для повної автоматизації кібератак. Ці події відбуваються на тлі того, як Mythos від Anthropic та нещодавно анонсована модель GPT-5.5-Cyber від OpenAI привертають значну увагу адміністрації Трампа, яка веде постійні дискусії з представниками галузі щодо потенційного регулювання та перевірки передових технологій ШІ. Наразі обидві компанії обмежили доступ до своїх моделей невеликими групами дослідників та перевіреними організаціями, при

цьому Anthropic описує цю стратегію як створення «переваги захисників», яка вимірюється місяцями, а не роками, до того, як передові наступальні можливості ШІ поширяться ширше». (*Maggie Miller. Google says hackers used AI to develop a major security flaw // POLITICO LLC (https://www.politico.com/news/2026/05/11/google-hackers-ai-security-00913247). 11.05.2026*).

«Розвиток штучного інтелекту та поширення моделей кіберзлочинності на основі сервісів значно знизили технічні бар'єри для зловмисників, що призвело до появи більш масштабних і прибуткових загроз для американських підприємств. Оскільки технічну реалізацію атак стає дедалі простіше автоматизувати, зловмисники все частіше зосереджуються на використанні людської природи: 63% організацій стають жертвами атак типу «Business Email Compromise» та підробки особи. Для постачальників керованих послуг (MSP) це створює величезний тиск щодо захисту клієнтських середовищ, водночас доводиться боротися з «тихим вбивцею» — надмірним розширенням інструментарію. Управління десятками перекриваючих один одного рішень з безпеки від різних постачальників створює фрагментовану архітектуру, що сприяє втомі від сповіщень та затримує реагування на інциденти...

Справжня кіберстійкість для MSP тепер залежить від операційної зрілості, а не від простої кількості продуктів безпеки. У середовищі, де атаки з різних векторів стали нормою, MSP повинні надавати пріоритет спрощенню, об'єднуючи свої засоби захисту в єдині платформи, що забезпечують централізований огляд та автоматизоване реагування. Це особливо важливо для захисту середовищ Microsoft 365, які стають головним полем битви для атак на облікові записи. Відмовившись від одноразових інструментів і перейшовши на стандартизовані, повторювані моделі обслуговування, MSP можуть досягти більш ефективного внутрішнього навчання та кращих результатів у сфері безпеки навіть за обмеженого бюджету та нестачі кваліфікованої робочої сили. Зрештою, операційна стійкість стала вирішальним чинником диференціації та конкурентною перевагою, що дозволяє MSP дотримуватися суворих угод про рівень обслуговування (SLA) та забезпечувати задокументовану, постійну дисципліну, необхідну для управління мінливими кіберризиками та відповідності нормативним вимогам». (*James Griffin. Why Cybersecurity Is Now an Operational Discipline for MSPs // Techstrong Group Inc. (https://securityboulevard.com/2026/05/why-cybersecurity-is-now-an-operational-discipline-for-msps/). 05.05.2026*).

«Останні звіти свідчать про різке зростання кількості кіберзагроз, пов'язаних із штучним інтелектом. Згідно з доповіддю Darktrace «State of AI Cybersecurity 2026», 87% фахівців з безпеки відзначають збільшення кількості атак на основі штучного інтелекту, 73% повідомляють про серйозні наслідки для організацій, а 87% стверджують, що штучний інтелект підвищує ефективність шкідливого програмного забезпечення; Звіт CrowdStrike «2026 Global Threat

Report» також повідомляє про 89-відсоткове зростання кількості атак із використанням ШІ порівняно з минулим роком, оскільки злочинці використовують ШІ для швидкої розвідки, автоматизованого ланцюгового використання вразливостей та фішингу з високим рівнем адаптивності, тоді як у звіті Світового економічного форуму «Global Cybersecurity Outlook 2026» вразливості, пов'язані з ШІ, визначені як кіберризик, що зростає найшвидше, для 87% світових лідерів... Ці можливості також використовуються національними державами для прискорення операцій та підтримки шпигунських кампаній і кампаній впливу, що ускладнює встановлення відповідальності та посилює тиск на створення механізмів зміцнення дипломатичної довіри та деескалації. Однією з головних нових проблем є автономний «агентний» ШІ, що діє всередині організацій: Darktrace повідомляє, що 92% керівників служб безпеки турбуються щодо агентів ШІ, а Gartner вказує на ризики «тіньових агентів» від некерованих інструментів та розгортання без коду або з мінімальним кодом, прогнозуючи, що до 2028 року більше половини реагувань на інциденти можуть стосуватися порушень, спричинених власними системами ШІ, підкреслюючи важливість управління ідентифікацією та доступом і порушуючи нові питання щодо відповідальності, ескалації та ненавмисного «відхилення від мети». Водночас «дідфейки» та гіперперсоналізований контент посилюють дезінформацію та соціальну інженерію, підриваючи довіру до комунікацій та збільшуючи рівень успішності шахрайства та фішингу... У плані захисту штучний інтелект покращує виявлення та локалізацію загроз — у звіті IBM «Вартість порушення безпеки даних 2025» зазначається, що середня глобальна вартість порушення знизилася до 4,44 млн доларів, що на 9% менше — проте управління відстає: 13% компаній повідомляють про атаки на свої рішення на базі штучного інтелекту, 97% не мають належного контролю доступу до інструментів штучного інтелекту, а «тіньовий штучний інтелект» може збільшити витрати, пов'язані з порушенням безпеки, приблизно на 670 000 доларів. Окрім ШІ, квантові обчислення додають стратегічної актуальності через ризики «зібрати зараз, розшифрувати пізніше», прискорюючи перехід до постквантової криптографії, що базується на стандартах та рекомендаціях таких органів, як NIST та CISA, а також паралельних зусиллях в ЄС та G7. Загалом, зв'язок між ШІ та кібербезпекою стає центральним у геополітиці та дипломатії — зачіпаючи експортний контроль, управління даними та відповідальну кіберповедінку — тоді як пріоритети політики дедалі більше зосереджуються на зміцненні рамок управління ШІ (враховуючи, що 77% організацій використовують генеративний ШІ, але лише 37% мають офіційні політики безпеки ШІ), поглибленні державно-приватного партнерства для інновацій у сфері оборони та обміну інформацією про загрози, а також інклюзивному встановленні глобальних норм та заходах з побудови довіри для зменшення ескалації та захисту критичної інфраструктури». (Nimra Khalil. *The Strategic Intersection Of AI And Cybersecurity In Contemporary Diplomacy – OpEd // Eurasia Review* (<https://www.eurasiareview.com/07052026-the-strategic-intersection-of-ai-and-cybersecurity-in-contemporary-diplomacy-oped/>). 07.05.2026).

«Міжнародний валютний фонд (МВФ) попередив, що сучасні кібератаки на основі штучного інтелекту становлять серйозну загрозу для глобальної фінансової стабільності, оскільки можуть спричинити ринкові потрясіння, проблеми з фінансуванням та кризи платоспроможності через високу взаємопов'язаність фінансової системи. Сучасні моделі штучного інтелекту здатні швидко виявляти та використовувати вразливості програмного забезпечення типу «нульового дня», про що свідчить майбутня високотехнологічна модель «Mythos» від компанії Anthropic. Ця конкретна загроза спонукала уряд США розпочати державно-приватні випробування та впровадити нову політику, що вимагає попередньої оцінки моделей штучного інтелекту технологічних гігантів. Голова МВФ Крісталіна Георгієва наголосила на нагальній потребі у глобальній співпраці та стратегіях забезпечення стійкості, зазначивши, що глобальна залежність від невеликої кількості хмарних провайдерів збільшує ризик поширення інфекції... Крім того, МВФ наголосив, що країни, що розвиваються, є надмірно вразливими до цих системних кіберзагроз через слабкішу систему захисту та обмеженість ресурсів. Цю вразливість посилює розрив у рівні впровадження штучного інтелекту: згідно з нещодавнім звітом Microsoft, рівень використання генеративного штучного інтелекту значно вищий у розвинених країнах (27,5%) порівняно з країнами, що розвиваються (15,4%). Ця нерівність зумовлена насамперед глобальною нерівністю у цифрових навичках, доступі до Інтернету, електропостачанні та історичними упередженнями щодо обробки англійської мови, хоча останні досягнення у сфері неєвропейських мов починають прискорювати впровадження ШІ у таких регіонах, як Азія». *(IMF warns AI cyber threats could severely shake markets // QATAR TRIBUNE (<https://www.qatar-tribune.com/article/233277/business/imf-warns-ai-cyber-threats-could-severely-shake-markets>). 10.05.2026).*

«У 2026 році в сфері кібербезпеки переважають атаки на основі штучного інтелекту, багаторівневі вимогання з використанням програм-вимагачів та серйозні вразливості ланцюгів постачання, спрямовані проти хмарних платформ та критичної інфраструктури. Два гучні інциденти, що сталися у травні 2026 року, чудово ілюструють ці зростаючі загрози. У секторі освіти відома група кіберзлочинців ShinyHunters скористалася вразливістю навчальної платформи Canvas від Instructure, зіпсувавши портали коледжів та потенційно викривши приватні дані мільйонів студентів і викладачів по всій країні. За словами експерта з кібербезпеки Джона Бруггмана, цей злом підкреслює властиві середовищам «Програмне забезпечення як послуга» (SaaS) ризики, пов'язані з залученням сторонніх постачальників, де компрометація одного постачальника може призвести до масового витоку даних та складних проблем із дотриманням нормативних вимог... Звертаючи увагу на інший, але не менш серйозний вектор загрози, зловмисники з угруповання Play нещодавно скористалися уразливістю «нульового дня» в Windows, щоб отримати системні привілеї та розповсюдити шкідливе програмне забезпечення у багатьох глобальних секторах, зокрема в ІТ, фінансах та роздрібній торгівлі. Відоме своїми тактиками подвійного шантажу —

блокування систем із погрозами оприлюднити викрадені дані — угруповання Play наочно демонструє руйнівний вплив сучасних програм-вимагачів на роботу підприємств. Для боротьби з цими складними загрозами експерти з безпеки наголошують, що організації повинні вийти за межі базового встановлення виправлень і впроваджувати проактивні стратегії локалізації загроз. Наразі до основних засобів захисту належать суворе управління ідентифікацією, покращена оперативна видимість, доступ до мережі за принципом «нульової довіри» (ZTNA), сегментація мережі для запобігання горизонтальному переміщенню та підтримання ізольованих резервних копій». **(Tim Sandle. Two new cyberthreats demonstrate how hackers are evolving // DIGITAL JOURNAL INC. (<https://www.digitaljournal.com/tech-science/two-new-cyberthreats-demonstrate-how-hackers-are-evolving/article>). 09.05.2026).**

«Згідно з доповіддю Thales «Bad Bot Report 2026», на сьогодні в Інтернеті домінує автоматизація на основі штучного інтелекту: у 2025 році на ботів припадатиме понад 53% усього веб-трафіку, а частка людей скоротиться до 47%. З автоматизованого трафіку 40% було класифіковано як зловмисну активність «шкідливих ботів» — це на 3% більше, ніж у попередньому році, що підкреслює зміни як в обсязі, так і в характері онлайн-активності. Thales повідомляє, що кількість атак ботів на базі штучного інтелекту зросла більш ніж у 12 разів, і що приблизно 27% атак ботів зараз спрямовані безпосередньо на API, обходячи захист користувацького інтерфейсу, щоб використовувати бізнес-логіку, витягувати дані або маніпулювати робочими процесами зі швидкістю машини...

Головною проблемою є те, що як легітимні, так і зловмисні боти дедалі частіше взаємодіють з тими самими додатками та API-інтерфейсами подібним чином, через що простого виявлення ботів стає недостатньо. Компанія Thales заявляє, що лише у 2025 році вона заблокувала 17,2 трильйона запитів від ботів, і стверджує, що організації повинні відійти від підходу, спрямованого виключно на «блокування ботів», на користь засобів контролю, заснованих на управлінні, які роблять акцент на прозорості дій автоматизованих систем, дотриманні політик та аналізі поведінки, щоб відрізнити прийнятну автоматизацію від зловмисної чи обманної діяльності». **(Tanya Weaver. AI bots account for more than half of all web traffic, with 40% classified as malicious // The Institution of Engineering and Technology (<https://eandt.theiet.org/2026/05/11/ai-bots-account-more-half-all-web-traffic-40-classified-malicious>). 11.05.2026).**

Кіберзлочинність та кібертероризм

«ФБР попереджає, що кібершахрайство дедалі частіше переорієнтовується з викрадення платіжних даних на викрадення дорогоцінних фізичних вантажів шляхом «стратегічного викрадення вантажів», коли злочинці видають себе за законних брокерів та перевізників, щоб захопити вантаж і

змінити маршрут доставки. Принаймні з 2024 року зловмисники отримують несанкціонований доступ до логістичних систем за допомогою підроблених електронних листів, фальшивих URL-адрес та зламаних облікових записів перевізників, а потім використовують ці надійні облікові записи для розміщення шахрайських оголошень про вантажі на дошках оголошень та обману відправників, брокерів і перевізників з метою отримання вантажів, які потім перенаправляються та перепродаються. У деяких випадках зловмисники намагаються встановити інструменти віддаленого моніторингу та управління (RMM) на системах перевізників через шкідливі посилання, щоб посилити контроль, і можуть навіть вимагати викуп у брокерів в обмін на інформацію про місцезнаходження викрадених товарів... Проблема швидко набирає обертів: за оцінками ФБР, збитки від крадіжок вантажів у США та Канаді у 2025 році сягнуть 725 мільйонів доларів, що на 60% більше, ніж у попередньому році, при цьому кількість підтверджених випадків зросла на 18%, а середня вартість однієї крадіжки збільшилася на 36% — до приблизно 273 990 доларів, оскільки злочинці стають дедалі вибагливішими. Відповідні звіти від Proofpoint вказують на те, що логістичні та автотранспортні компанії, особливо в галузі харчових продуктів та напоїв, є частими цілями, а великі компанії також постраждали від організованих злочинних угруповань. ФБР рекомендує застосовувати суворі процедури перевірки, включаючи незалежне підтвердження запитів на відправлення та забір вантажу через додаткові канали, використання багатоканальних перевірок особи, а не довіру до знайомих імен або адрес електронної пошти, а також збір детальної ідентифікаційної інформації, такої як фотографії водія та транспортного засобу, номери ліцензії та DOT/Motor Carrier, а також повні контактні дані перед видачею вантажу». *(Will McCurdy. Cybercriminals Are Now Coming After Freight Cargo. And They're Doing a Great Job // Ziff Davis, LLC. (<https://uk.pcmag.com/business-1/164731/cybercriminals-are-now-coming-after-freight-cargo-and-theyre-doing-a-great-job>). 02.05.2026).*

«Складна кіберзлочинна кампанія, пов'язана з В'єтнамом, відома під назвою «AccountDumpling», призвела до злому приблизно 30 000 акаунтів у Facebook по всьому світу, причому майже 69 відсотків жертв проживають у Сполучених Штатах. Операція є особливо ефективною, оскільки обходить традиційні фільтри безпеки електронної пошти, зловживаючи платформою Google AppSheet; оскільки фішингові приманки надсилаються безпосередньо з легітимних серверів Google, вони успішно проходять перевірки автентифікації SPF, DKIM та DMARC, ефективно використовуючи довіру до платформи для досягнення користувачів. Зловмисники використовують модульний підхід, застосовуючи чотири різні фішингові стратегії — від підроблених попереджень про порушення політики та винагород за верифікацію «Blue Badge» до оманливих пропозицій роботи від великих технологічних компаній — для збору облікових даних, кодів двофакторної автентифікації та фотографій з державних посвідчень...

Ці викрадені активи миттєво передаються через ботів Telegram, що дозволяє зловмисникам здійснювати захоплення облікових записів у режимі реального часу. Guardio Labs, яка викрила цю кампанію, простежила операцію до зловмисника з

В'єтнаму після виявлення метаданих автора у фішинговому PDF-файлі, що ідентифікували конкретну особу, яка публічно рекламує послуги з відновлення облікових записів. Це відкриття висвітлює замкнуту злочинну економіку, в якій зловмисники викрадають цінні бізнес-активи, використовують їх для проведення шахрайських кампаній, а потім намагаються знову отримати прибуток, продаючи послуги з «відновлення облікових записів» назад первинним жертвам». **(Dhivya. Attackers Abuse Google AppSheet, Netlify, and Telegram in Facebook Phishing Campaign // Cyber Security News (<https://cybersecuritynews.com/attackers-abuse-google-appsheet-netlify-and-telegram/>). 02.05.2026).**

«Галузь децентралізованих фінансів (DeFi) наразі переживає серйозну кризу, оскільки інвестори вивели з цього сектору майже 14 мільярдів доларів після низки гучних випадків порушення безпеки. Цей масовий відтік коштів призвів до скорочення загального обсягу ринку до приблизно 86 мільярдів доларів — найнижчого показника за останній рік. Причиною такого відтоку стали дві руйнівні кібератаки: крадіжка 290 мільйонів доларів з Aave, найбільшої кредитної платформи галузі, яку приписують хакерам, пов'язаним з Північною Кореєю, та пограбування біржі Drift на суму 280 мільйонів доларів. Ці інциденти викрили вразливість навіть найавторитетніших цифрових платформ до сучасних кіберзагроз, що спонукало багатьох трейдерів перевести свої активи назад до традиційних банківських установ...»

Атака на Aave мала особливо критичні наслідки: вона залишила платформу з безнадійною заборгованістю у розмірі 230 мільйонів доларів і загрожувала системним колапсом. У відповідь коаліція лідерів галузі, до якої увійшли співзасновник Ethereum Джозеф Любін та мільярдер Джастін Сан, організувала екстрену фінансову допомогу для стабілізації екосистеми. Незважаючи на ці зусилля, ціни на токени Aave та інших великих проєктів, таких як Uniswap, впали більш ніж на 30%. Експерти ринку попереджають, що ситуація з загрозами погіршується, оскільки хакери потенційно використовують штучний інтелект для експлуатації вразливостей коду, а квантові обчислення стають майбутнім ризиком. Як наслідок, американські законодавці прискорюють прийняття законів для встановлення суворих правил діяльності та посилення захисту користувачів, оскільки багато хто вважає, що галузь залишається головним об'єктом для професійних хакерів без надійних регуляторних запобіжних заходів». **(Annika Masrani. Aave and DeFi Investors Flee as a Wave of Devastating Hacks Wipes Out \$14 Billion in Market Value // TipRanks (<https://www.tipranks.com/news/aave-and-defi-investors-flee-as-a-wave-of-devastating-hacks-wipes-out-14-billion-in-market-value>). 06.05.2026).**

«Кібератака на Canvas — хмарну платформу для управління навчальним процесом, якою користуються понад 8 000 навчальних закладів та близько 30 мільйонів користувачів по всьому світу, — спричинила значні перебої в роботі університетів у США, Канаді, Австралії, Великій Британії, Новій Зеландії та

інших країнах. Компанія Instructure, яка розробляє Canvas, підтвердила, що 1 травня стався злом, і, як вважається, серед викрадених даних є імена, адреси електронної пошти, ідентифікаційні номери студентів та повідомлення між користувачами, хоча керівник служби інформаційної безпеки компанії заявив, що немає доказів того, що паролі, дати народження, державні ідентифікатори або фінансова інформація були скомпрометовані... Хоча компанія Instructure заявила, що станом на 2 травня інцидент було в основному локалізовано, за повідомленнями, активна група-вимагач ShinyHunters здійснила повторну атаку, змінивши зовнішній вигляд порталів входу в систему Canvas у сотнях навчальних закладів та розмістивши там записки з вимогою викупу, в яких попереджалося, що 12 травня буде опубліковано 275 мільйонів записів обсягом 3,65 терабайта даних із понад 8 800 навчальних закладів, якщо викуп не буде сплачено. ShinyHunters діє за моделлю вимагання «плати або ми опублікуємо», а не шифрує файли, і має перехресні зв'язки з іншими кіберзлочинними угрупованнями, зокрема Scattered Spider та LAPSUS\$...

Час, обраний для атаки, виявився особливо згубним, оскільки збігся з періодом іспитів у багатьох навчальних закладах. Університет штату Міссісіпі був змушений перенести іспити, а студенти таких навчальних закладів, як Оксфордський університет, не мали доступу до навчальних матеріалів і змушені були покладатися на документи, надіслані викладачами електронною поштою. Серед постраждалих британських навчальних закладів — університети Бірмінгема, Оксфорда та Единбурга; за повідомленнями, університет Бірмінгема вже відновив роботу, тоді як Оксфордський університет попередив, що платформа Canvas залишається недоступною, і точної дати відновлення роботи поки що немає. Університети в Австралії, зокрема Сіднейський університет, також постраждали, і студентів попередили не намагатися увійти на платформу...» **(Ross Kelly. Universities worldwide still struggling with fallout from Canvas cyber attack // Future US, Inc. (<https://www.itpro.com/security/cyber-attacks/universities-worldwide-still-struggling-with-fallout-from-canvas-cyber-attack>). 11.05.2026).**

«Компанія Instructure, розробник системи управління навчанням Canvas, повідомляє, що досягла угоди з «неавторизованим суб'єктом», який стоїть за нещодавніми атаками, щодо повернення викрадених даних. За її словами, хакери повернули інформацію та заявили, що знищили всі залишки копій, хоча Instructure не розкрила, хто саме був відповідальним за атаку, а також не повідомила про умови угоди. Група ShinyHunters, яка взяла на себе відповідальність, повідомила TechCrunch, що отримала дані про 275 мільйонів людей, що ці дані тепер видалені і що подальших вимог про виплату не буде...

Компанія Instructure повідомила, що система Canvas зазнала двох вторгнень: інцидент 29 квітня, під час якого зловмисники викрали назви курсів, адреси електронної пошти, дані про реєстрацію, повідомлення та імена користувачів, а також другий випадок, коли зловмисники змінили сторінки, які бачили деякі користувачі, що увійшли в систему. В результаті облікові записи Canvas у режимі «Free-For-Teacher» були тимчасово заблоковані. Ця угода викликала критику з боку

експертів з безпеки, які попереджають, що виплати або переговори з зловмисниками можуть спровокувати нові випадки вимагання, а ФБР порадило організаціям не платити та не вступати в контакт з тими, хто стверджує, що вкрав дані». (*Brad Matthews. Instructure, company behind Canvas learning platform, reaches deal with hackers to recover data // The Washington Times, LLC* (<https://www.washingtontimes.com/news/2026/may/12/instructure-company-behind-canvas-learning-platform-reaches-deal/>). 12.06.2026).

«Нещодавнє розслідування, проведене Cisco Talos, виявило триваючу кібератаку, яка використовує функцію Phone Link від Microsoft: спочатку на ПК з Windows встановлюється троян для віддаленого доступу під назвою CloudZ RAT (троян для віддаленого доступу). Кампанія, яка триває з січня, починається з того, що жертв обманом змушують встановити оновлення ScreenConnect, яке виглядає як легітимне, але інсталятор є підробленим і замість цього розгортає шкідливе програмне забезпечення, яке завантажує та запускає CloudZ. Після активації троян підключається до сервера, контрольованого зловмисником, розблоковує свою конфігурацію та може викрасти конфіденційну інформацію, таку як збережені облікові дані браузера, без очевидних ознак компрометації...

Атака стає ще більш небезпечною завдяки додатковому плагіну під назвою «Pheno», який спеціально націлений на додаток Phone Link. Він сканує та збирає синхронізовані дані з додатка, тимчасово зберігає їх, а потім передає на сервер зловмисника. Це означає, що в разі зараження ПК дані, якими обмінюються комп'ютер і підключений смартфон — наприклад, повідомлення чи одноразові паролі — також можуть бути перехоплені. Хоча отримані дані не вказують на те, що користувачам слід припинити використання Phone Link, вони підкреслюють, що безпека синхронізації між пристроями залежить від рівня захисту найменш захищеного пристрою. Експерти рекомендують завантажувати програмне забезпечення лише з надійних джерел, підтримувати активність антивірусних програм та інструментів виявлення загроз, а також швидко відключати заражені пристрої, щоб запобігти подальшому витоку даних...» (*Shimul Sood. Your Phone Link setup on Windows could be at risk from this Trojan // Authority Media* (<https://www.androidauthority.com/microsoft-phone-link-trojan-3664066/>). 06.05.2026).

«Хакери зламали офіційний веб-сайт DAEMON Tools у результаті атаки на ланцюжок постачання, вбудувавши троянські програми в інсталятори версій від 12.5.0.2421 до 12.5.0.2434 та розповсюджуючи бінарні файли з бекдорами з 8 квітня. За даними «Касперського», тисячі систем у понад 100 країнах були заражені після того, як користувачі завантажили та запустили цифрові підписані інсталятори, які містили вбудований шкідливий код у таких файлах, як DTHelper.exe, DiscSoftBusServiceLite.exe та DTShellHlp.exe. Після запуску

шкідливе програмне забезпечення забезпечувало свою стійкість, активувало бекдор під час запуску системи та підключалося до сервера управління...

Початковий шкідливий код виконував функцію програми для викрадення інформації, збираючи такі системні дані, як ім'я хоста, MAC-адреса, встановлене програмне забезпечення, запущені процеси та дані про локаль для профілювання. На основі цих розвідувальних даних невелика група жертв — близько десятка комп'ютерів — отримала шкідливий код другого етапу, що вказує на цільову кампанію, спрямовану на важливі організації в таких секторах, як роздрібна торгівля, наука, державні структури та виробництво, у таких країнах, як Росія, Білорусь і Таїланд. Принаймні в одному випадку зловмисники застосували більш досконалий штаб шкідливого програмного забезпечення, відомий як QUIC RAT, здатний використовувати різні протоколи зв'язку та вбудовувати шкідливий код у легітимні процеси.

Компанія «Касперський», що спеціалізується на кібербезпеці та виявила цей витік даних, зазначає, що завдяки складності атаки зловмисникам вдалося залишатися непоміченими майже місяць, і припускає, що вони, ймовірно, є носіями китайської мови...» (*Bill Toulas. DAEMON Tools trojanized in supply-chain attack to deploy backdoor // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/daemon-tools-trojanized-in-supply-chain-attack-to-deploy-backdoor/). 05.05.2026*).

«Округ громадських коледжів Сан-Дієго наразі бореться зі значною кібератакою, яка розпочалася минулої суботи та спричинила серйозні збої в роботі електронної пошти, веб-сайтів та систем реєстрації студентів. Округ, який обслуговує приблизно 90 000 студентів, був змушений відключити низку систем, хоча більшість занять продовжуються, незважаючи на певні технічні труднощі. Представники округу заявили, що їхні системи безпеки негайно виявили вторгнення і що наразі немає жодних доказів витоку даних... Головна увага в рамках заходів з відновлення приділяється налагодженню роботи системи реєстрації студентів, оскільки збій у роботі системи загрожує зривом майбутньої літньої сесії, на яку зазвичай записується близько 60 000 студентів. Поки триває розслідування щодо джерела атаки, округ інформує громадськість за допомогою SMS-повідомлень, офіційного додатку з питань безпеки та каналів у соціальних мережах, а його ІТ-команди працюють цілодобово над відновленням повної працездатності системи». (*Jacob Smith. Cyberattack Jolts San Diego Community Colleges, Knocks Key Systems Offline // SFist LLC (https://hoodline.com/2026/05/cyberattack-jolts-san-diego-community-colleges-knocks-key-systems-offline/). 05.05.2026*).

«Все більше користувачів Claude повідомляють про несанкціоновані покупки, пов'язані з їхніми обліковими записами, що зумовлено не злом систем Anthropic, а захопленням облікових записів, яке відбувається через вразливості в системах оплати та функціях подарункових підписок. Згідно з

повідомленнями про безпеку та дослідженнями, на які посилається The Guardian, сучасні фішингові атаки стають дедалі більш автоматизованими та підтримуються штучним інтелектом, що дозволяє шахраям отримувати викрадені паролі або перехоплювати активні сесії браузера за допомогою фішингових електронних листів або шкідливого програмного забезпечення. Опинившись в обліковому записі жертви, зловмисники уникають зміни облікових даних — що могло б викликати сповіщення — і натомість використовують лазівку у системі «подарунків», щоб надсилати численні подарункові підписки на електронні адреси, які вони контролюють...

Оскільки купівля подарунків зазвичай вимагає менше етапів перевірки, ніж внесення змін до облікового запису, і не завжди передбачає додаткову аутентифікацію, наприклад, за допомогою банківських кодів підтвердження, шахраї можуть швидко генерувати цифрові коди подарунків і перепродавати їх на сторонніх торговельних майданчиках, часто за криптовалюту, перш ніж жертви помітять списання коштів. Швидке зростання популярності платформ на базі штучного інтелекту зробило їх привабливою мішенню, особливо в тих випадках, коли засоби захисту, такі як моніторинг сеансів та перевірка платежів, не встигають за темпами розвитку...

Експерти з безпеки рекомендують користувачам видалити збережені способи оплати, вийти з усіх активних сеансів, щоб знешкодити будь-які викрадені облікові дані, а також перевіряти електронну пошту на наявність несподіваних підтверджень отримання подарунків. Хоча ця проблема не пов'язана з прямим злом інфраструктури Claude, вона демонструє, як швидко шахраї можуть скористатися прогалинами в системі управління обліковими записами, та підкреслює необхідність запровадження більш надійних заходів безпеки, таких як двофакторна автентифікація для операцій з подарунками». (*Amanda Caswell. Urgent Claude AI warning: Hackers are using a \$600 'gift' loophole to bypass 2FA // Future US, Inc. (<https://www.tomsguide.com/ai/urgent-claude-ai-warning-hackers-are-using-a-gift-loophole-to-bypass-2fa>). 06.05.2026*).

«Оскільки майже 70% населення світу дедалі більше покладається на тісно взаємопов'язану цифрову інфраструктуру, масштаби та серйозність кіберзагроз вийшли за межі окремих технічних збоїв і перетворилися на системні глобальні ризики. Гучні інциденти, такі як NotPetya та WannaCry, продемонстрували, як локальні хакерські атаки можуть перерости у катастрофи, що коштують мільярди доларів, впливаючи на критично важливі послуги у сотнях країн. Ця нова реальність спричинила концептуальний перехід від традиційної «кібербезпеки», зосередженої на запобіганні проникненню, до «кіберстійкості», яка наголошує на тому, як суспільства можуть колективно адаптуватися та відновлюватися, коли неминуче відбуваються успішні атаки...

Однак формуванню такої стійкості заважає фрагментований цифровий простір, що характеризується значною геополітичною нестабільністю, заплутаною мозаїкою глобальних нормативних актів та значними розбіжностями у можливостях між країнами та організаціями. Малі та середні підприємства (МСП) є

особливо вразливими, створюючи слабкі ланки у складних глобальних ланцюгах постачання. Новітні технології, такі як генеративний штучний інтелект та квантові обчислення, ще більше посилюють ці ризики, створюючи нові вразливі місця та ставлячи під загрозу існуючі системи шифрування.

Щоб вирішити ці проблеми, акцент слід перенести з переговорів на високому рівні на конкретну реалізацію колективної оборони. Це передбачає офіційне визначення державами об'єктів критичної інфраструктури, встановлення чітких правил повідомлення про інциденти та участь у заходах із зміцнення довіри, таких як створення прямих каналів комунікації для деескалації напруженості. Важливо, що розбудова національного та організаційного потенціалу — через розвиток навичок та об'єднання регіональних ресурсів — є необхідною передумовою ефективної співпраці. Ставлячись до промисловості, наукових кіл та громадянського суспільства як до оперативних партнерів та використовуючи постійні міжнародні механізми, такі як майбутній Глобальний механізм ООН з безпеки ІКТ, міжнародна спільнота може почати формувати потужну колективну відповідь, необхідну для захисту цифрових основ сучасного життя». **(Robin Geiss. Why cyber resilience needs to be concrete, cooperative and collective // World Economic Forum (<https://www.weforum.org/stories/2026/05/why-cyber-resilience-needs-to-be-concrete-cooperative-and-collective/>). 04.05.2026).**

«Хоча 4 травня відзначається як День «Зоряних воєн», це також нагадує про те, що тактики кіберзлочинців — такі як фішинг, шахрайство та крадіжка даних — віддзеркалюють обман і маніпуляції Темної сторони прямо тут, на Землі. Шахраї використовують тематичні розіграші, відчуття терміновості та знайомість, щоб обійти вашу розсудливість, тому якщо у вас виникло «погане передчуття» щодо повідомлення чи пропозиції, знайдіть хвилинку, щоб перевірити його, перш ніж натискати на посилання або ділитися даними. Імітація особи також еволюціонує: клонування голосу за допомогою штучного інтелекту може зробити так, що голос того, хто телефонує, звучатиме точно як голос близької людини, яка потрапила в біду, тому надзвичайно важливо покласти слухавку, передзвонити на перевірений номер та домовитися про сімейне паролі... Оскільки Темна Сторона процвітає завдяки слабким або повторно використовуваним пароліам, дотримання правил безпеки при створенні паролів є вашою першою лінією захисту від захоплення облікових записів. Так само ваші «дроїди» — ваші пристрої — потребують захисту від шкідливого та шпигунського програмного забезпечення за допомогою регулярних оновлень, перевірених джерел додатків та надійного програмного забезпечення для безпеки. Кіберзлочинці, подібно до Імперії, покладаються на викрадені дані; порушення безпеки розкривають вашу цифрову ідентичність (вашу «сигнатуру Сили») і сприяють більш переконливим атакам, тому розуміння та управління вашим цифровим слідом є життєво важливим. Щоб залишатися в безпеці, ви можете покладатися на розумні звички та інструменти, такі як Bitdefender Scamio для перевірки підозрілих повідомлень, Link Checker для виявлення небезпечних веб-сайтів та Digital Identity Protection для моніторингу витоків даних. Зупинившись перед тим, як діяти, та підтримуючи міцний захист, ви

можете захистити себе від реальних загроз, які набагато ближчі, ніж далека-далека галактика». (*Alina BÎZGĂ. May the Fourth Be With You: Cybersecurity Lessons From a Galaxy Far, Far Away // Bitdefender (<https://www.bitdefender.com/en-gb/blog/hotforsecurity/star-wars-day-cybersecurity-lessons>). 04.05.2026*).

«7 травня Австралійський центр кібербезпеки (ACSC), що входить до складу Австралійського управління радіорозвідки, попередив про триваючу шкідливу кампанію з розповсюдження шкідливого ПЗ для викрадення даних Vidar Stealer, в якій використовується техніка соціальної інженерії «ClickFix». Кампанія націлена на організації та інфраструктуру в різних секторах і зосереджена переважно на користувачах Microsoft Windows. Vidar Stealer призначений для викрадення конфіденційних даних, зокрема імен користувачів та паролів, інформації про кредитні картки, даних гарантів криптовалют, історії браузера та навіть токенів багатофакторної автентифікації... ACSC повідомляє, що зловмисники поєднують зламані сайти на WordPress із приманками ClickFix: жертв перенаправляють зі зламаних сторінок WordPress на сайти, що розповсюджують шкідливе програмне забезпечення, де відображаються підроблені CAPTCHA-запити та спонукають користувачів самостійно виконувати шкідливі команди або скрипти, що дозволяє обійти багато традиційних засобів захисту. Після встановлення Vidar Stealer використовує тактику ухилення, зокрема видаляє вихідний виконуваний файл і працює переважно в пам'яті, що ускладнює його виявлення та видалення... Щоб зменшити цю загрозу, ACSC рекомендує обмежити виконання неперевірених програм та скриптів, забезпечити повне оновлення компонентів WordPress, браузерів, механізмів виконання скриптів та операційних систем, оперативно встановлювати оновлення на кінцеві пристрої та сервери, що мають вихід в Інтернет, обмежити доступ до буфера обміну браузера для JavaScript з ненадійного вмісту, а також запровадити багатофакторну автентифікацію (MFA), стійку до фішингових атак». (*Danny Palmer. Australian Cyber Security Centre Issues Alert Over ClickFix Attacks // Reed Exhibitions Ltd. (<https://www.infosecurity-magazine.com/news/australian-cyber-security-centre/>). 08.05.2026*).

«Команда реагування на комп'ютерні надзвичайні ситуації Нігерії (ngCERT) опублікувала загальнонаціональне попередження про тривалу хвилю складних атак типу «розподілена відмова в обслуговуванні» (DDoS), які становлять загрозу для критичної цифрової інфраструктури як у державному, так і в приватному секторах. Ці атаки характеризуються дедалі більшою агресивністю та складністю; у них застосовуються багатовекторні операції, що поєднують об'ємні флуди, атаки на рівні протоколів та атаки на рівні додатків, щоб уникнути виявлення та перевантажити засоби захисту систем. Для здійснення цих скоординованих атак зловмисники використовують методи відбиття та посилення, одночасно експлуатуючи відомі вразливості програмного забезпечення — такі як Log4Shell та недоліки в Citrix і Drupal — для залучення скомпрометованих пристроїв до масштабних ботнетів...

Наслідки цих атак виходять далеко за межі тимчасових перебоїв у роботі сервісів, створюючи значні ризики для фінансової стабільності, операційної стійкості та репутації установ. Крім того, ngCERT попередило, що ці DDoS-атаки дедалі частіше використовуються як «димові завіси» для маскування більш серйозних загроз, таких як поширення програм-вимагачів та несанкціоноване викрадення даних. У відповідь на це агентство закликала організації застосовувати проактивний підхід до безпеки, рекомендуючи впровадження спеціальних засобів захисту від DDoS-атак, таких як очищення трафіку та обмеження швидкості, а також ретельне оновлення програмного забезпечення та зміцнення інфраструктури. Організаціям також рекомендується тісно співпрацювати з інтернет-провайдером для фільтрації шкідливого трафіку та впровадження надійних заходів забезпечення стійкості, включаючи балансування навантаження та постійний моніторинг мережі. Це попередження, яке слідує за аналогічним попередженням від Комісії з захисту даних Нігерії щодо загроз фінансовій системі, підкреслює зростаючий консенсус щодо того, що кіберстійкість є не лише технічним викликом, а й критично важливим національним економічним та безпековим імперативом для Нігерії». (*Cyber Security Agency Warns of Rising Cyber Attacks on Nigeria's Critical Infrastructure* // **THISDAY NEWSPAPERS LTD.** (<https://www.thisdaylive.com/2026/05/03/cyber-security-agency-warns-of-rising-cyber-attacks-on-nigerias-critical-infrastructure/>). 03.05.2026).

«Дослідники з безпеки центру SANS Internet Storm Center попередили про шкідливу рекламну кампанію в Google Ads, спрямовану на користувачів, які шукають Homebrew — популярний менеджер пакетів з відкритим кодом для macOS та Linux. Зловмисники розміщують у верхній частині Google спонсорований результат «Homebrew», який веде на клонований веб-сайт і пропонує користувачам скопіювати та вставити команду в Термінал; оскільки багато користувачів Homebrew звикли виконувати команди з командного рядка, шахраї використовують дії самої жертви для запуску шкідливого програмного забезпечення, а не пряме віддалене вторгнення. Вставлена команда призначена для обходу перевірок безпеки Apple та встановлення програми для викрадення інформації, відомої як MacSync, яка виконується в пам'яті та може викрадати конфіденційні дані, включаючи паролі Keychain та сесійні файли cookie, а також може націлюватися на розширення браузера для криптовалютних гаманців, такі як MetaMask...

У рекомендаціях з безпеки наголошується на необхідності уникати спонсорованих результатів пошуку, переходити лише на офіційний сайт Homebrew, ставитися до будь-яких прохань ввести команди в Терміналі як до серйозного тривожного сигналу, якщо джерело не є повністю надійним і зрозумілим, а також зменшувати ризик витоку облікових даних, використовуючи спеціальний менеджер паролів замість зберігання секретних даних у браузері чи Keychain. Користувачам, які підозрюють, що виконали шкідливу команду, рекомендується діяти швидко: негайно перевірити систему на наявність шкідливого програмного забезпечення та змінити паролі». (*Sara Heritage. Homebrew users are accidentally downloading*

malware instead of the real app // Valnet Inc. (<https://www.makeuseof.com/how-one-fake-google-ad-can-silently-steal-your-macs-passwords/>). 04.05.2026).

«Органи з управління надзвичайними ситуаціями Абу-Дабі попередили, що кількість кібератак зазвичай різко зростає в періоди криз, страху та плутанини, оскільки люди приймають поспішні рішення в цифровому просторі без належної перевірки та стають більш вразливими до чуток, втоми та соціальної інженерії. У нещодавно опублікованих «Рекомендаціях щодо обізнаності з питань кібербезпеки під час надзвичайних ситуацій» Центр управління надзвичайними ситуаціями, кризами та катастрофами Абу-Дабі висвітлив типові загрози та ознаки підозрілих повідомлень і посилянь, зазначивши, що підвищений рівень тривоги збільшує ймовірність того, що люди натиснуть на шкідливі посилення або поділяться конфіденційною інформацією. Ці рекомендації перегукуються з більш загальними попередженнями, опублікованими після нещодавніх геополітичних ескалацій, у яких аналітики з питань безпеки застерігають, що напруженість може спровокувати як опортуністичні атаки, так і діяльність, пов'язану з державою...

Дослідники у сфері кібербезпеки також зазначають, що штучний інтелект посилює ці ризики, автоматизуючи розвідку, створюючи надзвичайно переконливі фішингові повідомлення та масово генеруючи контент із використанням технології «дідфейк», що знижує бар'єри для злочинців та робить атаки дешевшими й більш поширеними. Компанія Microsoft також повідомила про постійне вдосконалення фішингових тактик, які поєднують соціальну інженерію зі зловживанням інфраструктурою та автентифікацією для обходу засобів захисту, і зазначила, що відстежила кампанії, які проводилися з 14 по 16 квітня та були спрямовані на понад 35 000 користувачів у 13 000 організаціях у 26 країнах. Microsoft зазначила, що встановити авторство може бути складно, але її аналіз показав, що в кампанії використовувалася легітимна служба доставки електронної пошти і, ймовірно, вона походила з віртуальної машини Windows, розміщеної в хмарі». *(Cody Combs. UAE cautions against 'rushed digital decision-making' in warning over potential cyber attacks // International Media Investments (<https://www.thenationalnews.com/news/us/2026/05/04/uae-cybersecurity-hackers-safety/>). 04.05.2026).*

«Останнє дослідження уряду Великої Британії щодо порушень кібербезпеки висвітлює значну та поширену загрозу: майже половина всіх підприємств — приблизно 612 000 компаній — повідомили про щонайменше одне кіберпорушення або атаку протягом минулого року. Цей ризик є особливо гострим для великих корпорацій, 69% яких зазнали атак, тоді як 29% усіх компаній стикаються з вторгненнями щотижня. Фішинг залишається найпоширенішим методом, який застосовується проти 38% підприємств, але загроза стає все серйознішою, оскільки злочинці використовують моделі штучного інтелекту

нового покоління для автоматизації виявлення та експлуатації вразливостей програмного забезпечення з безпрецедентною швидкістю та масштабом...

У відповідь на загострення ситуації з загрозами міністри уряду закликають керівників підприємств визнати кібербезпеку пріоритетним завданням, відповідальність за яке має нести керівництво найвищого рівня. Нова «Декларація про кіберстійкість» заохочує компанії вжити трьох важливих заходів: винести питання кібербезпеки на рівень ради директорів, підключитися до безкоштовної служби раннього попередження NCSC та запровадити обов'язкову сертифікацію Cyber Essentials, що підтримується урядом, у своїх ланцюгах постачання. Ця ініціатива, доповнена майбутнім законопроектом про кібербезпеку та стійкість, має на меті зміцнити такі важливі сфери, як енергетика, водопостачання та охорона здоров'я. Зосередившись на обізнаності персоналу та цілісності ланцюгів постачання, уряд прагне посилити національну стійкість та захистити економіку Великої Британії від зростаючого ризику кіберзбоїв, спричинених штучним інтелектом». (*Firms urged to strengthen cyber defences as criminals turn to AI // Business Biscuit (<https://businessbiscuit.com/business-news/business-tech-news/cyber-criminals-using-ai/>). 05.05.2026*).

«Хакери все частіше націлюються на спільноту розробників, створюючи підроблені репозиторії GitHub, що видають себе за популярні інструменти штучного інтелекту; остання кампанія зосереджена на «DeepSeek TUI». Імітуючи макет і оформлення справжніх проєктів, зловмисники спонукають користувачів завантажувати шкідливі архіви у форматі 7z. Дослідники з QiAnXin Threat Intelligence Center визначили цю кампанію як еволюцію операції «OpenClaw», викритої раніше у 2026 році, зазначивши, що той самий зловмисник почергово використовує величезний каталог підроблених інсталяторів на тему штучного інтелекту, зокрема для Claude, Grok та WormGPT...

Саме шкідливе ПЗ написано на мові Rust і використовує надзвичайно витончені методи ухилення від виявлення. Після запуску воно перевіряє середовище, щоб уникнути аналізу в пісочниці; якщо воно визначає, що знаходиться на справжньому комп'ютері користувача, воно систематично вимикає захист Windows Defender, змінює правила брандмауера та розпочинає багатоетапну доставку корисного навантаження. Шкідливе програмне забезпечення встановлює постійний доступ за допомогою різних методів, включаючи заплановані завдання, ключі реєстру «Run» та хуки Winlogon, підтримуючи при цьому зв'язок з командним центром через Telegram. З огляду на складність та прихованість цієї операції, експерти з безпеки настійно рекомендують розробникам ретельно перевіряти автентичність будь-якого репозиторію GitHub — приділяючи особливу увагу віку облікового запису, історії комітів та легітимності авторів — перед завантаженням програмного забезпечення, а також використовувати інструменти виявлення кінцевих точок, які відстежують аномальну активність PowerShell та ін'єкцію пам'яті». (*Tushar Subhra Dutta. Hackers Use Fake DeepSeek TUI GitHub Repositories to Deliver Malware // (<https://cybersecuritynews.com/hackers-use-fake-deepseek-tui-github-repositories/>). 11.05.2026*).

«Сучасні «пограбування» дедалі частіше відбуваються у цифровому, а не фізичному просторі: хакери використовують вразливості за екранами замість того, щоб виламувати вікна, тоді як гучні крадіжки, такі як викрадення французьких королівських коштовностей із Лувру, стають дедалі рідшими. З огляду на те, що щодня у світі відбувається понад 2 000 кібератак — приблизно одна кожні 39 секунд — багато організацій досі розглядають кібербезпеку як проблему ІТ або дотримання нормативних вимог, а не як основний пріоритет бізнесу, незважаючи на те, що кіберзлочинці можуть діяти в різних юрисдикціях і часто дотримуються звичного сценарію: проникають у системи, блокують доступ до даних, викрадають інформацію або кошти та вимагають викуп... Фінансові масштаби набагато більші, ніж у випадку багатьох традиційних злочинів: за даними аналізу уряду Великої Британії, середня вартість серйозної кібератаки на підприємство становить майже 195 000 фунтів стерлінгів, а за результатами моделювання зловживання, пов'язані з витоком даних організацій, можуть коштувати близько 755 мільйонів фунтів стерлінгів щорічно. Реальні наслідки підкреслюють серйозність ситуації, наприклад, кіберінцидент у Marks & Spencer, який зачепив мільйони клієнтів і, за оцінками, скоротив прибуток у 2025 році приблизно на 300 мільйонів фунтів стерлінгів. У звіті PwC, на який посилається текст, міститься попередження про те, що загрози набирають обертів, а соціальна інженерія стає дедалі витонченішою: використовуються створені за допомогою штучного інтелекту «дівпфейки», підробка служб технічної підтримки, викрадені особисті дані та багатоетапний фішинг, спрямований як на людей, так і на машини, оскільки злочинці використовують штучний інтелект як основний інструмент, а не як допоміжний засіб... У відповідь на це компанії звертаються до загальновизнаних стандартів безпеки та сертифікатів, посилюють заходи з безпечної розробки та управління ризиками постачальників, щоб відповідати вимогам таких рамок, як NIS2, а також інвестують у системи виявлення загроз у режимі реального часу — серед наведених прикладів можна згадати компанію Deutsche Telekom, яка щодня використовує штучний інтелект для аналізу величезних обсягів сигналів безпеки. Це підкреслює зростаючий консенсус щодо того, що підприємства повинні забезпечити свою «готовність до майбутнього» та ставитися до кібербезпеки як до стратегічного пріоритету, перш ніж інцидент змусить їх вирішувати це питання».
(Jordan Finkle. Cybersecurity is now where the real heists happen – but are companies ready? // DIGITAL JOURNAL INC. (<https://www.digitaljournal.com/tech-science/cybersecurity-is-now-where-the-real-heists-happen-but-are-companies-ready/article>). 12.05.2026).

«Microsoft попереджає, що захист від DDoS-атак перетворився на проблему проектування систем та довіри, а не лише на мережеву проблему, оскільки штучний інтелект суттєво знизив бар'єр для здійснення складних багатовекторних атак, які дедалі частіше націлені на додатки та API, а не лише на перевантаження пропускну здатності. Microsoft повідомляє про значне зростання активності DDoS-атак на Bing та інші сервіси протягом останніх п'яти-

шести років, зазначаючи, що з середини березня 2024 року обсяг DDoS-атак на рівні мережі зріс приблизно до 4 500 атак на день до червня 2024 року, а також відбувся перехід до більш прихованих технік на рівні додатків, які важче відрізнити від законної поведінки користувачів. Зловмисники також розширюють ботнети, використовуючи споживчі пристрої Інтернету речей (IoT), неправильно налаштовані хмарні робочі навантаження і навіть легітимну хмарну інфраструктуру для генерації трафіку, що зливається з нормальними моделями, при цьому все частіше атакуються периферійні сервіси, такі як CDN та маршрутизація «front-door», оскільки вони знаходяться між користувачами та додатками...

Головний висновок з практичного досвіду полягає в тому, що навіть блокування більшої частини шкідливого трафіку може виявитися недостатнім, якщо решта трафіку потрапить у «вузьке місце» системи. Тому організаціям слід розглядати DDoS-атаки як звичайну експлуатаційну ситуацію та застосовувати багаторівневий захист: поєднувати базові засоби контролю (обмеження пропускної здатності, геофенсінг, виявлення аномалій) із сучасними технологіями ідентифікації та аналізом поведінкових сигналів (зокрема JA4), високим рівнем операційної прозорості та багаторівневим захистом на периферійному та прикладних рівнях. Microsoft підкреслює роль хмарних засобів захисту та телеметрії — таких як Azure DDoS Protection для пом'якшення атак на рівні мережі та Azure Web Application Firewall на Azure Front Door для централізованої перевірки, керування правил, геофільтрації та контролю ботів — але наголошує, що ці інструменти повинні поєднуватися з найкращими практиками щодо додатків та архітектури. Компанія пропонує прогресію зрілості від «відкритих» служб із прямим походженням та реактивним пом'якшенням, через базове об'ємне екранування на основі CDN та інтелектуальне фільтрування на основі WAF, до стійких архітектур, що включають перегородки, автоматичні вимикачі, скидання навантаження та автоматичне вмикання/вимикання функцій, і, зрештою, до автономних захисних засобів на основі штучного інтелекту з прогнозним моделюванням, відмовостійкістю з використанням декількох CDN та превентивним масштабуванням...

Ключовою темою є «плавне погіршення якості роботи»: стійкість не означає повної відсутності наслідків, а полягає у свідомому наданні пріоритету основним користувацьким потокам, тимчасовому обмеженні дорогих або необов'язкових функцій, застосуванні багаторівневих сценаріїв роботи під навантаженням на основі сигналів довіри, а також у чіткому інформуванні користувачів під час збоїв. Загальний висновок полягає в тому, що сучасна стійкість до DDoS-атак вимагає інтегрованих засобів контролю на рівні мережі, периферії та додатків, а також заздалегідь перевірених оперативних інструкцій, які забезпечують працездатність критично важливих сервісів навіть у разі, коли частина трафіку атаки неминуче проривається». (*Kumar Srinivasamurthy. Defending consumer web properties against modern DDoS attacks // Microsoft (<https://www.microsoft.com/en-us/security/blog/2026/05/12/defending-consumer-web-properties-against-modern-ddos-attacks/>). 12.05.2026*).

«Socket і StepSecurity повідомляють, що популярний пакет `npm node-ipc` — бібліотека для міжпроцесної комунікації на JavaScript, яка щотижня завантажується понад 822 000 разів — знову зазнав атаки: у трьох нещодавно опублікованих версіях (9.1.6, 9.2.3 та 12.0.1) містять замаскований код для викрадення облікових даних та створення бекдору, що є другим серйозним інцидентом у ланцюжку постачання, пов'язаним із цим пакетом, з 2022 року. Дослідник у галузі безпеки Іан Ал (Ian Ahl) пов'язав цю уразливість із ймовірним захопленням давно неактивного облікового запису розробника («atiertant») після того, як зловмисники нібито отримали контроль над доменом електронної пошти для відновлення доступу (atlantis-software[.]net), термін дії якого закінчився, що дозволило їм виконати стандартне скидання пароля `npm` та отримати прихований доступ до публікації... Шкідливий код додається лише до файлу `node-ipc.cjs` (точка входу CommonJS) у вигляді зашифрованої функції, що виконується негайно, залишаючи модуль ESM чистим, тому проекти, які імпортують його за допомогою `require("node-ipc")`, наражаються на ризик. Під час завантаження модуля корисне навантаження запускає відокремлений процес, визначає відбиток хоста та збирає облікові дані та секрети з понад 100 цільових шаблонів — включаючи хмарні ключі (AWS/Azure/GCP), конфігурації Kubernetes та Docker, SSH-ключі, токени `npm`, облікові дані GitHub/GitLab, секрети Terraform та `.env`, історії оболонок та дані macOS Keychain — потім упаковує дані в `gzip`-архів у тимчасовому каталозі та виводить їх через DNS TXT-запити (не HTTP), використовуючи домен, схожий на Azure (sh[.]azurestaticprovider[.]net), та зону `bt[.]node[.]js`, що може створювати десятки тисяч TXT-запитів для одного архіву, роблячи сплески DNS TXT-трафіку ключовим індикатором виявлення. Зловмисники також змінили час створення всіх архівних файлів на 26 жовтня 1985 року — це характерний криміналістичний маркер, що дозволяє виявляти кешовані або дзеркальні копії...» (*Guru Baran. node-ipc npm Package with 822K Weekly Downloads Compromised in Supply Chain Attack // Cyber Security News (https://cybersecuritynews.com/node-ipc-npm-package-compromised/). 14.05.2026*).

«Компанія Jaguar Land Rover (JLR), що належить індійській Tata Motors, повідомила про чистий збиток у розмірі 244 млн фунтів стерлінгів (328 млн доларів) за фінансовий рік, що закінчився 31 березня, після того як її виторг впав майже на 21% до 22,9 млрд фунтів стерлінгів на тлі численних труднощів. Як і інші автовиробники, компанія постраждала від імпортних мит США, що змусило її призупинити поставки автомобілів до Сполучених Штатів у квітні, отримавши лише тимчасове полегшення, коли торговельна угода між Великобританією та США послабила тиск у липні. Ця перерва була затьмарена кібератакою, яка змусила JLR зупинити виробництво на понад місяць, що коштувало, за оцінками, 196 млн фунтів стерлінгів, а також погіршенням ринкових умов у Китаї та скороченням обсягів виробництва через виведення з обігу старих моделей напередодні випуску нових... Незважаючи на складний рік, компанія відзначила ознаки відновлення на початку цього року та заявила, що залишається впевненою у своїх силах і стійкою напередодні наступного року, незважаючи на

поточні геополітичні, інфляційні та регуляторні виклики...» (*US tariffs, cyberattack drive Jaguar Land Rover into loss // France 24* (<https://www.france24.com/en/live-news/20260514-us-tariffs-cyberattack-drive-jaguar-land-rover-into-loss>). 14.05.2026).

«Сучасні кіберзагрози дедалі частіше базуються на підході «identity-first»: зловмисники все менше зосереджуються на прориві периметра захисту, а все більше — на компрометації користувачів, облікових записів служб та систем автентифікації шляхом викрадення облікових даних та перехоплення сеансів, зокрема шляхом обходу багатофакторної автентифікації (MFA), атак на основі «втоми від push-повідомлень» та підміни SIM-карт, оскільки викрадена ідентичність дозволяє їм діяти як легітимні користувачі в середовищах, що базуються на системах доступу на основі дозволів... Водночас атаки на ланцюг постачання стають дедалі більш непрямими та масштабними, оскільки зловмисники компрометують надійних постачальників, хмарних провайдерів, постачальників керованих послуг, оновлення програмного забезпечення, залежності від відкритого програмного забезпечення та навіть розробницькі конвеєри й інструменти збірки, використовуючи довірчі відносини, які традиційні засоби захисту можуть не виявити на ранній стадії; це змушує організації інтегрувати контроль за ланцюгом постачання в систему управління ризиками шляхом постійного моніторингу постачальників, перевірки походження та застосування практик SBOM (специфікації програмного забезпечення), посилення контролю доступу сторонніх осіб, а також спільного планування реагування на інциденти... «Тіньові IT» також еволюціонують у «тіньовий ШІ», коли співробітники підключають несанкціоновані інструменти штучного інтелекту та автономні агенти до корпоративних систем і конфіденційних даних без належного контролю, що потенційно створює вразливості через код, написаний ШІ, автономні дії та непрозорий вплив на прийняття рішень, що робить необхідним посилення управління, моніторингу та постійного супроводу співробітників. Програми-вимагачі стали завдавати ще більшої шкоди завдяки подвійному шантажу, коли загрози викрадення та витоку даних створюють регуляторні та репутаційні збитки, які неможливо усунути лише за допомогою резервних копій, що вимагає швидшого виявлення, автоматизованого локалізування та скоординованого реагування на інциденти, яке охоплює як відновлення системи, так і наслідки порушення безпеки... Загалом, кампанії з проникнення перетворилися на багатоетапні, адаптивні, міждоменні операції, що поєднують фішинг, викрадення облікових даних, експлойти VPN та компрометацію ланцюгів постачання, поширюються по горизонталі в хмарних середовищах та середовищах SaaS і можуть тривати тижнями, перш ніж спричинити серйозні наслідки. Тому ефективне управління ризиками кібербезпеки у 2026 році вимагає комплексного аналізу шляхів доступу, багаторівневої системи захисту, надійних планів реагування та відновлення, а також системи управління, яка встигає за стрімкими змінами в технологіях та загрозах». (*Ralph Tkatchuk. Rising To The Challenges Of Cybersecurity Risk Management In 2026 // Minutehack* (<https://minutehack.com/news/rising-to-the-challenges-of-cybersecurity-risk-management-in-2026>). 15.05.2026).

«Два масштабні хакерські напади на DeFi у квітні, які, за загальним визнанням, пов'язані з угрупованнями, пов'язаними з Північною Кореєю, призвели до виведення майже 600 мільйонів доларів із протоколу Drift (285 мільйонів доларів) та Kelp DAO (292 мільйони доларів); слідчі вважають, що ці інциденти свідчать про дедалі витонченіші методи вибору цілей та розробки експлойтів, що базуються на штучному інтелекті. Атака на Drift стала результатом багатомісячної соціальної інженерії, під час якої хакери видавали себе за компанію, що займається кількісною торгівлею, щоб отримати схвалення шкідливих транзакцій, а потім використовували сфабрикований токен із завищеною історією торгів як заставу, щоб вивести реальні активи приблизно за 12 хвилин, що призвело до падіння загальної вартості заблокованих активів Drift з 550 мільйонів доларів до менше ніж 300 мільйонів доларів і спричинило закриття та запланований перезапуск за підтримки рятувальної операції на суму приблизно 148 мільйонів доларів, очолюваної Tether, тоді як пов'язаний проект Carrot, пізніше припинив свою діяльність... Зловмисники скористалися вразливістю, пов'язаною з єдиним верифікатором у міжланцюговому мості, та викрали обгорнутий ефір, а наслідки поширилися по всій екосистемі, коли зловмисники внесли близько 200 мільйонів доларів отриманих коштів як заставу на Aave, що спричинило кризу довіри, яка за два дні призвела до відтоку близько 9 мільярдів доларів з Aave та зниження загальної вартості заблокованих коштів у секторі DeFi-кредитування на понад 13 мільярдів доларів за 48 годин, підкресливши системну вразливість DeFi, де незворотні транзакції та взаємопов'язані заставні відносини можуть перетворити одне порушення на ланцюгову реакцію... Компанія TRM Labs, що спеціалізується на криміналістичному аналізі блокчейнів, заявила, що ці два пограбування становлять 76% збитків від хакерських атак на криптовалюти за 2026 рік, а декілька дослідників повідомили Bloomberg, що рекордний квітневий сплеск кількості зловживань у сфері DeFi (приблизно 28–30 випадків) свідчить про те, що зловмисники дедалі частіше використовують загальнодоступні інструменти штучного інтелекту, щоб скоротити час виявлення вразливостей з місяців до днів або годин. Компанія Anthropic попередила, що багато минулих атак на блокчейн могли бути здійснені автономно за допомогою агентів штучного інтелекту, і приховала свою потужну модель Mythos, обмеживши доступ до проекту Project Glasswing, що посилює занепокоєння галузі щодо того, що більш потужні моделі — у разі їх витоку або копіювання — можуть ще більше прискорити атаки, хоча немає доказів того, що хакери у квітні використовували Mythos... У відповідь на це компанії вивчають можливості безперервного сканування мереж, застосування «запобіжників» для транзакцій та запровадження більш жорстких систем управління ризиками застави, що враховують питання кібербезпеки. Однак деякі експерти стверджують, що одних лише захисних заходів може бути недостатньо для протистояння супротивникам, які мають державну підтримку та використовують штучний інтелект, і закликають до більш рішучих заходів з відстеження та повернення викрадених коштів». *(Alina Maria Stan. AI gave North Korean hackers a \$600 million month. DeFi is still working out how to respond //*

Cogneve, INC. (<https://thenextweb.com/news/ai-crypto-hacking-defi-north-korea-april-exploits>). 15.05.2026).

«6-7 травня 2026 року офіційний веб-сайт JDownloader зазнав злом, і протягом цього періоду зловмисники замінили посилання на «Альтернативний інсталятор для Windows» та інсталятор для оболонки Linux на шкідливі версії, тоді як інші канали розповсюдження (macOS, JAR, Flatpak, Winget та Snap) залишилися неушкодженими. Було виявлено, що шкідливі інсталятори для Windows розгортали троян для віддаленого доступу на базі Python, але користувачі, які просто оновили існуючу інсталяцію протягом цього періоду, не зазнали впливу... Розробники підтвердили інцидент 7 травня, відключили сайт для проведення розслідування та відновили його роботу 8–9 травня після встановлення виправлень безпеки, посилення конфігурації серверів та повторної публікації перевірених посилань на чисті інсталяційні файли; вони пов'язали злом із незахищеною уразливістю CMS, яка дозволила зловмисникам змінювати списки контролю доступу без аутентифікації. Користувачам, які завантажили інсталятори під час періоду компрометації, рекомендується перевірити файли, переконавшись, що інсталятори мають правильний цифровий підпис «AppWork GmbH», виконати повне сканування на наявність шкідливого програмного забезпечення та звернути увагу, що такі інструменти, як Malwarebytes, блокують домени, з якими RAT намагався встановити зв'язок». (**Pieter Arntz. Attackers replaced JDownloader installer downloads with malware // Malwarebytes** (<https://www.malwarebytes.com/blog/news/2026/05/attackers-replaced-jdownloader-installer-downloads-with-malware>). 15.05.2026).

«...З нагоди Національного дня обізнаності про шахрайство щодо людей похилого віку ФБР опублікувало важливе попередження, в якому наголошується, що особи віком понад 60 років стали основною мішенню для кіберзлочинців. У 2025 році Центр прийому скарг на інтернет-злочини ФБР зареєстрував понад 200 000 скарг від людей похилого віку, що становить зростання на 37%, а фінансові збитки стрімко зросли до 7,7 млрд доларів. Шахраї націлюються на цю демографічну групу не тільки через їхні накопичені заощадження, а й використовуючи психологічні фактори, такі як самотність та вищий рівень довіри порівняно з молодшими поколіннями...

До найпоширеніших шахрайських схем належать випадки, коли злочинці видають себе за родичів, які опинилися у скрутному фінансовому становищі, а також підроблені співробітники технічної підтримки, романтичні шахраї та організатори фальшивих благодійних акцій. Для боротьби з цими загрозами ФБР закликає людей похилого віку та їхні родини звертати увагу на певні тривожні ознаки: вимоги зберігати таємницю, штучно створене відчуття терміновості та прохання про оплату за допомогою банківських переказів або подарункових карток. Головна порада агентства щодо забезпечення безпеки — повністю ігнорувати небажані повідомлення, особливо дзвінки з невідомих номерів, оскільки

тривале спілкування лише збільшує ймовірність успіху шахрайства». (*Davey Winder. Seniors Targeted—FBI Issues Cyber Attack Advice For The Over 60s // Forbes Media LLC. (<https://www.forbes.com/sites/daveywinder/2026/05/16/seniors-targeted-fbi-issues-cyber-attack-advice-for-the-over-60s/>). 16.05.2026*).

«Атаки з захоплення облікових записів (АТО) становлять серйозну і дедалі більшу загрозу для сучасного бізнесу, часто виявляючись небезпечнішими за традиційні кібератаки, оскільки ґрунтуються на зловживанні законними обліковими даними, а не на явних порушеннях безпеки системи. На відміну від атак, що використовують шкідливе програмне забезпечення або вразливості програмного забезпечення, АТО відбувається тоді, коли неавторизований зловмисник отримує дійсний доступ до робочого облікового запису, що дозволяє йому діяти всередині організації, видаючи себе за «звичайного» користувача. Відсутність вторгнення в периметр ускладнює виявлення, оскільки команди з безпеки часто зосереджуються на технічних несправностях, а не на зловживанні обліковими даними. Наслідки є серйозними: дослідження показують, що 83% організацій зазнали принаймні однієї атаки АТО протягом останнього року, а порушення безпеки даних, пов'язані з захопленням облікових записів, спричиняють середні збитки у розмірі майже 5 мільйонів доларів...

Зловмисники зазвичай використовують такі методи, як «наповнення облікових даних» (використання паролів, що повторно використовуються з попередніх витоків даних), а також фішинг, підміну SIM-карт і «розпилення паролів», щоб отримати доступ. Отримавши доступ, вони можуть використовувати ці облікові записи для перегляду внутрішніх повідомлень, перенаправлення платежів, експорту конфіденційних файлів або горизонтального переміщення в інші підключені додатки. Оскільки одна скомпрометована ідентичність може надати доступ до важливих систем, таких як HR, система розрахунку заробітної плати та CRM-інструменти, підприємствам необхідно змінити свої стратегії виявлення, зосередившись на виявленні аномалій у поведінці. До основних попереджувальних сигналів належать незвичайні шаблони входу, несподівані зміни паролів, зміни правил поштової скриньки та доступ до конфіденційних інструментів, що виходять за межі звичайних обов'язків співробітника.

Для боротьби з цими загрозами підприємствам потрібен структурований план реагування, який передбачає першочергове локалізування ураженого облікового запису, ретельну оцінку масштабів збитків та зобов'язання щодо посилення безпеки на основі висновків, зроблених за результатами інциденту. Зрештою, для зменшення ризику несанкціонованого використання облікових даних (АТО) необхідно формувати культуру безпеки ідентифікації, в якій дисципліноване управління доступом має пріоритет над зручністю. Організації можуть значно знизити свій профіль ризику, впровадивши корпоративні менеджери паролів, запровадивши обов'язкове використання паролів, стійких до фішингу, запровадивши надійну багатофакторну автентифікацію та використовуючи моніторинг даркнету для виявлення вразливих облікових даних до того, як ними

зможуть скористатися зловмисники. Інтегруючи ці практики, компанії можуть краще захистити модель довіри на основі ідентифікації, на якій базуються сучасні робочі середовища, що ставлять цифрові технології на перше місце». (*Kate Menzies. How businesses can detect and prevent account takeover attacks // Proton AG (<https://proton.me/business/blog/account-takeover-attacks>). 19.05.2026*).

«Сектор роздрібної торгівлі товарами класу «люкс» є особливо привабливою мішенню для кіберзлочинців, оскільки він обслуговує заможних клієнтів та VIP-клієнтів і зберігає надзвичайно конфіденційні дані. Цю реальність підкреслює нещодавня хвиля атак, що зачепила провідні бренди класу «люкс» та преміум-сегмента, такі як Louis Vuitton, Cartier, Gucci, Balenciaga та Alexander McQueen. Хоча кіберінциденти в роздрібній торгівлі вже спричиняють значні операційні, юридичні та репутаційні наслідки, бренди класу «люкс» стикаються з посиленими ризиками, оскільки записи про клієнтів можуть розкривати не лише особисті дані та контактну інформацію, а й детальну історію покупок, рівень витрат, особисті вподобання, звички щодо дарування подарунків та потенційно конфіденційні стосунки, а оприлюднення адрес доставки додому може стати проблемою особистої безпеки для знаменитостей або заможних клієнтів. Програми лояльності та CRM ще більше посилюють цей вплив, об'єднуючи довгострокові дані про поведінку в детальні профілі, які, у разі витоку, можуть сприяти цілеспрямованим злочинам та витонченому соціальному інжинірингу...

Програмне забезпечення для вимагання викупу залишається головною загрозою, часто поєднуючись із викраденням даних та шантажем на кшталт «плати або ми оприлюднимо інформацію», також соціальна інженерія (зокрема, вішинг та видавання себе за співробітників служби IT-підтримки) та компрометація ланцюга постачання через надійних сторонніх постачальників технологій стають дедалі ефективнішими шляхами проникнення. Відповідно до британського GDPR, роздрібні продавці товарів класу «люкс» повинні швидко оцінювати серйозність порушення та виконувати зобов'язання щодо повідомлення — подаючи звіт до ICO протягом 72 годин, якщо це необхідно (стаття 33), та повідомляючи осіб без зайвої затримки, коли ризик є високим (стаття 34) — але оцінка ризику значною мірою залежить від контексту і може бути підвищеною для VIP-клієнтів, оскільки витік телефонних номерів, електронних адрес, адрес та історії покупок може уможливити видавання себе за іншу особу та цілеспрямоване шахрайство. Як результат, бренди класу «люкс» повинні планувати не лише те, чи повідомляти, а й те, як це зробити таким чином, щоб відобразити особистий, керований консультантами характер відносин із клієнтами найвищого рівня та запропонувати практичну підтримку, що виходить за межі стандартного моніторингу кредитоспроможності.

З оперативної точки зору кібератака може вивести з ладу системи торгових точок, зашифрувати платформи електронної комерції та порушити роботу систем управління запасами, виконання замовлень і комунікації з клієнтами, що матиме особливо серйозні наслідки, якщо вона відбудеться в пікові торговельні періоди, такі як передріздвяний час, великі розпродажі, тиждень моди або гучні рекламні вихідні. Стратегія комунікації стає критичним моментом у прийнятті рішень,

оскільки порушення, що стають відомими громадськості, можуть змусити розкрити інформацію раніше, ніж це передбачено регуляторними термінами, а формулювання та послідовність мають значення для довіри до бренду — особливо для VIP-клієнтів, яким може знадобитися безпосередній контакт перед публічними заявами. Необхідно зміцнювати стійкість за допомогою залучення керівництва, посилення контролю над ланцюгом поставок та договірних гарантій з обробниками даних (особливо постачальниками програм лояльності/CRM), перевірених планів реагування на інциденти та відновлення резервних копій, відповідного кіберстрахування, а також завчасного планування оцінки ризиків порушення безпеки, орієнтованої на VIP-клієнтів, та надсилання повідомлень, спираючись на рекомендації NCSC, такі як служба раннього попередження, вимоги Cyber Essentials для постачальників та Рамка кібероцінки». *(Ellie Ludlam, Harriet McCarthy. Cyber: protecting the brand, not just the bag // The Global Legal Post (<https://www.globallegalpost.com/news/cyber-protecting-the-brand-not-just-the-bag-1668208266>). 27.05.2026).*

«Компанія Foxconn, найбільший у світі виробник електроніки, що має понад 230 заводів у 24 країнах та річний дохід, який у 2025 році перевищить 260 мільярдів доларів, зазнала кібератаки, що призвела до перебоїв у роботі низки північноамериканських заводів. Компанія задіяла свої протоколи реагування на інциденти та вжила оперативних заходів для забезпечення безперебійності виробництва, а згодом повідомила, що постраждалі заводи відновлюють нормальний виробничий процес. Відповідальність за атаку взяла на себе група Nitrogen ransomware, яка стверджує, що викрала 8 терабайтів даних і понад 11 мільйонів документів, включаючи конфіденційні технічні матеріали, що належать таким великим технологічним компаніям, як Apple, AMD, Google, Intel і Nvidia, а також потенційно чутливу інформацію, що стосується Hewlett Packard Enterprise, JPMorgan Chase та інших... Група опублікувала зразки даних, зокрема схеми виробів, проекти друкованих плат, документацію щодо серверних платформ, технологічні процеси та банківські виписки, як доказ злом. Характер викраденої інформації є особливо серйозним, оскільки вона може дозволити зловмисникам виявляти вразливості продуктів, надати конкурентам можливість реверс-інжинірингу виробів або створення підробок, а також потенційно сприяти промислому шпигунству з боку суб'єктів, що діють за підтримки держави. Nitrogen, вперше виявлена у 2023 році, є групою, що займається подвійним вимаганням викупу, яка діє як операція «вимагання-як-послуга», створена з використанням витоку коду-конструктора Conti 2, і зазвичай поширює шкідливе програмне забезпечення за допомогою методів оптимізації пошукових систем та шкідливих підробок легальних програмних інструментів... Експерти з кібербезпеки зазначають, що методи, використані під час атаки, зокрема шкідлива реклама, завантаження DLL-файлів з сторонніх джерел та використання Cobalt Strike, є добре відомими та виявляються сучасними програмами безпеки, що ставить під сумнів ефективність існуючих заходів безпеки Foxconn. Компанія Foxconn не підтвердила, чи має намір сплатити викуп, а також не повідомила, як саме стався

злом. Це далеко не перший випадок, коли компанія стикається з програмним забезпеченням-вимагачем. У 2024 році її дочірня компанія Foxsemicon зазнала атаки LockBit, у 2022 році її завод у Тіхуані також постраждав від LockBit, а у 2020 році група DoppelPaymer атакувала її завод у Сьюдад-Хуаресі, зашифрувавши понад 1 200 серверів, викравши понад 100 гігабайтів даних, знищивши приблизно 30 терабайтів резервних копій та вимагаючи викуп у розмірі близько 34 мільйонів доларів. Повторні атаки на Foxconn підкреслюють постійну та зростаючу загрозу, яку програмне забезпечення для вимагання викупу становить для великих виробничих ланцюгів постачання та технологічного сектору в цілому». *(Alicia Hope. Cyber Attack by Nitrogen Ransomware Hits Foxconn, Disrupting North American Operations // Rezonen Pte. Ltd. (<https://www.cpomagazine.com/cyber-security/cyber-attack-by-nitrogen-ransomware-hits-foxconn-disrupting-north-american-operations>). 22.05.2026).*

«Нещодавні інциденти з кібербезпекою, пов'язані з Google та GitHub, продемонстрували зростаючу витонченість атак на основі штучного інтелекту та загроз у ланцюжку постачання програмного забезпечення. Компанія Google успішно заблокувала складну кібератаку на основі штучного інтелекту, спрямовану проти її служби двофакторної аутентифікації. За даними групи Threat Intelligence Group компанії, зловмисники використовували шкідливе програмне забезпечення, створене за допомогою штучного інтелекту, під назвою «PROMPTSPY», яке, як повідомляється, використовувало інструменти штучного інтелекту Gemini для автоматизації та масштабування експлуатації вразливостей серверів. Шкідливе програмне забезпечення було розроблено для обходу систем аутентифікації та компрометації облікових записів користувачів, використовуючи слабкі або застарілі конфігурації. Google швидко вжила заходів для локалізації загрози та закликала організації регулярно оновлювати своє програмне забезпечення, посилювати заходи з кібербезпеки та переходити на більш безпечні методи аутентифікації, такі як біометрична верифікація...

У ході окремої масштабної атаки на ланцюжок постачання дослідники з SafeDer виявили, що шкідливе ПЗ «Megalodon» заразило понад 5 500 репозиторіїв GitHub. Атака, визначена як кампанія «Poisoned Pipeline Execution», вперше з'явилася 18 травня 2026 року і була офіційно визнана GitHub через два дні. Вона спеціально націлена на автоматизовані робочі процеси в репозиторіях, що дозволяє зловмисникам вводити шкідливий код під час виконання конвеєра і потенційно поширюватися по численних програмних проєктах без негайного виявлення...

Обидва випадки свідчать про те, що кіберзлочинці дедалі частіше використовують штучний інтелект для автоматизації атак та націлювання на критичні етапи життєвого циклу розробки програмного забезпечення. Експерти з безпеки застерігають, що ці події підкреслюють нагальну необхідність посилення заходів кібербезпеки, підвищення рівня захисту ланцюгів постачання та посилення пильності, оскільки загрози, пов'язані зі штучним інтелектом, продовжують стрімко розвиватися». *(Naveen Goud. Google blocks AI Powered Cyber Attack on 2FA and Megalodon Malware attack on GitHub // Cybersecurity Insiders*

(<https://www.cybersecurity-insiders.com/google-blocks-ai-powered-cyber-attack-on-2fa-and-megalodon-malware-attack-on-github/>). 26.05.2026).

«Тисячі шкіл та університетів по всьому світу зазнали перебоїв у роботі внаслідок кібератаки на компанію Instructure — постачальника широко використовуваної системи управління навчанням Canvas. Цей випадок став суворим нагадуванням про те, що освітні установи стали головними мішенями для кіберзлочинців. У міру того як освіта дедалі більше залежить від цифрових платформ, хмарних сервісів та сторонніх постачальників, кіберризики перейшли від поодиноких зломів до складних атак на ланцюги постачання, які можуть швидко поширюватися на цілі мережі. Згідно з дослідженням BlueVoyant, 99% австралійських організацій зазнали негативного впливу від порушення безпеки сторонніх постачальників або ланцюга поставок протягом минулого року, проте лише 30% з них запровадили або оптимізували програми управління ризиками сторонніх постачальників (TPRM)...

Ефективне TPRM вимагає від організацій оцінювати та постійно контролювати постачальників протягом усього життєвого циклу — від моменту укладення договору до припинення співпраці — щоб гарантувати дотримання ними суворих стандартів безпеки, конфіденційності та відмовостійкості. Швидке поширення штучного інтелекту ще більше ускладнило ситуацію з загрозами: депфейки, фішинг на основі штучного інтелекту, атаки з піддробкою особи та «отруєння» даних стають дедалі поширенішими та важчими для виявлення. У таких умовах традиційних періодичних оцінок постачальників вже недостатньо.

Керівники освітніх установ повинні перейти до проактивного підходу, орієнтованого на забезпечення стійкості, який передбачає постійний моніторинг, обмін інформацією про загрози, надійну аутентифікацію, перевірку ланцюга постачання програмного забезпечення та чітке управління. Кіберризики, пов'язані зі сторонніми організаціями, більше не можна розглядати лише як питання закупівель чи дотримання нормативних вимог. В епоху стрімкої цифровізації безпека та стійкість освітніх установ значною мірою залежать від рівня кібербезпеки кожного підключеного постачальника та постачальника послуг...»
(Kash Sharma. *Cyber risk in education now extends far beyond the school gate* // TechDay (<https://securitybrief.com.au/story/cyber-risk-in-education-now-extends-far-beyond-the-school-gate>). 28.05.2026).

«GitHub підтвердив, що хакер викрав щонайменше 3 800 внутрішніх репозиторіїв; відповідальність за це взяла на себе відома злочинна група, яка виставила викрадені дані на продаж на підпільному форумі. Злом стався через те, що розробник використовував шкідливе розширення Visual Studio Code, а саме Nx Console, яке було заражене на короткий час за день до того, як про інцидент стало відомо. GitHub заявив, що не виявив жодних ознак того, що дані клієнтів постраждали, і негайно видалив заражене розширення. Відповідальність за злом взяла на себе TeamPCP — відносно нова, але ефективна хакерська група, яка

раніше використовувала вразливості відкритого програмного забезпечення та викрадала облікові дані з різних інструментів і платформ. Група також співпрацює з Lapsus\$ з метою продажу викрадених репозиторіїв, спочатку вимагаючи 50 000 доларів, але ціна з того часу зросла до 95 000 доларів, оскільки продажі перейшли на портал Lapsus...

Хоча доказів витоку даних користувачів немає, експерти застерігають, що цей інцидент може мати більш серйозні наслідки. Інженер з безпеки Борис Ціпот наголосив, що злом GitHub несе ризики, які виходять за межі безпосередньої крадіжки репозиторіїв, зокрема, це може призвести до витоку вихідного коду, конфіденційної інформації та внутрішньої логіки розробки, які можуть бути використані в майбутніх атаках або схемах вимагання викупу. Він порадив розробникам запровадити надійну аутентифікацію, обмежити доступ сторонніх осіб, регулярно оновлювати облікові дані та ставитися до середовищ розробки як до критично важливих активів.

Інцидент стався на тлі загальних побоювань щодо безпеки та надійності GitHub, включаючи нещодавні перебої в роботі та вразливості. GitHub має проблеми з безперебійністю роботи: останні дослідження показують, що за останні три місяці доступність становила лише близько 85%, а такі перебої, як шестигодинний простой Elasticsearch, викликають сумніви серед користувачів. Крім того, незабаром після порушення було виявлено критичну вразливість, яка дозволяла зловмисникам отримувати доступ до репозиторіїв за допомогою простої команди, що ще більше підкреслило операційні проблеми платформи...

Цей інцидент також підкреслює постійну загрозу з боку зловмисних розширень з відкритим кодом, які раніше використовувалися для зараження середовищ розробників шкідливим програмним забезпеченням та криптомайнерами. Такі експерти, як Ілкка Турунен, попереджають, що розробники зараз є головними мішенями в атаках на ланцюжок постачання, оскільки зловмисники використовують надійні інструменти, залежності та облікові дані для проникнення в організації. Турунен наголосив на необхідності для організацій отримати прозорість та впровадити превентивні заходи контролю у всьому робочому процесі розробників — не обмежуючись лише реактивним виявленням — для ефективного захисту від швидких загроз на рівні екосистеми.

Тим часом TeamPSR заявила, що продасть викрадені репозиторії за не менше ніж 50 000 доларів, але може оприлюднити дані безкоштовно, якщо не знайдеться покупець. Джейсон Сороко з Sectigo підкреслив, що такі порушення загрожують фундаментальній довірі до централізованих репозиторіїв коду, закликаючи керівників служб безпеки розглянути децентралізовані моделі хостингу та розробки на основі принципу «нульової довіри». Загалом, цей інцидент слугує суворим нагадуванням про зростаючу складність та вразливість сучасного ланцюга постачання програмного забезпечення, підкреслюючи необхідність комплексних стратегій безпеки». (*Scott Ikeda. GitHub Hacker Claims Security Breach Involved About 4,000 Internal Repositories, Takes Bids on Stolen Data // Rezonen Pte. Ltd. (<https://www.cpomagazine.com/cyber-security/github-hacker-claims-security-breach-involved-about-4000-internal-repositories-takes-bids-on-stolen-data/>). 25.05.2026*).

«Хакерство, по суті, — це мистецтво змусити систему робити те, для чого вона не була призначена, форма «нестандартного мислення», яка може бути як творчою, так і злочинною. Дотепер кіберзахист ґрунтувався на двох основних припущеннях: що люди діють у рамках соціальних та правових механізмів контролю (контракти, аудити, репутаційні та правові наслідки) і що звичайне програмне забезпечення є функціонально фіксованим, виконуючи обмежені робочі процеси без творчості. Атаки досягають успіху завдяки використанню розбіжностей між передбачуваною та фактичною поведінкою системи, або шляхом викрадення чи примусу до використання привілеїв довірених осіб, або шляхом зловживання недоліками програмного забезпечення та інтерфейсів...»

Агентний ІІІ підважує обидва ці припущення, оскільки він здатний міркувати, планувати, повторювати спроби, поєднувати кроки, писати код, використовувати АРІ та інструменти, а також шукати альтернативні шляхи досягнення мети — фактично поводячись як мислитель, здатний до дивергентного мислення, але з машинною швидкістю і без тих моральних та соціальних обмежень, які зазвичай регулюють наміри людини. Це поєднання творчого вирішення проблем, привілейованого доступу та відсутності людської відповідальності створює «ідеальну форму хакера», навіть якщо агент за своєю суттю не є зловмисним. «Момент Mythos» подається як доказ того, що ця зміна вже не є теоретичною, з посиланням на твердження, що Mythos Preview від Anthropic виявив тисячі серйозних вразливостей, поєднав експлойти ядра Linux для отримання повного контролю та створив експлойти за лічені години, а не тижні, як це могло б знадобитися експертам. Висновок полягає в тому, що в епоху агентів організації повинні припинити намагатися виводити наміри і замість цього розглядати привілеї як контрольовану змінну, застосовуючи принципи Zero Trust: жорстко контролюючи дозволи, обмежуючи доступність за допомогою мікросегментації та обмежуючи те, що може робити будь-який користувач, ідентичність, робоче навантаження, агент або інструмент, коли розбіжне мислення неминуче знаходить непередбачувані шляхи». (*Satyam Tyagi. The Mythos Moment: When Hacking Tools Move from “Functional Fixedness” to “Divergent Hacker Thinking” // Techstrong Group Inc. (<https://securityboulevard.com/2026/05/the-mythos-moment-when-hacking-tools-move-from-functional-fixedness-to-divergent-hacker-thinking/>). 12.05.2026*).

«Північнокорейські хакери, пов'язані з групою Lazarus, застосовують більш приховану тактику, що базується на ланцюжку постачання програмного забезпечення: вони ховають шкідливе ПЗ у Git-хуках — автоматизованих скриптах, які запускаються під час звичайних дій розробників — замість того, щоб покладатися на фішинг або шкідливі посилання. Ця техніка є частиною тривалої операції «Contagious Interview», в

рамках якої зловмисники видають себе за рекрутерів на таких сайтах, як LinkedIn, надсилають розробникам тест на кодування, розміщений у репозиторії GitHub, і запускають інфікування, щойно жертва клонує репозиторій та починає з ним працювати... Дослідники з OpenSourceMalware виявили шкідливий код, вбудований у каталог .github репозиторію як хук pre-commit, що означає: він запускається, коли розробник намагається зафіксувати зміни, ще до запису коміту, і зазвичай не викликає підозр, оскільки репозиторії для тестування завдань рідко піддаються ретельній перевірці. Після запуску хук визначає операційну систему та зв'язується з віддаленим сервером, замаскованим під легітимну інфраструктуру розробників, щоб завантажити спеціальний корисний вантаж для Windows, macOS або Linux з метою викрадення облікових даних та криптогаманців, а також встановлення постійного доступу... Ці корисні навантаження пов'язані з відомими сімействами шкідливого ПЗ Lazarus, такими як BeaverTail та InvisibleFerret, які підтримують перехоплення натискань клавіш, віддалений доступ, викрадення даних браузера та файлів, а в деяких випадках — повторне виконання через додаткові хуки, наприклад post-checkout. Рекомендовані заходи захисту включають: розгляд невідомих або пов'язаних з рекрутингом репозиторіїв як ненадійних; перевірку каталогів хуків перед використанням; запуск таких проектів в ізольованих віртуальних машинах без збережених облікових даних; впровадження організаційних політик для перевірки Git-хуків; та повідомлення про підозрілі шаблони хуків у канали розвідки загроз». (**Tushar Subhra Dutta. North Korean Hackers Weaponize Git Hooks to Deploy Cross-Platform Malware // Cyber Security News (<https://cybersecuritynews.com/north-korean-hackers-weaponize-git-hooks/>). 12.05.2026**).

«Кіберзлочинне угруповання TeamPCP та підпільне співтовариство BreachForums організували конкурс, який перетворює атаки на ланцюжок постачання програмного забезпечення з відкритим кодом на гру, заохочуючи учасників заразити якомога більше пакетів з відкритим кодом за допомогою інструменту для атак під назвою «Shai-Hulud». Учасники повинні надати свої ніки на форумі та докази доступу, а переможці визначаються за щотижневою та щомісячною кількістю завантажень уражених пакетів; система підрахунку балів навіть дозволяє зловмисникам об'єднувати завантаження з декількох менших пакетів, стимулюючи безрозбірливе поширення, подібне до черв'яка, по всій екосистемі. Хоча приз становить лише 1 000 доларів, що виплачуються в Monero, дослідники стверджують, що конкурс спрямований не стільки на виплату винагороди, скільки на вербування та мотивацію хакерів з низьким рівнем кваліфікації до здійснення компрометацій з великим впливом заради репутації та права похвалитися, ефективно залучаючи до роботи широку аудиторію, тоді як TeamPCP отримує вигоду від більш широкої цінності інфільтрованої інфраструктури.

Група TeamPCP вже давно спеціалізується на атаках на критично важливі ланки ланцюга постачання програмного забезпечення — зокрема на засоби безпеки, конвеєри CI/CD, GitHub Actions, образи Docker та екосистеми на кшталт

прт і PyPI — з метою викрадення облікових даних, таких як секретні ключі CI/CD, хмарні ключі, токени розробників та вихідний код, для подальших атак. Socket Research зазначає, що крадіжка облікових даних TeamPCP вже вплинула на компанії, що займаються штучним інтелектом, урядові хмарні служби, виробництво та корпоративні технології, а також що група нещодавно уклала партнерство з синдикатом Vest, який займається виманюванням викупу. Завдяки відкритому коду Shai-Hulud та прив'язці успіху до показників за кількістю завантажень, конкурс загрожує спровокувати хвилю наслідувань, що може значно збільшити ризик для розробників та захисників підприємств у всій екосистемі відкритого коду». **(Abinaya. TeamPCP and BreachForums Hackers Running \$1,000 Contest for Supply Chain Attacks // Cyber Security News (<https://cybersecuritynews.com/hackers-1000-contest-supply-chain-attacks/>). 14.05.2026).**

«Компанія Microsoft повідомляє, що пов'язана з Росією шпигунська група Secret Blizzard модернізувала свій давно використовуваний бекдор Kazuar, перетворивши його на модульну однорангову бот-мережу, оптимізовану для прихованого довгострокового функціонування та збору розвідувальної інформації. Secret Blizzard, діяльність якої перетинається з інструментарієм Turla/Venomous Bear і пов'язана з російською ФСБ, історично націлювалася на урядові, дипломатичні, оборонні та критичні системи в Європі, Азії та Україні; сам Kazuar спостерігається з 2017 року, а його кодова лінія сягає 2005 року і з'являлася в кампаніях проти європейських урядів, а пізніше — проти України... Новіша архітектура Kazuar поділяється на три модулі — Kernel, Bridge та Worker, — де Kernel координує завдання та самостійно обирає один заражений хост-«лідер» (на основі показників часу безвідмовної роботи та стабільності) для зовнішнього зв'язку, тоді як інші заражені хости залишаються «неактивними», щоб зменшити зовнішній трафік та уникнути виявлення. Модуль Bridge забезпечує проксі-зв'язок між лідером та віддаленою інфраструктурою управління через такі канали, як HTTP, WebSockets або Exchange Web Services, тоді як для внутрішньої координації ботнету використовуються стандартні механізми міжпроцесного зв'язку Windows (Windows Messaging, Mailslots, іменовані канали) з повідомленнями Protobuf, зашифрованими за допомогою AES, щоб злитися з нормальним системним шумом... Модуль Worker виконує шпигунські функції, зокрема запис натискань клавіш, створення знімків екрана, викрадення даних з файлової системи, розвідку, збір електронних листів з Outlook/MAPI, моніторинг вікон та викрадення нещодавно відкритих файлів, а також проміжне зберігання та шифрування даних на локальному комп'ютері перед їх виведенням через модуль Bridge. Microsoft відзначає високу налаштованість шкідливого програмного забезпечення — близько 150 опцій — а також вбудовані обходи безпеки для AMSI, ETW та WLDLP, і радить захисникам надавати пріоритет поведінковому виявленню над статичними сигнатурами, оскільки модульна, налаштована конструкція Kazuar робить його особливо важким для виявлення». **(Bill Toulas. Russian hackers turn Kazuar backdoor into modular P2P botnet // Bleeping Computer® LLC**

(<https://www.bleepingcomputer.com/news/security/russian-hackers-turn-kazuar-backdoor-into-modular-p2p-botnet/>). 16.05.2026).

«Група зловмисників, відома під назвою «The Gentlemen», стрімко перетворилася на одну з найагресивніших кіберзлочинних угруповань: вона з'явилася на публіці наприкінці 2025 року, а на початку 2026 року увійшла до двійки найактивніших загроз у сфері програм-вимагачів. За даними LevelBlue, ця група, ймовірно, є еволюційним продовженням попередньої партнерської діяльності, пов'язаної з екосистемою Qilin, яку, за повідомленнями, курував російськомовний оператор на псевдонімі «hastalamuerte», що забезпечило їй усталений досвід та мережі. Станом на 10 травня 2026 року група заявила про 352 атаки у першій половині року, жертвами яких стали компанії у понад 70 країнах, що спричинило значний вплив на сфери професійних послуг, виробництва, технологій та охорони здоров'я... Ця операція націлена на широке коло корпоративних середовищ — Windows, Linux, NAS, BSD та VMware ESXi — і використовує структурований алгоритм дій, який зазвичай починається з використання викрадених облікових даних або незахищених віддалених служб, передбачає викрадення даних до їх шифрування з метою подвійного шантажу та може паралізувати інфраструктуру віртуалізації для швидкого виведення з ладу великих серверних парків. Її програмне забезпечення для вимагання викупу для Windows, написане на Go та захищене паролем виконання для унеможливлення запуску в пісочниці, використовує випадкові шестисимвольні розширення файлів і залишає записку READMEGENTLEMEN.txt, повністю шифруючи невеликі файли та великі файли частинами для максимальної швидкості та порушення роботи, одночасно зупиняючи служби, пов'язані з базами даних, резервним копіюванням, віртуалізацією та віддаленим доступом, щоб заблокувати відновлення... Група також використовує партнерську платформу для створення шкідливих програм, ведення переговорів, оцінки доходів від викупу та обробки завантажених викрадених даних; крім того, є непідтверджені повідомлення про те, що хтось продає нібито внутрішні дані «Gentlemen», включаючи інформацію про переговори та картування, за біткойни. LevelBlue радить захисникам зміцнити системи, що підключені до Інтернету, такі як VPN та брандмауери, запровадити багатофакторну автентифікацію (MFA), регулярно змінювати скомпрометовані облікові дані, вимкнути неактивні облікові записи та виявляти ранні ознаки вторгнення, такі як незвичайні входи адміністратора, інструменти розвідки, утиліти віддаленого доступу, зміни групової політики та масове вимкнення служб, одночасно ізолюючи та регулярно тестуючи резервні копії та середовища ESXi для забезпечення можливостей відновлення». (*Tushar Subhra Dutta. The Gentlemen Ransomware Attacks Windows, Linux, NAS, BSD, and ESXi Attacks // Cyber Security News* (<https://cybersecuritynews.com/the-gentlemen-ransomware-attacks-windows/>). 19.05.2026).

«У першій половині 2025 року пов'язана з Північною Кореєю група кібершпигунів «Kimsuky» провела чотири складні та відмінні одна від одної кампанії «спір-фішингу», які охопили широке коло організацій у корпоративному, оборонному, криптовалютному та академічному секторах. Незважаючи на різноманітність приманок — від підроблених резюме та матеріалів на тему криптовалют до документів про конкурси в оборонній сфері та форм для вступу — ці кампанії мали спільну оперативну стратегію. Після відкриття файлу-приманки шкідливе програмне забезпечення зазвичай закріплювалося в системі протягом п'яти хвилин, вимикаючи контроль облікових записів користувачів Windows (UAC), реєструючи винятки для Defender та використовуючи планувальник завдань. Зловмисники активно використовували замасковані файли LNK або JSE з подвійними розширеннями, які успішно видавали себе за нешкідливі документи PDF або HWP, щоб обдурити нічого не підозрюючих користувачів...

Група продемонструвала високий рівень витонченості, направляючи обмін даними через надійні платформи — такі як необроблені API-інтерфейси GitHub, CDN від Microsoft та тунелі VSCode — щоб замаскувати шкідливу діяльність під звичайний мережевий трафік, ефективно обходячи засоби безпеки, що базуються на репутації. Крім того, вони використовували методи «living-off-the-land», застосовуючи вбудовані компоненти Windows, такі як certutil та rundll32, для виконання шкідливих кодів, що допомагає їм залишатися непоміченими. За словами аналітиків LogPresso, здатність Kimsuky швидко змінювати інфраструктуру управління та контролю робить статичне блокування доменів або хешів файлів ненадійною оборонною стратегією. Натомість захисникам рекомендується застосовувати стратегії виявлення на основі поведінки, такі як моніторинг незвичайних записів у планувальнику завдань, несанкціоноване вимкнення функцій безпеки Windows та підозріле використання легітимних тунельних служб, оскільки зосередження уваги на моделях поведінки наразі є єдиним надійним методом протидії такому адаптивному зловмиснику». (*Tushar Subhra Dutta. Kimsuky Hackers Use LNK and JSE Lures to Target Recruiters, Crypto Users, and Defense Officials // Cyber Security News (https://cybersecuritynews.com/kimsuky-hackers-use-lnk-and-jse-lures-to-target-recruiters/). 19.05.2026).*

Вірусне та інше шкідливе програмне забезпечення

«Шкідливе програмне забезпечення з відкритим кодом еволюціонує від масової проблеми типосквоттингу та підроблених пакетів до більш прихованої та цілеспрямованої загрози, яка використовує довіру розробників до знайомих назв пакетів, перевірених супровідників, стандартних шляхів випуску та автоматизованих робочих процесів CI/CD. На відміну від випадкових вразливостей, це шкідливе програмне забезпечення навмисно розроблено для запуску на ранніх етапах — часто під час інсталяції — тому компрометація може

відбутися на комп'ютерах розробників або в конвеєрах збірки ще до запуску традиційних перевірок безпеки на «кінці конвеєра», що дозволяє зловмисникам викрасти токени, облікові дані та секрети середовища або отримати доступ до систем випуску... Відстеження компанією Sonatype понад 454 600 нових шкідливих пакетів у 2025 році (загалом понад 1,233 млн) свідчить про дедалі більш масштабні та організовані кампанії, які зараз мають більш поетапний та наполегливий характер і використовують горизонтальне переміщення, завантаження вторинних корисних навантажень, обфускацію, відкладене виконання та видалення слідів. Недавні інциденти ілюструють ці закономірності: SANDWORM_MODE продемонстрував адаптивну, багатоетапну поведінку і навіть націлювся на інструменти штучного інтелекту; інциденти, пов'язані з Trivy та LiteLLM, підкреслили, як зловмисники можуть зловживати надійною інфраструктурою випуску, обліковими записами служб та токенами, щоб отримати довіру та розширити радіус ураження; а атака, пов'язана з axios, продемонструвала, як невеликі зміни транзитивних залежностей можуть спричинити виконання під час інсталяції, доставку корисного навантаження та очищення... Ключовим кроком у зміні підходу до захисту є перенесення управління залежностями на більш ранній етап — перевірка компонентів до їх інсталяції за допомогою контрольованих каналів споживання, таких як проксі-репозиторії, виявлення шкідливого програмного забезпечення під час завантаження, а також обов'язкових до виконання політик, що блокують або ізолюють підозрілі пакети, одночасно перевіряючи транзитивні залежності, скрипти інсталяції, метадані випусків та аномальну поведінку при публікації. Оскільки середовища розробників та CI/CD тепер містять цінні активи, їх необхідно захищати так само, як і виробничі системи, за допомогою принципу мінімальних привілеїв, обмеження доступу до облікових даних, моніторингу поведінки та швидкої скоординованої ротації секретів, замінюючи припущення про довіру до відкритого коду постійною верифікацією».

(Aaron Linskens. *The Evolution of Open Source Malware: From Volume to Trust Abuse* // Sonatype Inc. (<https://www.sonatype.com/blog/the-evolution-of-open-source-malware-from-volume-to-trust-abuse>). 05.05.2026).

«Компанія SentinelLabs виявила нову платформу шкідливого програмного забезпечення під назвою PCPJack, яка компрометує незахищену хмарну інфраструктуру на базі Linux з метою викрадення великого обсягу облікових даних, при цьому активно видаляючи інструментарій TeamPCP із заражених систем, щоб «взяти під свій контроль» процес вторгнення. Ця платформа націлена на широко розповсюджені хмарні та розробницькі сервіси, такі як Docker, Kubernetes, Redis, MongoDB, RayML, а також уразливі веб-додатки, і часто переміщується по мережі, збираючи SSH-ключі та перераховуючи внутрішні демони Docker та кластери Kubernetes. PCPJack поширюється через скрипт оболонки (bootstrap.sh), який створює прихований робочий каталог, встановлює залежності Python, завантажує модулі, забезпечує стійкість та запускає оркестратор (monitor.py); на початку виконання він явно шукає та видаляє процеси, контейнери, файли та артефакти стійкості TeamPCP...

Операція, судячи з усього, спрямована на масштабне викрадення облікових даних та, ймовірно, їх монетизацію шляхом шахрайства, розсилки спаму, перепродажу облікових даних або вимагання. У ході операції збираються секретні дані, що охоплюють хмарні облікові записи та інструменти (наприклад, DigitalOcean), облікові дані розробників та систем штучного інтелекту (включно з ключами OpenAI та Anthropic), платформи для спільної роботи (токенів Slack), бази даних, конфігурації WordPress та месенджери (Discord). Викрадені дані шифруються (X25519 ECDH з ChaCha20-Poly1305) і виводяться частинами на канали Telegram. Для поширення PCPJack сканує Інтернет на наявність незахищених хмарних сервісів, витягує додаткові цілі з наборів даних імен хостів Common Crawl та експлуатує відомі вразливості, включаючи обхід аутентифікації в проміжному програмному забезпеченні Next.js (CVE-2025-29927), проблему десеріалізації React/Next.js Server Actions («React2Shell», CVE-2025-55182), недоліки плагінів WordPress у WPVivid Backup (CVE-2026-1357) та W3 Total Cache (CVE-2025-9501), а також ін'єкцію у файловий менеджер CentOS Web Panel (CVE-2025-48703). Збереження даних досягається за допомогою різних механізмів, таких як служби systemd, завдання cron, перезапис cron у Redis або контейнери з привілеями. Крім того, SentinelLabs виявила на інфраструктурі зловмисників інструменти-бекдори на базі Sliver, що підтримують різні архітектури процесорів...

Оскільки тактика та цілі цієї кампанії дуже нагадують попередні кампанії TeamPCP — відомої групи, що спеціалізується на хмарних технологіях і пов'язана з інцидентами в ланцюгах постачання, пов'язаними з використанням таких інструментів, як Trivy, та шкідливих пакетів PyPI/npm — компанія SentinelLabs припускає, що за PCPJack може стояти колишній партнер або член TeamPCP. Рекомендовані заходи щодо мінімізації ризиків включають впровадження багатофакторної автентифікації (MFA), захист доступу до метаданих хмарних сервісів (наприклад, IMDSv2 на AWS), забезпечення належної автентифікації та захисту Docker і Kubernetes, застосування принципу мінімальних привілеїв та уникнення зберігання секретних даних у вигляді звичайного тексту». **(Bill Toulas. New PCPJack worm steals credentials, cleans TeamPCP infections // Bleeping Computer® LLC (<https://www.bleepingcomputer.com/news/security/new-pcpjack-worm-steals-credentials-cleans-teampcp-infections/>). 07.05.2026).**

«...Шкідливий репозиторій на Hugging Face ненадовго очолив рейтинг найпопулярніших проектів платформи, видаючи себе за легітимний проект OpenAI «Privacy Filter», і був завантажений приблизно 244 000 разів, перш ніж про нього повідомили та його видалили. 7 травня дослідники HiddenLayer виявили репозиторій під назвою Open-OSS/privacy-filter і з'ясували, що він скористався типографською помилкою в назві релізу OpenAI, скопіював документацію до моделі та містив скрипт loader.py, який маскувався під нешкідливий код штучного інтелекту, одночасно вимикаючи перевірку SSL та завантажуючи віддалений JSON-пакет, що запускав невидиму команду PowerShell. Цей ланцюжок завантажував і запускав пакетний файл, який намагався підвищити привілеї, додавав остаточне шкідливе ПЗ до виключень Microsoft Defender та

виконував sefirah — інфостілер на базі Rust, призначений для викрадення облікових даних браузера та даних сеансу, токенів Discord, даних криптовалютних гаманців, облікових даних SSH/FTP/VPN, конфіденційних локальних файлів, системної інформації та знімків екрана, а потім стискає та викрадає дані на сервер управління та контролю за адресою recargaropular[.]com... Шкідливе ПЗ використовувало механізми захисту від аналізу, спрямовані проти віртуальних машин, пісочниць та відладчиків. Слідчі зазначили, що показники завантажень та «лайків» могли бути завищені за рахунок автоматизованих акаунтів, хоча точна кількість жертв залишається невідомою. Команда HiddenLayer також виявила зв'язок цієї ж інфраструктури завантажувачів з іншими шкідливими репозиторіями та зафіксувала збіги з кампанією типосквоттингу в prn, що поширювала імплант WinOS 4.0. Користувачам, які завантажили файли, рекомендується перевстановити ОС на уражених машинах, змінити всі облікові дані, замінити криптогаманці та фрази-посів, а також анулювати сесії та токени, підкреслюючи, що Hugging Face продовжує зловживатися для розповсюдження шкідливих артефактів ML, незважаючи на існуючі заходи безпеки». **(Bill Toulas. Fake OpenAI repository on Hugging Face pushes infostealer malware // Bleeping Computer® LLC (<https://www.bleepingcomputer.com/news/security/fake-openai-repository-on-hugging-face-pushes-infostealer-malware/>). 09.05.2026).**

«Національний інститут стандартів і технологій (NIST) готується опублікувати нові рекомендації з кібербезпеки, спрямовані саме на штучний інтелект, які мають на меті зменшити цифрові загрози, пов'язані з використанням ШІ, та водночас сприяти його безпечному впровадженню. За словами Вікторії Піллітері, яка очолює Групу з інженерії безпеки та управління ризиками NIST, проєкт профілю рамки кібербезпеки для ШІ, який очікує на затвердження, має з'явитися «десь цього літа». Ця структура супроводжуватиметься рекомендаціями щодо «контрольного накладення» — індивідуальними базовими стандартами кібербезпеки для різних типів систем ШІ, які розробляються спільно з Центром стандартів та інновацій у сфері ШІ (CAISI) NIST і спочатку зосереджуються на загрозах, пов'язаних із прогнозним, генеративним та агентивним ШІ... NIST готується опублікувати нові рекомендації з кібербезпеки, спрямовані саме на штучний інтелект, які мають на меті зменшити цифрові загрози, пов'язані з використанням ШІ, і водночас сприяти його безпечному впровадженню.

За словами Вікторії Піллітері, яка очолює Групу з інженерії безпеки та управління ризиками NIST, проєкт профілю рамки кібербезпеки для ШІ, який очікує на затвердження, має з'явитися «десь цього літа»...

Ця структура супроводжуватиметься рекомендаціями щодо «контрольного накладення» — індивідуальними базовими стандартами кібербезпеки для різних типів систем ШІ, які розробляються спільно з Центром стандартів та інновацій у сфері ШІ (CAISI) NIST і спочатку зосереджуються на загрозах, пов'язаних із прогнозним, генеративним та агентивним ШІ». **(Alexandra Kelley. NIST aims for summer release of AI cyber guidelines // Government Media Executive Group LLC.**

(<https://www.nextgov.com/artificial-intelligence/2026/05/nist-aims-summer-release-ai-cyber-guidelines/413559/>). 14.05.2026).

«Дослідники виявили раніше невідоме шкідливе програмне забезпечення під назвою TencShell — складну платформу для віддаленого керування, яка надає зловмисникам можливість інтерактивного контролю над ураженими системами Windows і підкреслює, як зловмисники дедалі частіше перепрофілюють загальнодоступні інструменти для здійснення цілеспрямованих вторгнень. У квітні 2026 року компанія Cato Networks виявила та заблокувала спробу розгортання цього шкідливого програмного забезпечення проти глобальної виробничої компанії, перехопивши атаку на її об'єкти в Індії та простеживши її до стороннього користувача з легітимним доступом, що демонструє, як надійні ділові зв'язки можуть бути використані як точка входу... TencShell — це модифікована та перепакована версія фреймворку Rshell з відкритим кодом, яка була змінена таким чином, щоб імітувати трафік API, схожий на трафік Tencent, завдяки чому її командно-контрольна діяльність маскується під звичайні веб-запити. Імплант підтримує зняття знімків екрана та пряму трансляцію через WebSocket, імітацію клавіатури та миші для повної віддаленої взаємодії, доступ до артефактів браузерів Chrome та Edge (включно з сесіями, файлами cookie та даними для входу), обхід UAC для отримання підвищених привілеїв без запитів, а також додаткові функції, такі як проксі SOCKS5, завантаження DLL, передача файлів та збереження через ключ запуску реєстру, замаскований під «OneDriveHealthTask»... У ході атаки використовувався багатоетапний ланцюжок доставки, в якому початковий дроппер завантажував файл, замаскований під звичайний веб-шрифт у форматі .woff, який насправді містив шеллкод Donut для завантаження корисних навантажень безпосередньо в пам'ять, а потім рефлексивно відображав TencShell у пам'ять, щоб уникнути залишків на диску. Фахівцям із захисту рекомендується стежити за незвичайними вихідними веб-запитами до невідомих кінцевих точок, підозрілими завантаженнями файлів .woff поза звичайним контекстом браузера та несподіваними записами автозапуску в реєстрі Windows». (*Tushar Subhra Dutta. New Malware Framework Enables Screen Control, Browser Artifact Access, and UAC Bypass // Cyber Security News* (<https://cybersecuritynews.com/new-malware-framework-enables-screen-control/>). 14.05.2026).

«Дослідники з компанії Cato Networks виявили новий, раніше невідомий шкідливий імплант під назвою «TencShell», який, як вони припускають, пов'язаний із зловмисником, що діє в інтересах Китаю. Це відкриття було зроблено у квітні 2026 року під час спроби вторгнення в індійське відділення міжнародної виробничої компанії. Складний ланцюжок атак включав дроппер першого рівня, ін'єкцію в пам'ять та канал зв'язку «команда-контроль» (C2), замаскований під легітимний веб-трафік компанії Tencent... Сам імплант є модифікованою версією фреймворку Rshell C2 з відкритим кодом, який

призначений для міжплатформної атакувальної безпеки та включає функції віддаленого виконання команд і взаємодії з агентами штучного інтелекту. Цей інцидент підкреслює зростаючу тенденцію, коли зловмисники адаптують загальнодоступні інструменти з відкритим кодом для здійснення складних вторгнень, маскуючи свою шкідливу діяльність під звичайний корпоративний трафік, щоб уникнути виявлення. У разі успіху атака могла б надати зловмиснику повний доступ до середовища об'єкта атаки». (**Kevin Poireault. China-Linked Hackers Deploy New TencShell Malware Against Global Manufacturer // Reed Exhibitions Ltd.** (<https://www.infosecurity-magazine.com/news/china-hackers-tencshell-malware/>). 15.05.2026).

«Дослідники у сфері кібербезпеки виявили надзвичайно витончену кампанію з розповсюдження шкідливого програмного забезпечення, спрямовану на хмарні середовища Python через три скомпрометовані версії (1.4.1, 1.4.2 та 1.4.3) пакета **durabletask** на PyPI. Після імпортування в середовищі Linux прихований дропер завантажує корисний вантаж другого рівня, файл **gore.pyuz**, із нещодавно зареєстрованого домену управління та контролю (C2). Після виконання перевірок на уникнення пісочниць та систем з російською локалізацією корисне навантаження працює як агресивний інфостілер, систематично збираючи та шифруючи облікові дані від основних хмарних провайдерів (AWS, Azure, GCP), Kubernetes, Docker, HashiCorp Vault, менеджерів паролів та інструментів розробки штучного інтелекту. Окрім викрадення даних, шкідливе програмне забезпечення функціонує як черв'як, автономно поширюючись на інші екземпляри EC2 через AWS Systems Manager (SSM) та на сусідні підсистеми Kubernetes...

Шкідливе ПЗ демонструє високий рівень оперативної безпеки, використовуючи як резервний канал управління (C2) систему «мертвої скриньки» на базі GitHub із криптографічною автентифікацією, яка запускається за ключовим словом «**FIRESCALE**». Воно також має унікальний метод витоку даних, що автоматично створює публічні репозиторії GitHub, названі на честь російського фольклору, для завантаження викрадених даних у разі виходу з ладу основних каналів. Крім того, зловмисник може дистанційно запустити модуль, який забезпечує стійкість у **systemd** під виглядом монітора PostgreSQL і розгортає геополітично націлений віпер; якщо система виявляє налаштування локалі Ізраїлю чи Ірану, вона має випадкову ймовірність збільшити гучність системи до максимуму, відтворити аудіофайл та виконати катастрофічне очищення диска. Організації, які встановили уражені версії, повинні припустити негайне компрометацію, змінити всі відкриті облікові дані хмарних сервісів та розробників, заблокувати пов'язані мережеві індикатори та шукати конкретні маркери інфікування — такі як файл **.sys-update-check** — щоб зупинити поперечне переміщення черв'яка...» (**Raphael Silva. Microsoft's durabletask package on PyPi Compromised. Mini Shai Hulud attacks again... again! // Aikido Security BV** (<https://www.aikido.dev/blog/durabletask-package-compromised-mini-shai-hulud>). 19.05.2026).

«У новому звіті глобальної страхової компанії QBE, підготовленому у співпраці з консалтинговою компанією Control Risks, що спеціалізується на ризиках, міститься попередження про те, що атаки програм-вимагачів на будівельний сектор Великої Британії спричиняють у середньому 24 дні простою на кожен випадок, що загрожує зривом цілих проектів. У звіті під назвою «Від креслень до порушень» підкреслюється, що все ширше впровадження в секторі інформаційного моделювання будівель, підключених операційних технологій та систем на базі штучного інтелекту розширює площину атаки, пов'язуючи системи обробки даних із фізичним управлінням обладнанням, що перетворює операційні досягнення на потенційні загрози безпеці. Коли відбувається атака програм-вимагачів, втрачається доступ до креслень, даних про проекти та цифрових платформ, що призводить до зростання витрат і створює негайні наслідки для субпідрядників...

Масштаби загрози різко зросли: у 2025 році активність шкідливого програмного забезпечення для Інтернету речей (IoT), спрямованого проти будівельної галузі, зросла на 410% порівняно з попереднім роком, а недостатня сегментація між IT- та OT-системами стала причиною 81% зареєстрованих інцидентів в OT-секторі. Геополітичний тиск додає ще більшого ризику: у Великобританії в період з 2022 по 2026 рік було зафіксовано 15 кібератак, пов'язаних з державою, — це більше, ніж у порівнянних європейських країнах, — а будівельні компанії залишаються вразливими через свою участь у критичній національній інфраструктурі. Національний центр кібербезпеки Великобританії зафіксував 204 кібератаки національного значення за рік до вересня 2025 року, що на 89 більше, ніж у попередньому році. Регуляторні вимоги також посилюються: директива ЄС NIS2 вимагає оперативного повідомлення про інциденти та відповідальності керівництва, а запропонований у Великобританії законопроект про кібербезпеку та стійкість, як очікується, поширить свою дію на багато будівельних компаній. QBE закликає галузь з самого початку розглядати кіберризик як основний ризик проекту, а не як проблему IT, та залучати страховиків на ранніх етапах планування проекту». (*Jonalyn Cueto. Cyber threats putting UK construction projects at risk, insurer warns // KM Business Information UK Ltd* (<https://www.insurancebusinessmag.com/uk/news/cyber/cyber-threats-putting-uk-construction-projects-at-risk-insurer-warns-574224.aspx>). 06.05.2026).

«Угорський медіагігант Mediaworks, один із провідних гравців у проурядовому медіапросторі країни, підтвердив масштабний витік даних, що стався внаслідок атаки програм-вимагачів, здійсненої угрупованням World Leaks. За повідомленнями, це угруповання, що займається вимаганням, викрало та опублікувало на своєму порталі в даркнеті майже 8,5 терабайтів конфіденційних файлів, зокрема дані про нарахування заробітної плати, фінансову звітність та

внутрішню переписку. Найбільш суперечливим є те, що місцеві ЗМІ повідомили, що викрадені дані містили редакційні нотатки від початку 2025 року, які свідчать про те, що компанія планувала звернутися за допомогою до Москви, щоб дискредитувати президента України Володимира Зеленського... Хоча компанія Mediaworks розпочала розслідування та погрожує судовими позовами журналістам, які висвітлюють викрадені дані — називаючи такі публікації кримінальним злочином — незалежні ЗМІ, такі як Media1, відмовилися підкоритися, посиляючись на значний суспільний інтерес до цієї інформації. World Leaks, перейменована версія угруповання Hunters International, зосереджується переважно на крадіжці даних, а не на шифруванні, і має досвід атак на глобальні організації. Цей інцидент став продовженням попередніх кібератак на Mediaworks з боку хактивістської групи Anonymous, яка звинуватила компанію в тому, що вона є пропагандистським інструментом прокремлівської політики». **(Daryna Antoniuk. Ransomware group claims breach of pro-Orbán Hungarian media firm // Recorded Future News (<https://therecord.media/ransomware-group-claims-breach-of-pro-orban-media-firm>). 04.05.2026).**

«У звіті BlackFog стверджується, що про випадки використання програм-вимагачів повідомляється значно рідше, ніж насправді: за оцінками, лише кожна дев'ята атака стає відомою широкому загалу. У першому кварталі цього року компанія BlackFog виявила 2 160 нерозголошених інцидентів із використанням програм-вимагачів у 97 країнах — це приблизно на 2% більше, ніж у минулому році, — тоді як публічно було повідомлено лише про 264 атаки, хоча офіційні дані вказували на 15-відсоткове зниження порівняно з минулим роком. Дослідження показало, що середня сума викупу перевищує 1 млн доларів (1 028 214 доларів) і що наслідки відчутні у 39 країнах, причому кількість атак на логістику зросла на 200% у порівнянні з минулим роком, а найчастіше атакованим сектором стала сфера охорони здоров'я (72 атаки, 27%), за якою йдуть державні установи (32, 12%) та технологічний сектор (28, 11%)... Серед інцидентів, про які стало відомо громадськості, найактивнішим варіантом був Qilin (22 атаки, 8%), за ним йшли ShinyHunters (16, 6%) та INC (11, 4%), тоді як 38% публічно відомих випадків залишилися неідентифікованими; серед нерозкритих атак також лідирував Qilin (339, 16%), за ним йшли The Gentlemen (200, 9%) та Akira (190, 9%), причому загалом жертвами стали 79 груп. Генеральний директор BlackFog д-р Даррен Вільямс попередив, що програмне забезпечення для вимагання викупу залишається дуже активним, все частіше використовуючи штучний інтелект для автоматизації викрадення даних, а оскільки витік даних відбувається у 96% атак, організації повинні зосередитися на запобіганні витоку даних зі своїх систем, а не припускати, що ризик можна контролювати після того, як це сталося». **(Ian Barker. Only one in nine ransomware attacks is made public // BetaNews, Inc. (<https://betanews.com/article/only-one-in-nine-ransomware-attacks-is-made-public/>). 06.05.2026).**

«Традиційні стратегії резервного копіювання дедалі частіше виявляються неспроможними захистити організації від програм-вимагачів, оскільки сучасні зловмисники систематично націлюються на системи резервного копіювання та знищують їх ще до початку шифрування. Отримавши адміністративні облікові дані, кіберзлочинці можуть виявити репозиторії резервних копій, змінити політики зберігання даних та видалити точки відновлення, фактично перетворюючи критично важливу систему безпеки на єдину точку відмови. Ця системна вразливість зберігається значною мірою тому, що багато організацій покладаються на фрагментовані архітектури, де системи резервного копіювання не ізольовані від виробничих середовищ, не мають багатофакторної автентифікації та використовують спільні облікові дані, що робить їх легкою мішенню для горизонтального переміщення...»

Щоб протидіяти цьому, фахівці з ІТ та безпеки повинні перейти до підходу, орієнтованого на «пріоритет стійкості», за якого до інфраструктури резервного копіювання застосовуються такі ж суворі стандарти безпеки, як і до виробничих систем. Наріжним каменем цієї стратегії є незмінність — забезпечення того, щоб резервні копії не можна було змінювати або видаляти протягом визначеного періоду, навіть адміністратору. Однак однієї незмінності недостатньо; вона має поєднуватися зі строгим розділенням ідентичностей, багатофакторною автентифікацією та ізоляцією мережі, щоб запобігти отриманню зловмисниками адміністративного доступу, необхідного для саботажу системи...

Зрештою, найефективніший захист полягає у відході від розрізнених засобів безпеки та резервного копіювання на користь інтегрованих, уніфікованих платформ, таких як Acronis Cyber Platform. Об'єднавши захист кінцевих точок, виявлення загроз та управління резервним копіюванням, організації можуть своєчасно виявляти аномалії, зменшити операційну складність та гарантувати, що точки відновлення залишаються чистими та перевіреними. У міру зростання загроз від програм-вимагачів організації повинні переглянути свою архітектуру резервного копіювання, виходячи з припущення, що зловмисники будуть активно шукати дані для відновлення, і гарантувати безперервність роботи не лише за рахунок наявності резервних копій, а й їхньої здатності вистояти під час самої атаки». *(Subramani Rao. Why ransomware attacks succeed even when backups exist // Bleeping Computer® LLC (<https://www.bleepingcomputer.com/news/security/why-ransomware-attacks-succeed-even-when-backups-exist/>). 06.05.2026).*

«Уряди дедалі ефективніше протидіють діяльності зловмисників, що використовують програми-вимагачі, застосовуючи такі заходи, як арешти, конфіскація інфраструктури та санкції, проте довгострокова ефективність цих заходів залишається недостатньо вивченою. За словами Макса Смітса, співдиректора Virtual Routes, хоча ці дії успішно спрямовані проти конкретних злочинних угруповань, вони не обов'язково змінюють екосистему програм-вимагачів у довгостроковій перспективі або у стратегічно вигідний спосіб. Щоб усунути цю прогалину, Смітс та Королівський інститут об'єднаних служб (RUSI) запровадили нову практичну концепцію, покликану допомогти політикам та

правоохоронним органам вийти за межі бінарних оцінок «успіх чи провал» під час аналізу урядових контрзаходів...

Ця концептуальна модель базується на припущенні, що втручання не просто пригнічують злочинну діяльність, а натомість комплексно змінюють ландшафт програм-вимагачів. Щоб відобразити цю складність, модель оцінює чотири ключові аспекти: серйозність, масштаб, тривалість та оборотність, а також сигнальну цінність. Застосовуючи цю концепцію, захисники можуть отримати більш глибоке розуміння довгострокового впливу своїх дій — це є надзвичайно важливим з огляду на стійкість груп, що використовують програмне забезпечення для вимагання викупу. Ці злочинні організації часто адаптуються до тиску, змінюючи назву або діючи під різними брендами, що створює постійні труднощі для тих, хто їх відстежує. Зрештою, цей системний підхід має на меті замінити реактивні тактики знешкодження на більш стратегічну, довгострокову методологію оцінки впливу державних заходів на екосистему загроз, що постійно розвивається».

(Mathew J. Schwartz. *Wielding Disruption: Strategies to Counter Ransomware Evolve* // Information Security Media Group, Corp. (<https://www.inforisktoday.com/wielding-disruption-strategies-to-counter-ransomware-evolve-a-31662>). 14.05.2026).

«Організовані кіберзлочинці все частіше адаптують традиційні схеми використання програм-вимагачів для здійснення масштабних крадіжок вантажів за допомогою кіберзасобів, що, за повідомленнями, призведе до збитків у Північній Америці у розмірі щонайменше 725 мільйонів доларів у 2025 році. Замість розгортання шкідливого програмного забезпечення зловмисники використовують розвідку, фішинг та крадіжку облікових даних, щоб проникнути в електронні поштові скриньки співробітників логістичних служб. Опинившись всередині, вони непомітно змінюють транспортні документи, маніпулюють даними про маршрути або створюють фальшиві ідентифікаційні дані автоперевізників, щоб обдурити законних водіїв і змусити їх доставляти дорогі вантажі — від споживчих товарів до фармацевтичних препаратів — безпосередньо на склади злочинців, звідки товари швидко повертаються в ланцюг постачання... Транспортний сектор є особливо вразливим до таких атак, оскільки малі та середні автопарки часто працюють з мінімальною рентабельністю, не маючи необхідних бюджетів на кібербезпеку, спеціалізованого персоналу та базових засобів захисту, таких як багатофакторна автентифікація. Приваблені високою вартістю викрадених коштів, які легко відмити, та меншими юридичними ризиками порівняно з атаками на фінансові або медичні установи, злочинці розглядають логістичну галузь як надзвичайно прибуткову «м'яку ціль»; ця проблема посилюється тим, що компанії не повідомляють про крадіжки через побоювання за свою репутацію. Для боротьби з цією зростаючою загрозою Національна асоціація автомобільних вантажних перевезень (NMFTA) започаткувала кілька важливих ініціатив, зокрема Центр запобігання шахрайству у сфері вантажних перевезень та Рамку зменшення злочинів у сфері кібербезпеки вантажних перевезень, яка адаптує стандартні протоколи безпеки спеціально для галузі автомобільних вантажних перевезень. Крім того, NMFTA активно залучає експертів із ширшої спільноти кібербезпеки,

щоб забезпечити захист цієї життєво важливої критичної інфраструктури, та висвітлити ці виклики на своїй майбутній Конференції з кібербезпеки 2026 року». **(Ben Wilkens. Cyber-Enabled Cargo Crime: How Cybercrime Tradecraft is Used to Steal Freight // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/cyber-enabled-cargo-crime-how-cybercrime-tradecraft-is-used-to-steal-freight/). 14.05.2026).**

«Малі підприємства дедалі частіше стають головними мішенями для програм-вимагачів, і це не випадково: вони часто володіють цінними даними, мають обмежений час на реагування та слабкі або несистематично застосовувані засоби захисту, хоча багато власників досі вважають, що програми-вимагачі нападають переважно на лікарні чи великі бренди. За даними «Обсерваторії витоків даних» компанії Proton, на малі та середні підприємства припадає 63% витоків, зафіксованих з січня 2025 року, та понад 352 мільйони викрадених записів, причому вони переважають у найнебезпечніших інцидентах: 61% випадків порушення безпеки даних високого ризику стосуються малих та середніх підприємств, причому лише на малі підприємства припадає 48% цих критичних випадків, а на малі та середні підприємства припадає 60% випадків порушення безпеки, що призвели до витоку понад 100 000 записів... Дані уряду Великої Британії також свідчать про зростання кількості випадків використання програм-вимагачів: 1% британських підприємств повідомили про такі випадки протягом минулого року (у порівнянні з менш ніж 0,5% у 2024 році), що, за підрахунками, становить близько 19 000 інцидентів по всій країні, тоді як фішинг залишається найпоширенішим способом проникнення і часто слугує першим кроком до викрадення облікових даних, компрометації облікових записів та, зрештою, запуску програм-вимагачів... Сучасні програми-вимагачі становлять загрозу як для доступності систем, так і для безпеки даних, оскільки зловмисники дедалі частіше не лише шифрують системи, а й викрадають дані та погрожують їх оприлюднити. Доступ до систем вони зазвичай отримують через типові помилки користувачів, такі як перехід за фішинговими посиланнями, використання паролів, що вже використовувалися в інших випадках витоку даних, незахищені служби віддаленого доступу та незакриті вразливості; проникнувши всередину, зловмисники переміщуються по системі, розширюють свої права та блокують можливості відновлення даних, після чого вимагають від жертв викуп, зазвичай у вигляді криптовалюти. Оскільки жоден окремий інструмент не може повністю запобігти атакам програм-вимагачів, захист малих та середніх підприємств вимагає практичного багаторівневого підходу, спрямованого на обмеження легких шляхів доступу та покращення процесів відновлення: впровадження багатофакторної аутентифікації (особливо для електронної пошти, хмарних сервісів, адміністративного та віддаленого доступу), поліпшення гігієни паролів за допомогою унікальних облікових даних та контрольованого обміну через менеджер паролів (оскільки Proton виявив, що 48% опитаних керівників малих та середніх підприємств не мали такого менеджера, а 39% згадали інциденти, спричинені людською помилкою), дотримання дисципліни щодо встановлення оновлень для

ОС та систем, що підключені до Інтернету, посилення фільтрації електронної пошти та веб-контенту, навчання персоналу з урахуванням того, що помилки все одно траплятимуться, а також регулярне створення ізольованих перевірених резервних копій із використанням підходів на кшталт «3-2-1» та сканування резервних копій перед відновленням... У разі атаки на мале та середнє підприємство (МСП) у рекомендаціях наголошується на необхідності швидкого локалізування інциденту (ізоляція пристроїв та облікових записів, збереження доказів), повідомлення відповідних органів (у тому числі до Національного центру з кібербезпеки Великої Британії (NCSC), якщо це доречно), уникнення виплати викупу, оскільки це не гарантує відновлення даних чи запобігання їх витоку і може спровокувати повторні атаки, а також ретельного відновлення з чистих резервних копій із заміною облікових даних та закриттям початкового каналу доступу; у Великобританії інциденти, пов'язані з персональними даними, можуть спричинити обов'язок повідомлення ICO про GDPR протягом 72 годин, якщо існує ймовірний ризик для фізичних осіб. Загалом, програмне забезпечення для вимагання викупу для малих та середніх підприємств є, по суті, проблемою безперервності бізнесу та безпеки облікових даних, і послідовне застосування основних заходів — багатофакторної автентифікації, надійного управління обліковими даними, встановлення виправлень, захисту електронної пошти, принципу мінімальних привілеїв та перевірених резервних копій — може запобігти тому, щоб один фішинг або вкрадений пароль призвели до зупинки роботи всієї компанії». **(Kate Menzies. How to prevent and recover from ransomware attacks on small businesses // Proton AG (<https://proton.me/business/blog/ransomware-small-business>). 14.05.2026).**

«Атака програм-вимагачів на компанію Synnovis у червні 2024 року, яка надає послуги з аналізу крові кільком великим медичним фондам Національної служби охорони здоров'я (NHS), серйозно порушила графік понад 10 000 прийомів у лондонських лікарнях, змусила скасувати процедури, а згодом була пов'язана зі смертю пацієнта в лікарні Кінгс-Коледж. Цей інцидент продемонстрував, що кібератаки на сферу охорони здоров'я вже не є абстрактними ІТ-проблемами, а є безпосередніми загрозами, які реалізуються в реальному часі, створюючи додатковий тиск на і без того перевантажений медичний персонал та безпосередньо ставлячи під загрозу людські життя. У міру того, як лікарні, клініки та практики сімейних лікарів стають все більш взаємопов'язаними в цифровому просторі, поверхня атаки продовжує розширюватися. Сучасні лікарні тепер функціонують як складні, технологічно орієнтовані середовища, де системи управління будівлею (BMS) контролюють усе: від систем опалення, вентиляції та кондиціонування повітря (HVAC) і розподілу енергії до безпеки та профілактичного обслуговування. Хоча ці розумні системи забезпечують значні переваги в плані енергоефективності, сталого розвитку та скорочення часу простою, вони непомітно підірвали природний захист, який колись забезпечувала ізольована застаріла інфраструктура. Сьогодні енергетичні платформи підключаються до ширших мереж, хмарних аналітичних систем та

сторонніх пристроїв Інтернету речей (IoT) з неоднаковими стандартами безпеки, створюючи нові вразливості...

Усвідомлення ризиків зростає, проте рівень впевненості залишається низьким: хоча 94% співробітників Національної служби охорони здоров'я (NHS) розуміють свої обов'язки щодо кібербезпеки, лише 36% вважають, що їхні системи належним чином підготовлені. Небезпеки є реальними та серйозними. Злом системи управління будівлею (BMS) під час спекотної погоди може призвести до маніпулювання системами клімат-контролю у вразливих палатах, а поширення програм-вимагачів з енергетичних платформ може вивести з ладу резервні генератори та критичну енергетичну інфраструктуру. Дослідження показують, що кожна хвилина відключення електроенергії в лікарні може коштувати понад 6 000 фунтів стерлінгів, але людські втрати від перерваних операцій, перенаправлених екстрених випадків та порушеного догляду за пацієнтами неможливо оцінити. Організовані злочинні угруповання навмисно націлюються на організації охорони здоров'я саме тому, що вони перебувають під сильним тиском щодо швидкого відновлення послуг, часто шляхом сплати викупу...

Замість того, щоб гальмувати цифрову трансформацію, яка є необхідною для управління старінням населення та досягнення цілей «Net Zero», сектор повинен з самого початку впровадити надійну кібербезпеку як одну з основних вимог. Це включає ізоляцію мереж управління енергоспоживанням від клінічних систем за допомогою правильно налаштованих брандмауерів та VLAN, впровадження безпечних протоколів зв'язку, таких як KNX Data Secure, із шифруванням та багатофакторною автентифікацією, а також забезпечення того, щоб усе обладнання — включаючи інтелектуальні автоматичні вимикачі — було ретельно сертифіковано щодо мережевої безпеки, контролю доступу та управління вразливостями. Атака на Synnovis має стати суворим нагадуванням про те, що кіберзагрози тепер виходять за межі викрадених даних і поширюються на інтелектуальні системи, які опалюють палати, забезпечують живлення обладнання для підтримки життєдіяльності та підтримують роботу лікарень. Тому кібербезпеку слід переосмислити не як додатковий IT-компонент, а як основний компонент безпеки пацієнтів і пріоритет першої лінії, рівнозначний самому клінічному персоналу. Технології для досягнення цього вже існують; необхідна лише фундаментальна зміна мислення». *(Nigel Thomas. Comment: Why cybersecurity matters // Healthcare Today (<https://healthcaretoday.com/article/comment-why-cybersecurity-matters>). 25.05.2026).*

Фішингові атаки

«Дослідники з безпеки компанії «Касперський» попередили, що зловмисники все частіше зловживають сервісом Amazon Simple Email Service (SES) для проведення фішингових кампаній, які обходять стандартні перевірки безпеки. Amazon SES — це легальна хмарна платформа для доставки електронної пошти, яка використовується для транзакційних та

маркетингових повідомлень. Оскільки вона базується на надійній інфраструктурі та протоколах автентифікації, таких як SPF, DKIM і DMARC, фішингові листи, надіслані через неї, можуть виглядати справжніми та обходити багато спам-фільтрів. За словами аналітика «Касперського» Романа Деденка, зловмисники отримують доступ до SES, використовуючи скомпрометовані облікові дані системи управління ідентифікацією та доступом AWS, які часто випадково виставляються у відкритих репозиторіях GitHub, файлах конфігурації, образах Docker або незахищених контейнерах S3. Отримавши доступ, вони можуть надсилати великі обсяги фішингових листів з IP-адрес, що не внесені до чорного списку, які, на перший погляд, походять із надійної інфраструктури Amazon...

Ці кампанії не спрямовані насамперед на викрадення облікових даних акаунтів Amazon, а націлені на інші платформи та спрямовані на здійснення шахрайських схем, таких як шахрайство з рахунками-фактурами. Хоча Amazon не є єдиною компанією, чії сервіси використовують для фішингу — подібні тактики застосовувалися щодо таких платформ, як PayPal і Google — компанія «Касперський» зазначає, що зловживання службою SES стає стійкою тенденцією. Проте Amazon заперечує наявність доказів зростання цієї тенденції та наголошує, що забороняє зловживання своїми послугами, розслідує повідомлення про порушення та закликає клієнтів захищати свої облікові записи й повідомляти про підозри щодо зловживань до служби AWS Trust & Safety...» (*Davey Winder. 'Uptick In Attacks'—Amazon Weaponized As Compromised Credentials Used // Forbes Media LLC. (<https://www.forbes.com/sites/daveywinder/2026/05/06/uptick-in-attacks-amazon-weaponized-as-compromised-credentials-used/>). 06.05.2026*).

«Дослідники з ANY.RUN виявили широкомасштабну фішингову кампанію, спрямовану на системи RMM (дистанційного моніторингу та управління), в рамках якої зловмисники використовують підроблені сторінки Microsoft, Adobe та OneDrive, щоб спонукати користувачів завантажувати легітимні інструменти дистанційного управління, такі як ScreenConnect та LogMeIn Rescue. Оскільки ці інструменти та інфраструктура, на якій розміщені фішингові сторінки (часто це легітимні платформи, наприклад n8n.cloud), окремо виглядають цілком нешкідливими, їх виявлення за допомогою традиційних засобів безпеки є надзвичайно складним... Ці атаки в основному спрямовані на сектори, що залежать від віддаленої ІТ-підтримки, зокрема на сфері освіти, технологій, банківської справи та державного управління, причому найвища активність спостерігається у США, Канаді, Європі та Австралії. У рамках цих кампаній користувач може натиснути на посилання, яке виглядає як завантаження файлу Adobe PDF, але замість цього отримує виконуваний файл або скрипт VBS, який таємно вимикає функції безпеки Windows, встановлює інструмент RMM та створює несанкціонований постійний віддалений доступ для зловмисника... Щоб протидіяти цьому, аналітики з безпеки не можуть покладатися виключно на репутацію домену або аналіз за допомогою статичних інструментів; вони повинні досліджувати весь ланцюжок атаки — від початкової фішингової приманки до виконання коду та підключення до мережі. ANY.RUN рекомендує використовувати

інтерактивні пісочниці для поведінкового аналізу, що забезпечує чітке уявлення про те, як зловживають цими легітимними інструментами, що в підсумку скорочує час на попередню оцінку загроз, мінімізує непотрібні ескалації та дозволяє швидше й точніше реагувати на загрози». (*Balaji N. New Phishing-to-RMM Attacks: How Analysts Can Detect Trusted-Tool Abuse Early // Cyber Security News (<https://cybersecuritynews.com/phishing-to-rmm-attacks-detection/>). 06.05.2026*).

«Доннча О'Сірбхайл (Donncha Ó Cearbhaill), який зазвичай розслідує кампанії з розповсюдження шпигунського ПЗ, сам став жертвою фішингової атаки в Signal, під час якої зловмисники видавали себе за «ChatBot служби підтримки безпеки Signal», повідомили про підозрілу активність і намагалися обманом змусити його надати код підтвердження, щоб прив'язати його обліковий запис до пристрою, який вони контролювали. О'Сірбхайл одразу розпізнав шахрайство і використав його для розслідування того, що, на його думку, є набагато ширшою кампанією, спрямованою проти користувачів Signal, з використанням тактики, що відповідає попередженням від CISA, британського агентства з кібербезпеки, та голландської розвідки, які пов'язують подібні спроби злому облікових записів Signal із суб'єктами, пов'язаними з російським урядом; Der Spiegel також повідомляв про успішні зломи в Німеччині, зокрема серед політиків... Не розкриваючи всіх своїх методів, О'Сірбхайл зазначив, що він виявив понад 13 500 цілей і спостерігав динаміку «сніжного кома», коли зламані групові чати відкривали зловмисникам доступ до нових контактів для подальших атак, при цьому зазначивши, що серед цілей були журналісти, з якими він раніше працював, а також його колега. Він також пов'язав цю операцію з автоматизованою системою масових атак під назвою «ApocalypseZ», виявив ознаки того, що інструментарій та інтерфейс оператора були російською мовою, а також побачив, що чати жертв перекладалися російською мовою, що підкріплює підозри про зв'язки з тією самою російською кампанією. Він продовжує стежити за цією активністю та очікує, що справжня кількість цілей є більшою, і радить стурбованим користувачам Signal увімкнути «Блокування реєстрації», яке використовує PIN-код, щоб запобігти реєстрації їхнього номера на іншому пристрої». (*Lorenzo Franceschi-Bicchieri. A spyware investigator exposed Russian government hackers trying to hijack Signal accounts // TechCrunch Media LLC. (<https://techcrunch.com/2026/05/14/a-spyware-investigator-exposed-russian-government-hackers-trying-to-hijack-signal-accounts/>). 14.05.2026*).

«У лютому 2026 року платформа «фішинг як послуга» EvilTokens успішно зламала понад 340 організацій, що використовують Microsoft 365, скориставшись структурною вразливістю сучасної кібербезпеки: зловживанням дозволом OAuth, або «фішингом згоди». Замість того, щоб викрадати паролі, зловмисники обманом змушують користувачів пройти легітимну багатофакторну автентифікацію (MFA) та натиснути на екрані згоди OAuth. Ця дія легально надає зловмиснику дійсний «токен оновлення» з тривалим терміном дії,

що дає доступ до конфіденційних даних, таких як електронні листи та диски. Оскільки цей процес імітує законну поведінку системи та відбувається після перевірки MFA, традиційні засоби захисту периметра та скидання паролів не можуть його виявити або зупинити; лише явне скасування токена може усунути цю вразливість...

Ця загроза стрімко зростає, оскільки користувачів привчили сліпо погоджуватися на екрани з запитом згоди для незліченної кількості сторонніх інтеграцій, розширень браузера та агентів штучного інтелекту. Ризик зростає, коли окремі користувачі надають доступ до декількох додатків, створюючи «токсичні комбінації» — несанкціоновані мости між різними системами (наприклад, CRM і спільний диск), які жоден власник додатка не може контролювати. Щоб боротися з цим, команди з безпеки повинні перенести свою увагу з традиційної аутентифікації на моніторинг рівня згоди. Експерти радять ставитися до додатків OAuth з суворим наглядом, постійно проводячи інвентаризацію сторонніх додатків, впроваджуючи політику регулярного поновлення згоди та використовуючи нові платформи безпеки на основі штучного інтелекту, такі як Reso. Ці платформи автоматично зіставляють ідентичності людей та нелюдей, відстежують дозволи OAuth та з'єднання агентів штучного інтелекту в режимі реального часу, а також дозволяють точно скасовувати доступи на рівні токенів, ефективно захищаючи рівень виконання, де фактично формуються сучасні мости доступу». (*The New Phishing Click: How OAuth Consent Bypasses MFA // The Hacker News* (<https://thehackernews.com/2026/05/the-new-phishing-click-how-oauth.html>). 19.05.2026).

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Артем Володимирович Ревенський, російський хакер, відомий під псевдонімом «Digit», погодився визнати свою провину за федеральними звинуваченнями США, пов'язаними з кібератаками на об'єкти критичної нафтогазової інфраструктури у Сполучених Штатах, Україні та кількох європейських країнах. Прокурори стверджують, що Ревенський був членом Sector16, хакерської групи, що фінансується російським урядом і націлена на країни, які вважаються противниками Москви. Йому висунуто звинувачення, зокрема у змові з метою пошкодження захищених комп'ютерів, електронному шахрайстві та крадіжці особистих даних, за що загалом передбачено покарання у вигляді позбавлення волі на строк до 27 років, хоча угода про визнання вини містить рекомендацію щодо пом'якшення покарання...

Згідно з судовими документами, у 2025 році угруповання Sector16 здійснило злом нафтогазових об'єктів у Техасі, Північній Дакоті, Нью-Йорку та Пенсильванії, в результаті чого на певний час отримало контроль над нафтовими насосами та системами зберігання. Група також націлилася на інфраструктуру в Україні,

зокрема на об'єкт з природного газу в Полтаві та АЗС у Києві, і обговорювала плани виведення з ладу всієї енергомережі України в обмін на виплати, які, за повідомленнями, становили десятки тисяч доларів. Прокурори стверджують, що Ревенський готував пропозиції, обіцяючи фізичні збитки, зокрема пожежі та вибухи, які могли б призвести до людських жертв. Група також взяла на себе відповідальність за атаки на інфраструктуру у Франції та Німеччині, хоча масштаби збитків залишаються нез'ясованими...

Ревенського заарештували в Домініканській Республіці в листопаді 2025 року та екстрадували до Сполучених Штатів. Окрім атак на інфраструктуру, прокуратура стверджує, що він допомагав фінансувати діяльність угруповання «Sector16» за допомогою глобальної шахрайської схеми з бронювання готелів, яка передбачала використання викрадених особистих даних та співучасть готелів, що дозволило отримати понад 150 000 доларів незаконних доходів». **(Patrick Howell O'Neill. Russian to Plead Guilty in Oil and Gas Facility Hack // Bloomberg L.P. (<https://www.bloomberg.com/news/articles/2026-05-01/russian-charged-in-oil-and-gas-facility-hacks-pleads-guilty>). 01.05.2026).**

«Міністерство юстиції США засудило 40-річного Райана Голдберга та 36-річного Кевіна Мартіна до чотирьох років ув'язнення кожного за їхню участь у атаках з використанням програм-вимагачів у 2023 році, здійснених як партнери операції «ALPHV/BlackCat» (RaaS — «програми-вимагачі як послуга»). Обидва чоловіки працювали у сфері кібербезпеки — Голдберг як менеджер з реагування на інциденти, а Мартін як переговорник з викупу — але замість того, щоб допомагати жертвам, вони використовували свої знання для здійснення вторгнень, розгортання програм-вимагачів та вимагання викупу з організацій, віддаючи 20% виручки від викупу операторам BlackCat в обмін на доступ до платформи та інфраструктури групи... У період з квітня по грудень 2023 року вони здійснили атаки на низку американських організацій і принаймні в одному випадку вимагали 1,2 мільйона доларів у біткойнах, які згодом були розділені та відмиті. У цій справі також фігурує співучасник Анджело Мартіно (41 рік), який визнав свою провину і чекає на винесення вироку; прокурори стверджують, що він зловживав своєю роллю переговорника, передаючи зловмисникам конфіденційну інформацію про жертв — таку як ліміти страхового покриття та стратегії переговорів — з метою збільшення вимог щодо викупу, а в деяких випадках допомагав розгортати шкідливе програмне забезпечення. Представники Міністерства юстиції США наголосили на тому, що така поведінка є зрадою довіри в екосистемі кібербезпеки. Винесення вироку відбулося на тлі більш масштабних заходів США проти угруповання BlackCat, зокрема конфіскації інфраструктури ФБР та випуску в 2023 році інструменту для розшифрування, який допоміг жертвам уникнути виплати викупу на суму, за оцінками, 99 мільйонів доларів». **(Filip TRUŤA. Four Years in Prison for Cybersecurity Pros Turned Ransomware Attackers // Bitdefender (<https://www.bitdefender.com/en-gb/blog/hotforsecurity/four-years-in-prison-for-cybersecurity-pros-turned-ransomware-attackers>). 04.05.2026).**

«Громадянин Латвії Деніс Золотарьов був засуджений до 102 місяців ув'язнення у федеральній в'язниці за те, що виступав посередником у переговорах від імені груп-вимагачів «Karakurt», «TommyLeaks» та «SchoolBoys Ransomware». Його заарештували за кордоном у грудні 2023 року, доставили до США в серпні 2024 року, а згодом він визнав себе винним у змові з метою відмивання грошей та електронного шахрайства. Прокурори заявили, що з червня 2021 року по березень 2023 року група здійснила атаки з використанням програм-вимагачів щонайменше проти 53 жертв, завдавши збитків на суму понад 56 мільйонів доларів, включаючи викрадення конфіденційної особистої інформації та медичних даних, а в одному випадку — виведення з ладу системи 911 урядової установи... Золотарьов не здійснював зломів особисто, але відіграв ключову роль, аналізуючи викрадені дані, ведучи переговори щодо виплати викупу та надаючи консультації щодо тактики вимагання, зокрема погрожуючи оприлюднити інформацію про пацієнтів дитячого віку, щоб чинити тиск на жертву з медичної галузі. Він отримував 10 відсотків від суми викупу, яку допомагав домогтися, а отримані кошти переказували через криптовалютні гаманці, перш ніж конвертувати їх у російські рублі. Американські чиновники заявили, що ця справа демонструє, що міжнародних кіберзлочинців можна переслідувати та покарати, незважаючи на їхні спроби сховатися за засобами анонімізації та іноземними локаціями, і вони висловили вдячність численним відділенням ФБР та міжнародним партнерам за допомогу в забезпеченні екстрадиції та розслідуванні». (*Global ransomware group negotiator involved in \$56 million cyberattacks sentenced to 8.5 years in prison // Department of Justice* (<https://www.justice.gov/usao-sdoh/pr/global-ransomware-group-negotiator-involved-56-million-cyberattacks-sentenced-85-years>). 04.05.2026).

«В результаті операції «Ramz» — масштабної міжнародної операції з боротьби з кіберзлочинністю під керівництвом Інтерполу — було вилучено 53 сервери, заарештовано 201 особу та встановлено особи ще 382 підозрюваних у країнах Близького Сходу та Північної Африки (MENA); кількість жертв, пов'язаних із припиненою злочинною діяльністю, склала 3 867 осіб. Операція тривала з жовтня 2025 року до 28 лютого 2026 року та охоплювала 13 країн, включаючи Алжир, Йорданію, Катар, Марокко, Оман та ОАЕ. Вона була спрямована проти фішингової інфраструктури, кампаній із поширення шкідливого програмного забезпечення, платформ «фішинг як послуга» та інвестиційних і фінансових шахрайств і була описана як перша регіональна ініціатива щодо боротьби з кіберзлочинністю такого масштабу... Слідчі обмінялися майже 8 000 розвідувальних матеріалів для забезпечення транскордонних операцій з протидії злочинній діяльності, а на національному рівні Катар вилучив зламані пристрої, які використовувалися для поширення шкідливого програмного забезпечення; Йорданія ліквідувала шахрайську схему з онлайн-торгівлі, викривши жертв торгівлі людьми, яких примушували до участі в шахрайських операціях, та заарештувала двох організаторів; Оман вимкнув заражений шкідливим програмним забезпеченням сервер у приватній оселі, який розкривав конфіденційні дані; Алжир

ліквідував платформу «фішинг як послуга» та заарештував підозрюваного; а Марокко вилучило пристрої, що містили банківські дані та інструменти для фішингу... Інтерпол співпрацював із партнерами з приватного сектору, такими як Group-IB, «Касперський», Shadowserver, Team Cymru та TrendAI, з метою виявлення інфраструктури та індикаторів компрометації. Ця робота здійснювалася за підтримки Міністерства внутрішніх справ Катару та за фінансової підтримки ЄС і проєкту «CyberSouth+» Ради Європи, що підкреслює як зростаючу витонченість регіональних кіберзлочинних мереж, так і необхідність постійного обміну розвідданими між державним і приватним секторами та спільних правоохоронних заходів». (*Abinaya. Operation Ramz Seizes 53 Servers Linked to Cyber Scams and Malware Threats // Cyber Security News (<https://cybersecuritynews.com/operation-ramz-seizes-53-servers/>). 19.05.2026*).

«Підрозділ Microsoft з боротьби з цифровими злочинами у співпраці з міжнародними партнерами, зокрема ФБР, Європолем та Resecurity, успішно ліквідував «Fox Tempest» — високоорганізовану кіберзлочинну групу, яка надавала послуги з підписання шкідливого програмного забезпечення як сервісу (MSaaS). Ця група давала змогу іншим зловмисникам обходити засоби захисту, підписуючи шкідливе програмне забезпечення короткостроковими підробленими сертифікатами, завдяки чому шкідливе програмне забезпечення виглядало легітимним і надійним для систем безпеки. Зловживаючи процесом підписання артефактів Microsoft, Fox Tempest створила понад 1 000 підроблених сертифікатів для підписання коду та керувала сотнями орендарів Azure для підтримки своєї незаконної платформи signspace.cloud. Діючи під виглядом легітимного бізнесу, група монетизувала свої послуги за допомогою багаторівневих планів передплати, стягуючи з клієнтів тисячі доларів за пріоритетний доступ до цих можливостей підписання...»

Фох Темпест виступала постачальником критично важливої інфраструктури для численних відомих угруповань, що займаються виманюванням викупу, та операторів шкідливого програмного забезпечення — зокрема Rhysida, INC, Qilin, Akira, Lumma Stealer та Vidar — надаючи їм можливість масово розповсюджувати шкідливі бінарні файли за допомогою шкідливої реклами та SEO-отруєння. Наслідки були серйозними і торкнулися секторів охорони здоров'я, освіти, державного управління та фінансів у всьому світі. У відповідь Microsoft вжила комплексних юридичних та технічних заходів, конфіскувавши інфраструктуру угруповання, анулювавши понад 1 000 сертифікатів та подавши позов проти Fox Tempest і пов'язаної з нею організації Vanilla Tempest, щоб забезпечити остаточне виведення з ладу їхніх серверів та доменів. Зараз Microsoft закликає організації впроваджувати багаторівневі стратегії захисту, такі як суворий контроль ідентифікації та правила зменшення площі атаки, водночас наголошуючи, що постійна співпраця між державним і приватним секторами є необхідною для протидії професійним, орієнтованим на надання послуг сучасним кіберзлочинним угрупованням». (*Pierluigi Paganini. Microsoft dismantled malware-signing network*

Технічні аспекти кібербезпеки

«Розроблена дослідницькою групою під керівництвом Мордехая Гурі з ізраїльського Університету імені Бен-Гуріона, ODINI — це складне шкідливе ПЗ для перевірки концепції, яке виявляє вразливості в комп'ютерах з «повітряним розривом», навіть якщо вони захищені клітками Фарадея. Зазвичай організації у військовій, фінансовій та критичній інфраструктурній галузях використовують ці фізичні ізоляційні бар'єри для захисту конфіденційних даних від електромагнітних перешкод та віддалених вторгнень у мережу. Однак ODINI демонструє, що система, інфікована через атаки на ланцюг постачання або скомпрометовані USB-накопичувачі, все одно може викрасти цінні активи, такі як паролі та ключі шифрування, шляхом маніпулювання центральним процесором (CPU) машини...

Шкідливе програмне забезпечення діє шляхом навмисної модуляції навантаження на процесор, створюючи динамічні коливання енергоспоживання, що, у свою чергу, генерує низькочастотні магнітні поля. Оскільки ці низькочастотні хвилі мають надзвичайно низький імпеданс, вони легко проникають крізь стандартні корпуси комп'ютерів та суцільне металеве екранування кліток Фарадея. Код передачі не вимагає адміністративних прав і використовує прості операції процесора, щоб уникнути виявлення звичайним антивірусним програмним забезпеченням. Застосовуючи сучасні схеми модуляції, такі як амплітудна та частотна маніпуляція, шкідливе програмне забезпечення точно кодує викрадені дані на ці магнітні хвилі...

У ході дослідження було виявлено два основні варіанти атаки. Стандартна техніка ODINI передбачає використання спеціального магнітного датчика, розміщеного на відстані від 100 до 150 сантиметрів від комп'ютера, що забезпечує швидкість передачі даних 40 біт на секунду. Другий варіант, названий MAGNETO, використовує ту саму маніпуляцію з процесором, але як приймач використовує вбудований магнітометр зараженого смартфона. Хоча MAGNETO є повільнішим — передача даних відбувається зі швидкістю 5 бітів на секунду на відстані 12,5 сантиметрів — він є особливо прихованим, оскільки працює навіть тоді, коли приймаючий телефон перебуває в режимі польоту або розміщений у сумці Фарадея.

Захист від такого витоку даних за допомогою магнітних полів є серйозним викликом. Стандартні клітки Фарадея неефективні проти низькочастотних передач, а спеціалізовані екрануючі матеріали, такі як муметал, часто виявляються занадто дорогими для практичного застосування. Експерти з безпеки пропонують використовувати апаратні засоби для заглушення сигналів, щоб перекрити приховані сигнали протилежним магнітним шумом, або програмні засоби, які створюють випадкові навантаження на процесор для порушення сигналу. Однак,

зрештою, найнадійнішим захистом залишаються суворі правила фізичного зонування, які забороняють перебування будь-яких зовнішніх електронних пристроїв у безпосередній близькості від чутливих систем з повітряним зазором...» (*Guru Baran. ODINI Malware Uses CPU Magnetic Emissions to Breach Faraday-Shielded Air-Gapped Computers // Cyber Security News (https://cybersecuritynews.com/odini-malware-air-gapped-computers/). 11.05.2026).*

Виявлені вразливості технічних засобів та програмного забезпечення

«Команда розробників Exim випустила версію Exim 4.99.2 для усунення чотирьох нещодавно виявлених вразливостей безпеки, які могли б дозволити зловмисникам викликати збій процесів поштового сервера, пошкодити пам'ять або спричинити витік конфіденційної інформації. Це вимагає негайного встановлення виправлень, оскільки Exim широко використовується як агент передачі повідомлень, підключений до Інтернету. Виправлені проблеми включають збій, спричинений DNS, на системах на базі musl, викликаний неправильно сформованими записами PTR (CVE-2026-40684), читання та запис за межами області, що може призвести до пошкодження купи, коли оператори JSON обробляють недійсний зовнішній вхід у пошкоджених конфігураціях (CVE-2026-40685), умову читання за межами області, пов'язану з неправильно сформованими заголовками з великими кінцевими символами UTF-8, що може призвести до витоку даних у електронних листах у межах одного з'єднання (CVE-2026-40686), та недоліки за межами області в аутентифікаторі SPA, які можуть призвести до збою екземпляра або витоку пам'яті купи під час взаємодії зі скомпрометованими зовнішніми службами SPA або NTLM (CVE-2026-40687)... У попередженні зазначається, що зловмисники часто сканують мережу в пошуках поштових серверів без оновлень, а також що підтримка старих версій Exim більше не здійснюється, що означає: застарілі системи можуть залишатися вразливими назавжди, якщо їх не оновити; адміністраторам рекомендується негайно оновити систему до версії 4.99.2 та перевірити перевірку заголовків і вхідних даних для JSON-даних та даних у форматі UTF-8, що надходять іззовні». (*Abinaya. Multiple Exim Mail Server Vulnerabilities Leads to Crash with Malicious DNS data // Cyber Security News (https://cybersecuritynews.com/exim-mail-server-vulnerabilities/). 02.05.2026).*

«Компанія Palo Alto Networks опублікувала термінове попередження щодо критичної уразливості «нульового дня» (CVE-2026-0300) у своєму порталі аутентифікації PAN-OS User-ID, яка наразі використовується в обмежених атаках. Уразливість пов'язана з переповненням буфера, що дозволяє неавторизованим зловмисникам виконувати довільний код з правами

суперкористувача на брандмауерах серій PA та VM, підключених до Інтернету, за допомогою спеціально сформованих пакетів. Організація з моніторингу загроз Shadowserver вказує, що понад 5 800 таких брандмауерів наразі знаходяться у мережі, переважно в Азії та Північній Америці... Оскільки патч безпеки для цієї уразливості найвищого рівня серйозності ще не випущено, Palo Alto Networks настійно закликає адміністраторів негайно мінімізувати ризик, обмеживши доступ до порталу виключно для надійних внутрішніх мереж або повністю вимкнувши портал автентифікації. Ця постійна загроза підкреслює тривожну тенденцію частих експлоїтів «нульового дня», спрямованих на системи PAN-OS в останні роки, що становить значний ризик для глобальної інфраструктури, враховуючи, що продукти безпеки компанії використовуються понад 70 000 організацій по всьому світу, включаючи 90% компаній зі списку Fortune 10 та більшість великих банків США...» (**Sergiu Gatlan. Palo Alto Networks warns of firewall RCE zero-day exploited in attacks // Bleeping Computer® LLC** (<https://www.bleepingcomputer.com/news/security/palo-alto-networks-warns-of-actively-exploited-firewall-zero-day/>). 06.05.2026).

«Дослідник у галузі безпеки Том Реннінг виявив, що Microsoft Edge розшифровує всі збережені паролі та завантажує їх у пам'ять у вигляді відкритого тексту під час кожного запуску браузера, де вони залишаються протягом усього сеансу — навіть якщо користувач ніколи не відвідує відповідні веб-сайти. Компанія Microsoft підтвердила, що така поведінка є передбаченою розробниками, зазначивши, що це сприяє швидшому входу в систему, а для її зловживання зловмиснику потрібно мати адміністративний доступ до пристрою... Однак Реннінг зазначив, що Edge, здається, є єдиним серед браузерів на базі Chromium, який обробляє паролі таким чином. Наприклад, Google Chrome розшифровує паролі лише тоді, коли це потрібно для автозаповнення, і використовує шифрування, прив'язане до програми (Application-Bound Encryption), щоб пов'язати ключі розшифрування з автентифікованим процесом браузера, що ускладнює зловмисникам вилучення облікових даних з пам'яті...

Хоча експерти визнають, що зловмисник із правами адміністратора фактично має повний контроль над системою, вони застерігають, що сучасне шкідливе програмне забезпечення для викрадення даних часто націлене саме на той момент, коли облікові дані з'являються в пам'яті. Тому зберігання паролів у відкритому вигляді в пам'яті протягом сеансу роботи браузера може підвищити ризик. Фахівці з безпеки зазвичай рекомендують взагалі уникати зберігання паролів у браузерах і замість цього використовувати спеціальний менеджер паролів для більш надійного захисту». (**Manisha Priyadarshini. Edge browser has a serious password safety problem, but Microsoft says it's by design // Digital Trends Media Group** (<https://www.digitaltrends.com/computing/microsoft-edge-has-a-serious-password-problem-and-microsoft-says-it-is-working-as-intended/>). 06.05.2026).

«Майже через тиждень після того, як cPanel і WebHost Manager (WHM) повідомили про критичну вразливість у своєму програмному забезпеченні для управління веб-серверами, хакери почали використовувати цю вразливість для масового злому веб-сайтів. Ця вразливість, що має номер CVE-2026-41940, дозволяє зловмисникам отримати повний контроль над уразливими серверами через їхні панелі управління. За даними Shadowserver, понад 550 000 серверів cPanel залишаються потенційно вразливими, і хоча кількість ймовірно скомпрометованих екземплярів зменшилася з приблизно 44 000 до близько 2 000, широкомасштабне зловживання вже відбулося...»

Минулого тижня дослідники у сфері безпеки повідомили про активні атаки, а серед доказів завданих збитків — веб-сайти, індексовані Google, на яких з'являлися повідомлення у стилі програм-вимагачів із заявами про те, що файли було зашифровано. Агентство з кібербезпеки та безпеки інфраструктури США (CISA) додало цю вразливість до свого каталогу відомих експлуатованих вразливостей і закликала урядові установи негайно встановити виправлення. Однак атаки, ймовірно, почалися задовго до публічного розкриття інформації, оскільки один хостинг-провайдер виявив підозрілу активність ще 23 лютого. Компанія cPanel підтвердила отримання запитів від ЗМІ, але не надала додаткових коментарів». ***(Lorenzo Franceschi-Bicchierai. Hackers are mass-exploiting the cPanel bug to gain control of thousands of websites // TechCrunch Media LLC. (<https://techcrunch.com/2026/05/04/hackers-are-still-exploiting-the-cpanel-bug-to-gain-control-of-thousands-of-websites/>). 04.05.2026).***

«Агентство з кібербезпеки та безпеки інфраструктури США (CISA) попередила, що зловмисники активно використовують нещодавно виявлену вразливість Linux під назвою «Copy Fail» (CVE-2026-31431) — лише через день після того, як дослідники з Theori опублікували деталі та експлойт для підтвердження концепції. Ця вразливість стосується криптографічного інтерфейсу algif_aead ядра Linux і дозволяє локальним користувачам без привілеїв отримати права суперкористувача шляхом запису чотирьох контрольованих байтів у кеш сторінок будь-якого файлу, доступного для читання. Theori описала свій експлойт на базі Python як «100% надійний», продемонструвавши успішне підвищення привілеїв на Ubuntu 24.04 LTS, Amazon Linux 2023, RHEL 10.1 та SUSE 16, і зазначила, що той самий експлойт працює без модифікацій у більшості основних дистрибутивів Linux, що використовують вразливі ядра, створені з 2017 року...»

Хоча провідні постачальники Linux вже почали випускати виправлення, CISA внесла цю вразливість до свого каталогу відомих експлуатованих вразливостей (KEV) і наказала федеральним цивільним агентствам США усунути вразливість у системах протягом двох тижнів, посилаючись на високий ризик, який становлять такі недоліки, що дозволяють підвищити привілеї. Хоча ця директива офіційно поширюється лише на федеральні агентства, CISA закликала всі організації надати пріоритет встановленню виправлень. Це попередження з'явилося після виправлення іншої давньої помилки в Linux, що дозволяла підвищувати привілеї,

що підкреслює постійні ризики, пов'язані з широко використовуваними компонентами з відкритим кодом». (*Sergiu Gatlan. CISA says 'Copy Fail' flaw now exploited to root Linux systems // Bleeping Computer® LLC (<https://www.bleepingcomputer.com/news/security/cisa-says-copy-fail-flaw-now-exploited-to-root-linux-systems/>). 04.05.2026*).

«Компанія Progress Software попередила, що зловмисники можуть скористатися двома нещодавно виявленими вразливостями в її інструменті керованого обміну файлами MOVEit Automation для отримання несанкціонованого доступу до даних організацій. Серед цих вразливостей — критична проблема, що дозволяє обійти аутентифікацію (CVE-2026-4670), та вразливість високого рівня, що дозволяє підвищити привілеї (CVE-2026-5174), які в сукупності можуть призвести до несанкціонованого доступу, отримання адміністративного контролю та витоку даних. Progress випустила виправлення та закликала клієнтів оновити програмне забезпечення до останньої версії за допомогою повного інсталятора, зазначивши, що це єдиний ефективний спосіб усунення проблеми, який вимагатиме тимчасового вимкнення програмного забезпечення... Дані сканування Інтернету свідчать, що понад 1 440 пристроїв, доступних з відкритого Інтернету, досі працюють на вразливих версіях, зокрема системи, пов'язані з державними та місцевими урядовими установами. Програма MOVEit привернула до себе підвищену увагу після того, як у 2023 році уразливість «нульового дня» стала причиною масштабної хакерської кампанії за участю групи-вимагачів Cl0p». (*Eric Geller. New MOVEit vulnerabilities prompt urgent patch warning // TechTarget, Inc. (<https://www.cybersecuritydive.com/news/moveit-vulnerabilities-authentication-bypass-privilege-escalation/819187/>). 04.05.2026*).

«Дослідники у сфері кібербезпеки закликають мільярди користувачів WhatsApp негайно оновити додаток після того, як компанія Meta повідомила про дві уразливості, що впливають на те, як WhatsApp обробляє медіавкладення та попередній перегляд файлів на Android, iOS та Windows. Ці уразливості можуть дозволити зловмисникам маскувати шкідливі файли під виглядом законних документів — що потенційно може призвести до виконання шкідливого коду при відкритті на уразливих пристроях з Windows — або зловживати попереднім переглядом мультимедійних файлів та зовнішніми URL-адресами на мобільних пристроях для перенаправлення користувачів на небезпечний контент. Хоча немає доказів того, що ці проблеми вже використовуються в реальних умовах, експерти попереджають, що вони можуть значно підвищити ризик фішингу, поширення шкідливого програмного забезпечення та шахрайства за допомогою соціальної інженерії, включаючи дедалі більш витончені атаки «вішингу», що використовують дзвінки, голосові нотатки або аудіо, згенероване штучним інтелектом... Уразливості, зареєстровані під номерами CVE-2026-23863 та CVE-2026-23866 і виявлені в рамках програми винагороди за виявлення помилок компанії Meta, були усунені в останніх версіях

WhatsApp. Користувачам рекомендується оновити програму через офіційні магазини додатків та канали для настільних ПК, уникати відкриття невідомих вкладень та переходу за підозрілими посиланнями, увімкнути двофакторну автентифікацію та самостійно перевіряти термінові або незвичайні запити. Це попередження з'явилося на тлі нещодавніх проблем із безпекою WhatsApp, таких як фішингові кампанії, шкідливі групові файли та спроби захоплення облікових записів, що ще раз підкреслює: оновлення програмного забезпечення залишається одним із найефективніших засобів захисту». (**Daniel Tannenbaum. Cybersecurity Experts Urge WhatsApp Users to Update App Following Discovery of Two New Security Flaws** // **Solihull Observer** (<https://solihullobservers.co.uk/lifestyle/cybersecurity-experts-urge-whatsapp-users-to-update-app-following-discovery-of-two-new-security-flaws/>). 08.05.2026).

«Компанія Anthropic запустила публічну програму винагород за виявлення вразливостей на платформі HackerOne, розширивши таким чином канал повідомлень про проблеми безпеки порівняно з попередніми, більш обмеженими ініціативами, та запропонувавши винагороди, розмір яких залежить від рівня серйозності за шкалою CVSS, за вразливості, виявлені в широкому спектрі ресурсів, що належать Anthropic, зокрема Claude.ai, API Anthropic, Claude Code, настільних та мобільних клієнтів, внутрішньої інфраструктури, SDK, та інтеграції MCP і розширення Chrome, розроблені Anthropic, включаючи при цьому такі області, як сторонні сервери MCP, архівні репозиторії з відкритим кодом, соціальна інженерія та інформаційні проблеми з низьким рівнем серйозності. Цей крок є продовженням програми розкриття вразливостей від серпня 2024 року, яка функціонувала переважно як канал повідомлення і тепер перенаправляє дослідників до нової програми винагород, і він з'являється через місяць після того, як Anthropic представила Claude Mythos та Project Glasswing — ініціативу з кібербезпеки з обмеженим доступом для більш просунутої моделі, яка, за словами Anthropic, може ефективніше виявляти та пов'язувати вразливості, але яка обмежена обраними партнерами, такими як Amazon, Microsoft, Cisco, CrowdStrike та Linux Foundation, щоб посилити оборонні можливості до того, як поширяться наступальні методи використання... Запуск традиційної програми винагород, що керується людьми, на тлі гучних заяв про виявлення вразливостей, пов'язаних з діяльністю агентів, підкреслює, що традиційні зовнішні дослідження все ще мають значення для безпеки в реальному світі, і посилив скептицизм щодо того, наскільки перевіреними є заяви Mythos, включаючи критику з боку дослідників, які стверджують, що Anthropic не забезпечила достатньої прозорості тестування, даних про помилкові спрацювання або незалежної перевірки, а також може розмивати межу між виявленням вразливостей і демонстрацією реального впливу; деякі аналізи також показали, що менші моделі з відкритою вагою можуть відтворювати частину рекламаних можливостей. Водночас Британський інститут безпеки штучного інтелекту повідомив, що модель Mythos Preview показала високі результати в контрольованих багатоетапних симуляціях кібератак та експертних

СТФ-завданнях, зокрема, виконавши складний сценарій захоплення мережі ефективніше, ніж попередні передові моделі, водночас застерігаючи, що такі результати можуть не переноситися на добре захищені виробничі середовища... Загалом, запуск програми винагород свідчить про те, що, незважаючи на те, що компанія Anthropic просуває передові кібермоделі, вона все ще покладається на всебічну незалежну перевірку з боку людей — особливо у випадку таких високоризикових агентних кодувальних середовищ, як Claude Code, де критичними проблемами можуть бути несанкціоноване виконання команд, обхід обмежень доступу або використання прихованих інструментів». (*Paul Sawers. Anthropic puts the “myth” in Mythos with its HackerOne bug bounty program // The New Stack (<https://thenewstack.io/anthropic-public-bug-bounty/>). 10.05.2026*).

«Згідно з квартальним звітом про загрози від Beazley Security за 1 квартал 2026 року, кількість уразливостей, що зазнали експлуатації, зросла на 43% у перші три місяці року, що було спричинено атаками на ланцюги постачання з використанням штучного інтелекту та різким зростанням кількості активно експлуатованих уразливостей типу «нульового дня». Протягом кварталу було виявлено понад 15 200 нових вразливостей, у тому числі майже 3 900 з високим рівнем ризику, а кількість записів у каталозі відомих експлуатованих вразливостей CISA зросла на 43% порівняно з 4 кварталом 2025 року, що свідчить про прискорення процесу їхнього використання в реальних умовах; компанія Beazley також зафіксувала 15-відсоткове зростання кількості повідомлень клієнтам про критичні вразливості «нульового дня», багато з яких впливають на периферійну інфраструктуру, таку як VPN та брандмауери... Після спокійного початку березня сталося дві значні події: автономний агент штучного інтелекту просканував публічні репозиторії коду, виявив неправильно налаштовані засоби контролю доступу та сприяв злому широко використовуваного сканера безпеки з відкритим кодом Trivy; а також група хактивістів, пов'язана з Іраном, здійснила атаку на виробника медичного обладнання Stryker, зловживаючи Microsoft Intune для віддаленого стирання даних з понад 200 000 систем по всьому світу. У звіті наголошується на атаках на ланцюжок постачання розробників як на ключовій тенденції, наводячи приклад використання TeamPSR агента штучного інтелекту («hackerbot-claw») для експлуатації неправильних налаштувань CI/CD GitHub та зараження Trivy шкідливим програмним забезпеченням для викрадення облікових даних, що створює каскадний ризик для нижчестоящих інструментів та організацій, таких як LiteLLM, та підкреслює зосередження зловмисників на нелюдських ідентичностях та конвеєрах автоматизації... Кількість випадків використання програм-вимагачів залишалася в основному стабільною: основним каналом проникнення, як і раніше, були викрадені облікові дані (74% зафіксованих вторгнень), при цьому спостерігалось зростання кількості операцій, спрямованих виключно на вимагання викупу, під час яких дані викрадаються без їхнього шифрування. Загалом компанія Beazley робить висновок, що зловмисники не так змінюють тактику, як використовують автоматизацію на основі штучного інтелекту та надійні платформи для здійснення атак швидше та в більших масштабах, що

підкреслює необхідність впровадження надійних базових заходів контролю поряд із вдосконаленням систем захисту ланцюга поставок та захисту від уразливостей «нульового дня». (*Exploited vulnerabilities jump 43% in Q1 as cyber criminals leverage AI for more effective attacks - Beazley Security // Cision US Inc. (<https://www.prnewswire.com/news-releases/exploited-vulnerabilities-jump-43-in-q1-as-cyber-criminals-leverage-ai-for-more-effective-attacks---beazley-security-302769253.html>). 12.05.2026*).

«Цього місяця у сфері кібербезпеки відбулася значна подія: кількість виправлень уразливостей зростає до безпрецедентного рівня, що свідчить про перехід до ери безпеки зі «швидкістю штучного інтелекту». Тільки цього місяця Google Chrome виправив 127 уразливостей в одному оновленні — це значне збільшення порівняно зі звичайним діапазоном від шести до 30 — тоді як у останньому оновленні Microsoft «Patch Tuesday» було виправлено 138 CVE. З понад 500 уразливостями, виправленими з січня, Microsoft наразі йде до того, щоб побити свій річний рекорд. Ця різка висхідна крива пов'язана насамперед із тим, що дослідники безпеки дедалі частіше використовують інструменти на базі штучного інтелекту; наприклад, Mozilla використала штучний інтелект Claude Mythos, щоб виявити 400 уразливостей у коді Firefox лише у квітні...

Однак цей сплеск активності, зумовлений штучним інтелектом, має й негативні наслідки. Деякі організації, такі як хмарний провайдер Nextcloud, були змушені тимчасово призупинити свої програми винагороди за виявлення вразливостей через надмірний наплив автоматизованих повідомлень низької якості, які є «сміттям ШІ». Що ще гірше, ця технологія створює небезпечну асиметрію: хоча ШІ допомагає захисникам швидше виявляти вразливості, він також дозволяє зловмисникам з такою самою швидкістю здійснювати реверс-інжиніринг виправлень і перетворювати експлойти на зброю. Останні дані вказують на «середній час до експлуатації» у мінус сім днів, що означає, що зловмисники регулярно експлуатують вразливості ще до того, як про них стає відомо громадськості...

Цю ситуацію називають «фазою Уробороса» (Ouroboros phase) у сфері кібербезпеки, коли швидкість виявлення загроз за допомогою машин перевищує людські можливості щодо їх усунення. Експерти застерігають: якщо організації не зможуть зрівняти швидкість виявлення з швидкістю усунення, ІТ-відділи ризикують перетворитися на «безплатних стажерів для машин», які змушені боротися з нескінченним циклом виявлених машинами вразливостей, що залишають системи постійно незахищеними». (*Davey Winder. Ouroboros of cybersecurity is confirmed as the AI vulnerability disclosure cycle eats itself // TechFinitive (<https://www.techfinitive.com/ouroboros-of-cybersecurity-is-confirmed-as-the-ai-vulnerability-disclosure-cycle-eats-itself/>). 14.05.2026*).

«Компанія Rapid7 Labs виявила критичну уразливість, що дозволяє обійти систему автентифікації (CVE-2026-20182), яка впливає на контролер

Cisco Catalyst SD-WAN (раніше відомий як vSmart). Ця вразливість, що має максимальний бал CVSS 10,0, знаходиться у службі «vdaemon» на UDP-порту 12346, яка відповідає за критично важливі комунікації на рівні управління, включаючи структуру маршрутизації SD-WAN-оверлею. Помилка пов'язана з несправністю логіки встановлення з'єднання пристрою: коли підключений вузол ідентифікує себе як пристрій типу «vHub» під час процесу автентифікації, контролер пропускає всі етапи перевірки сертифікатів та підписів і беззастережно позначає вузол як «автентифікований». Як наслідок, віддалений неавтентифікований зломисник може повністю обійти заходи безпеки, не потребуючи дійсних облікових даних або сертифікатів, підписаних центром сертифікації...

Як тільки зломисник отримає цей статус автентифікованого користувача, він зможе скористатися уразливістю системи для введення шкідливого відкритого ключа у файл авторизованих SSH-ключів користувача vmanage-admin. Ця дія надає зломиснику постійний доступ з високим рівнем привілеїв до контролера через службу NETCONF на TCP-порту 830, що дозволяє йому виконувати довільні команди та фактично скомпрометувати всю інфраструктуру маршрутизації SD-WAN. Компанія Cisco підтвердила наявність уразливості та випустила оновлення програмного забезпечення для усунення цієї проблеми. Оскільки обхідних рішень немає, організаціям, що використовують уражений контролер Cisco Catalyst SD-WAN, настійно рекомендується негайно оновити програмне забезпечення до виправлених версій, зазначених в офіційному повідомленні Cisco Security Advisory, щоб зменшити ризик повного компрометації мережі». (*Jonah Burgess, Stephen Fewer. CVE-2026-20182: Critical authentication bypass in Cisco Catalyst SD-WAN Controller (FIXED) // Rapid7 (<https://www.rapid7.com/blog/post/ve-cve-2026-20182-critical-authentication-bypass-cisco-catalyst-sd-wan-controller-fixed/>). 14.05.2026*).

«Дослідники з компанії Cyera попередили, що зломисники можуть поєднати чотири вразливості в платформі автономних ШІ-агентів з відкритим кодом OpenClaw, які на сьогодні вже виправлені (і які разом отримали назву «Claw Chain»), щоб перейти від початкового проникнення до постійного контролю на системному рівні, що дасть змогу викрасти облікові дані та встановити бекдори. Найбільш критична проблема (CVE-2026-44112, CVSS 9.6), що впливає на всі версії OpenClaw, випущені до 23 квітня 2026 року, використовувала розбіжність між часом перевірки та часом використання в пісочниці, дозволяючи зломиснику змінювати умови між перевіркою безпеки та виконанням, щоб перенаправити записи за межі пісочниці та втрутитися в конфігурацію хоста для забезпечення стійкості... Шлях атаки доповнювали ще три уразливості: CVE-2026-44115 призводила до розкриття змінних середовища через зловживання прогалиною між перевіркою команди та виконанням оболонки; CVE-2026-44118 дозволив локально запущеному процесу з дійсним токеном підвищити рівень контролю до рівня власника, оскільки OpenClaw довіряв контрольованому клієнтом прапорцю власності без перевірки на стороні сервера; а CVE-2026-44113 дозволив вийти з пісочниці під час читання, замінивши

перевірений шлях до файлу на перенаправлення для доступу до системних файлів та внутрішніх облікових даних. Дослідники зазначили, що оскільки агент виконує дії, використовуючи легітимні привілеї та робочі процеси, зловмисна діяльність може нагадувати нормальну поведінку агента та уникнути традиційних засобів контролю, розширюючи радіус ураження та ускладнюючи виявлення... За оцінками компанії Cyera, отриманими за допомогою Shodan і ZoomEye, приблизно 245 000 серверів OpenClaw можуть бути доступними з відкритого Інтернету, причому на багатьох із них, ймовірно, відсутні засоби аутентифікації або мережеві обмеження. Швидке поширення цієї платформи — яка спочатку була запущена під назвою Clawdbot і за три місяці стала проектом GitHub із найбільшою кількістю зірочок — супроводжувалося численними проблемами безпеки: було опубліковано сотні попереджень, пов'язаних із виконанням команд та витоком облікових даних. Експерти також попередили, що особисте використання таких агентів може стати точкою входу в підприємство, коли ці агенти контактують з робочими пристроями, обліковими даними або системами, перетворюючи кінцевих користувачів на шлях до компрометації організації». *(Rashmi Ramesh. Patched OpenClaw Flaws Let Hackers Hijack AI Agents // Information Security Media Group, Corp. (<https://www.inforisktoday.com/patched-openclaw-flaw-let-hackers-hijack-ai-agents-a-31720>). 19.05.2026).*

«...Критична вразливість, що дозволяє обійти аутентифікацію (CVE-2024-9643), наразі спричиняє сплеск активності масштабних ботнетів, спрямованих проти промислових стільникових маршрутизаторів Four-Faith F3x36. Ця вразливість, що має рейтинг CVSS 9,8, пов'язана з жорстко заданими адміністративними обліковими даними, вбудованими у веб-інтерфейс управління пристроєм, що дозволяє неавторизованим зловмисникам отримати повні адміністративні привілеї та виконувати довільні команди. З моменту її розкриття експлуатація цієї уразливості перейшла у фазу «масового використання», при цьому зловмисники використовують глобально розподілену мережу скомпрометованих пристроїв для інтеграції маршрутизаторів у ботнети. Ці скомпрометовані системи в основному використовуються для запуску розподілених атак типу «відмова в обслуговуванні» (DDoS), проксі-трафіку зловмисного характеру та слугують плацдармом для горизонтального переміщення у більш чутливі внутрішні корпоративні або промислові мережі... Оскільки ці маршрутизатори широко використовуються на периферії мережі у віддалених середовищах — таких як склади, комунальні підприємства та філії — де за ними часто недостатньо стежать і їх рідко оновлюють, вони стали привабливими довгостроковими цілями для кіберзлочинців. Щоб зменшити ці ризики, організаціям настійно рекомендується негайно встановлювати оновлення прошивки, обмежувати доступ до інтерфейсів управління за допомогою брандмауерів або VPN, а також впроваджувати постійний моніторинг мережі для виявлення та блокування підозрілих вихідних з'єднань, пов'язаних із цими тривалими кампаніями ботнетів». *(Abinaya. Hackers Hijacking Four-Faith Industrial Routers for Botnet Activity // Cyber Security News*

(<https://cybersecuritynews.com/hijacking-four-faith-industrial-routers-for-botnet/>). 19.05.2026).

«Звіт Verizon про розслідування випадків витоку даних за 2026 рік, заснований на аналізі понад 31 000 інцидентів безпеки та понад 22 000 підтверджених випадків витоку даних у 145 країнах з листопада 2024 року по жовтень 2025 року, показує, що експлуатація вразливостей стала провідним вектором початкового доступу, на який припадає близько третини відомих випадків витоку даних, за ним йдуть зловживання обліковими даними (13%), а потім фішинг та інші методи соціальної інженерії. У звіті міститься попередження про те, що ефективність виправлення вразливостей погіршується навіть на тлі зростання їхньої кількості: минулого року організації виправили лише близько чверті критичних вразливостей (у порівнянні з 38% у попередньому році) і витратили на це більше часу (в середньому 43 дні проти 32), тоді як навіть найефективніші команди виправили лише 30–40% активно експлуатованих вразливостей протягом першого тижня; виправлення також відбувається повільно в хмарних середовищах сторонніх розробників, де відсутність або неправильна конфігурація MFA, слабкі паролі та проблеми з дозволами часто зберігаються протягом місяців... Активність, пов'язана з програмним забезпеченням-вимагачем, продовжує зростати і зараз фігурує приблизно в половині випадків порушення безпеки (48%, порівняно з 44%), включаючи випадки вимагання викупу лише за дані та крадіжки з організацій або їхніх постачальників послуг; більшість виявлених жертв не платили (69%), а в тих випадках, коли виплати все ж відбувалися, середня сума знизилася приблизно до 140 000 доларів. Verizon також пов'язує тенденцію до поширення програм-вимагачів із зростаючою роллю третіх сторін (залучених приблизно до половини випадків порушення безпеки) і зазначає, що у багатьох жертв програм-вимагачів виявлено ознаки крадіжки облікових даних або зараження інфостілерами за кілька тижнів до атаки. Хоча період, за який зібрано дані, закінчується до останнього сплеску популярності агентних інструментів штучного інтелекту, у звіті наводяться показники на початок 2026 року, які свідчать про те, що штучний інтелект прискорює дослідження вразливостей та їх використання як зброї і може допомогти автоматизувати етапи атаки, хоча більшість шкідливих програм, створених штучним інтелектом, які спостерігалися досі, використовують звичні, а не нові техніки, що підкріплює висновок Verizon про те, що захист вимагає «удосконалення, а не революції» і що міцні основи та управління ризиками залишаються найефективнішою відповіддю в умовах прискорення атак». (*Mathew J. Schwartz. Verizon Breach Report: Vulnerability Exploitation Surges // Information Security Media Group, Corp.* (<https://www.databreachtoday.co.uk/verizon-breach-report-vulnerability-exploitation-surges-a-31719>). 19.05.2026).

«Агентство з кібербезпеки та безпеки інфраструктури (CISA) запровадило нову форму публічного повідомлення, яка дозволяє постачальникам

технологій, незалежним дослідникам та іншим експертам з безпеки подавати пропозиції щодо включення вразливостей до каталогу «Відомі вразливості, що експлуатуються» (KEV). Ця ініціатива покликана посилити здатність CISA швидко виявляти та поширювати інформацію про вразливості, які активно експлуатуються хакерами. За словами представників CISA, раннє виявлення та скоординоване розкриття інформації про вразливості є критично важливими інструментами для зменшення ризиків у сфері кібербезпеки у великому масштабі.

У формі повідомлення вимагається надати детальну інформацію про вразливість, зокрема її номер CVE, докази активного використання, рекомендації щодо усунення ризику, а також зазначити, чи впливає вона на декілька продуктів або постачальників. Цей крок зроблено після критики, що CISA раніше повільно оновлювала каталог KEV, а деякі експерти описували його як запізнілий індикатор поточних кібератак. З моменту запуску в листопаді 2021 року каталог KEV швидко розширився і зараз містить близько 1 600 вразливостей. CISA продовжує розширювати та часто оновлювати каталог, що відображає зростання кількості активно експлуатованих програмних недоліків...

Зростаюче значення каталогу KEV також підкреслює більш загальні проблеми в сфері управління вразливостями в державних установах. У той час як CISA розширює свій каталог, Національний інститут стандартів і технологій (NIST) визнав, що йому важко встигати за великим обсягом нещодавно виявлених вразливостей. Нещодавно NIST оголосив, що скоротить деякі свої зусилля з розширення бази даних про вразливості та зосередиться переважно на найсерйозніших загрозах. У сукупності ці події ілюструють зростання масштабів та складності управління ризиками кібербезпеки, оскільки відомства шукають ефективніші способи відстеження та реагування на вразливості, що експлуатуються». (*Eric Geller. CISA asks cybersecurity community to alert it to vulnerability exploitation // TechTarget, Inc. (https://www.cybersecuritydive.com/news/cisa-cve-vulnerability-exploitation-nominations/820870/). 21.05.2026*).

Технічні та програмні рішення для протидії кібернетичним загрозам

«Компанія Greylock очолила раунд початкового фінансування на суму 45 мільйонів доларів для Sylake — нового стартапу, який прагне створити систему кібербезпеки на базі штучного інтелекту з агентною архітектурою, призначену для клієнтів, яким необхідний повний контроль над своїми даними. Sylake заснували троє відомих ветеранів галузі безпеки: Нір Зук, засновник і багаторічний технічний директор Palo Alto Networks; Вілсон Сю, який пропрацював понад десять років у Palo Alto Networks і очолював її інженерну організацію; та Ехуд (Уді) Шамір, співзасновник SentinelOne, який згодом працював видатним інженером у Palo Alto Networks... Підхід компанії

зосереджений на використанні комплексних даних та контексту в рамках єдиної платформи безпеки, але з повним забезпеченням її функціонування виключно в суверенному середовищі самого клієнта — для великих організацій, що є об'єктом цілеспрямованих атак і не можуть використовувати продукти безпеки на базі публічних хмарних сервісів через нормативні обмеження або вимоги безпеки. Greylock підкреслила свої давні відносини з Зуком, що сягають часів Check Point та її ранніх інвестицій у Palo Alto Networks, і заявила, що співпрацює з Cylake, щоб запровадити сучасну безпеку на основі штучного інтелекту на ринку, де інновації відстають для клієнтів, обмежених суверенними вимогами». **(Asheem Chandna. Introducing Cylake: AI-Native Cybersecurity with Total Data Sovereignty // Greylock Partners (https://greylock.com/portfolio-news/introducing-cylake-ai-native-cybersecurity-with-total-data-sovereignty/). 03.05.2026).**

«Компанія Avast запустила оновлену платформу Avast One, яка покликана стирати традиційну межу між безкоштовним і платним антивірусом. Для цього вона пропонує потужний базовий набір безкоштовних функцій — провідний у галузі антивірус, захист від шахрайства та веб-захист — через єдину панель управління, а потім дозволяє користувачам додавати функції у вигляді модульних доповнень, замість того щоб купувати жорсткі абонентські пакети з набором інструментів, якими вони, можливо, не користуватимуться... До додаткових модулів входять засоби захисту та сервіси, такі як захист за допомогою штучного інтелекту, VPN без ведення журналів, моніторинг витоків даних та очищення пристроїв; деякі з цих додатків у базовій версії надаються безкоштовно, наприклад, інструмент очищення для звільнення місця на диску та видалення непрацюючих ярликів, а також BreachGuard для захисту персональних даних, який перевіряє їх на витік та допомагає зменшити кількість цільової реклами... Для більш складних потреб користувачі можуть придбати такі розширені функції, як «Преміум-захист» для захисту від підозрілих електронних листів, банківських операцій та віддаленого доступу, SecureLine VPN (з 60-денною пробною версією), а також преміум-версії Cleanup і BreachGuard, що додають сповіщення про витік даних, поглиблене сканування на наявність зломів та додаткові рекомендації щодо конфіденційності, завдяки чому платформа позиціонується як настроюваний пакет засобів безпеки за принципом «платіть лише за те, що вам потрібно». **(Benedict Collins. Avast unveils revolutionary new modular antivirus platform – industry leading device protection & scam detection, with optional no-log VPN, data breach monitoring, and device cleanup // Future US, Inc. (https://www.techradar.com/pro/security/avast-unveils-revolutionary-new-modular-antivirus-platform-industry-leading-device-protection-and-scam-detection-with-optional-no-log-vpn-data-breach-monitoring-and-device-cleanup). 19.05.2026).**

«SilentGlass — це пристрій для кібербезпеки, розроблений Національним центром кібербезпеки (NCSC) Великої Британії, що входить до складу GCHQ, для протидії зростаючій загрозі, пов'язаній із дедалі «розумнішими»

комп'ютерними моніторами та цифровими відеопідключеннями. У таких середовищах, як захищені урядові об'єкти, гібридні робочі місця та домашні офіси, ці підключення потенційно можуть бути використані для злому ноутбуків та інших підключених пристроїв, особливо в тих випадках, коли обладнання з різними рівнями довіри використовує один і той самий монітор. SilentGlass було створено як просте апаратне рішення типу «plug-and-play», яке встановлюється між ноутбуком і монітором, блокуючи використання цього фізичного з'єднання як шляху для кібератаки, тим самим підвищуючи безпеку та підтримуючи безпечніше спільне використання робочих місць і гнучкий графік роботи. Спочатку розроблена для внутрішнього урядового використання, ця технологія продемонструвала ширший потенціал у державному секторі, критичній національній інфраструктурі та приватних підприємствах з високими вимогами до кібербезпеки... Щоб вивести продукт на ринок, одночасно забезпечивши ефективне управління та контроль за безпекою, NCSC обрав підхід до комерціалізації, заснований на ліцензуванні. Управління з питань передачі технологій (GOTT) відіграло важливу роль у цьому процесі, надаючи консультації щодо ліцензування інтелектуальної власності, фінансуючи та надаючи наставництво місцевому менеджеру з управління інтелектуальними активами, налагоджуючи зв'язки NCSC із ширшою екосистемою передачі технологій та підтримуючи стратегію ліцензування в уряді. Ця допомога дозволила NCSC ефективно керувати процесом комерціалізації та знайти відповідного партнера шляхом проведення справедливої та конкурентної процедури... У результаті було укладено угоду про надання глобальної ліцензії на інтелектуальну власність щодо SilentGlass з британською компанією, і тепер цей пристрій доступний у всьому світі. Це дозволяє використовувати технологію кібербезпеки з високим рівнем надійності, яка спочатку була розроблена для урядових потреб, на користь значно ширшого кола організацій, а також демонструє, як інновації та інтелектуальна власність державного сектору можуть бути комерціалізовані для підтримки як національної безпеки, так і економічного зростання». (*HM Government licensing cyber security tech for a global market // GOV.UK* (<https://www.gov.uk/government/case-studies/hm-government-licensing-cyber-security-tech-for-a-global-market>). 20.05.2026).

Основи кібергігієни

«Згідно зі звітом «State of Passkeys 2026», опублікованим альянсом FIDO, поширення серед споживачів засобів аутентифікації без паролів досягло значних рубежів, хоча інерція організацій продовжує гальмувати їхнє широке впровадження в корпоративному секторі. На основі опитування 11 000 споживачів та 1 400 ІТ-керівників у 10 країнах у звіті було виявлено, що 90% споживачів зараз знають про парольні ключі, а 75% використовують їх принаймні для деяких облікових записів. Ця зміна зумовлена очевидними перевагами парольних ключів, які забезпечують надійний захист від фішингу, замінюючи вразливі паролі біометричною автентифікацією. Оскільки приблизно третина

споживачів повідомила про злом облікових записів протягом останнього року, а багато хто відмовився від онлайн-транзакцій через втому від паролів, очевидним є суспільний попит на більш безпечну та зручну аутентифікацію...

Однак у звіті наголошується на значному розриві між готовністю споживачів та діями підприємств. Хоча 68% організацій у всьому світі активно тестують або впроваджують парольні ключі, лише 30% перейшли на їх використання як основного методу автентифікації. Більшість підприємств — 57% у всьому світі — досі покладаються на системи, що базуються на паролях, які залишаються вразливими до фішингових атак. ІТ-відділи часто згадують такі перешкоди, як несумісність із застарілими системами, труднощі з отриманням схвалення бюджету, а також обґрунтовані побоювання щодо відновлення облікових записів та пристроїв. Зрештою, хоча перехід до майбутнього без паролів для споживачів вже йде повним ходом, у звіті робиться висновок, що підприємствам необхідно подолати значну інституційну та технічну інерцію, щоб ефективно захистити свої цифрові середовища від постійних ризиків, пов'язаних із сучасними кіберзагрозами». (*Rob Pegoraro. Passkey-Adoption Report Finds Many Orgs Don't Know How to Quit Passwords // Ziff Davis, LLC. (<https://uk.pcmag.com/security/164821/passkey-adoption-report-finds-many-orgs-dont-know-how-to-quit-passwords>). 07.05.2026*).

«Опитування 1 200 американців, проведене на замовлення NordVPN, свідчить про те, що кіберзлочинці дедалі частіше відходять від хакерських атак, спрямованих на пристрої, на користь тактик, орієнтованих на людей, які передбачають викрадення особистих даних шляхом маніпуляцій, зокрема шахрайських дзвінків, фішингових SMS та електронних листів від імені відомих компаній, а також підроблених сторінок входу, призначених для викрадення паролів. Хоча 91% респондентів заявили, що їх турбують шахрайські дії у сфері кібербезпеки, багато хто недооцінює те, що шахрайські дзвінки та фішинг часто є першим кроком до більш серйозних збитків, яких вони найбільше побоюються: 56% більше турбуються про крадіжку особистих даних або шахрайство, ніж про шахрайські дзвінки, проте 46% заявляють, що отримують шахрайські дзвінки щодня, а 17% повідомляють, що особисто стикалися з крадіжкою особистих даних або шахрайством... Технічний директор NordVPN Маріюс Брієдіс попередив, що злочинці досягають успіху, коли жертви, відчуваючи поспіх або тиск, надто швидко довіряють їм, і всього за кілька кліків телефонний дзвінок або повідомлення перетворюються на крадіжку особистих даних. NordVPN радить не поспішати, коли повідомлення здаються терміновими, перевіряти інформацію та посилання перед тим, як відповідати, використовувати багатофакторну автентифікацію та надійні паролі, завантажувати файли лише з перевірених джерел, застосовувати фільтрацію телефонних дзвінків та, по можливості, ігнорувати невідомі номери, а також використовувати програмне забезпечення для безпеки, здатне протидіяти різноманітним загрозам». (*Giselle Castro-Sloboda. NordVPN Survey: Americans Worry Most About the Wrong Part of*

Cybercrime // Ziff Davis company (<https://www.cnet.com/tech/nordvpn-survey-cybercrime/>). 15.05.2026).
