**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

№ 2 (лютий)

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. № 2 (лютий). 148 с.

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

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

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

ЗМІСТ

Світові тенденції в галузі кібербезпеки 4
Сполучені Штати Америки та Канада 34
Країни ЄС та Великобританія 43
Австралія та Нова Зеландія 56
Китай, Індія, Японія, Південна Корея та країни Індо-тихоокеанського регіону 57
Ізраїль, Туреччина та країни Близького сходу 63
Країни Африки 65
Кіберстрахування 68
Кібервійни та протидія зовнішній кібернетичній агресії 68
Кіберзахист критичної інфраструктури 77
Кіберзахист виробничих об’єктів 80
Кіберзахист закладів охорони здоров’я 83
Захист персональних даних та соціальні мережі 84
Правове забезпечення захисту персональних даних 85
Масштабні витоки персональних даних 86
Кібербезпека Інтернету речей. Штучний інтелект 91
Штучний інтелект, як інструмент боротьби із кіберзлочинністю 98
Штучний інтелект, як зброя кіберзлочинців 102
Кіберзлочинність та кібертероризм 104
Діяльність хакерів та хакерські угруповування 124
Вірусне та інше шкідливе програмне забезпечення 125
Фішингові атаки 137
Операції правоохоронних органів та судові справи проти кіберзлочинців 139
Технічні аспекти кібербезпеки 141
Виявлені вразливості технічних засобів та програмного забезпечення 141
Технічні та програмні рішення для протидії кібернетичним загрозам 147
Основи кібергігієни 147

«Світ вступає в нову еру геополітичної конкуренції, в якій посилюється суперництво між великими державами, а швидкі технологічні зміни переформатують спосіб функціонування країн, компаній та суспільств. У цих умовах кібербезпека перетворилася з технічної проблеми на стратегічне питання, яке має ключове значення для міжнародних відносин, стійкості бізнесу та довіри громадськості. Згідно з прогнозом Global Cybersecurity Outlook 2026, 91% найбільших організацій змінили свої стратегії кібербезпеки у відповідь на геополітичну нестабільність…

Цю зміну зумовлюють три ключові чинники: поглиблення зв'язку між кібербезпекою та геополітикою, зростання кількості нормативних актів, спрямованих на захист суверенітету, та нагальна потреба у стійкості. Кібероперації зараз є основними інструментами державного управління, які використовуються для шпигунства, саботажу та впливу, що робить кожну організацію, а особливо кожного керівника служби інформаційної безпеки, геополітичним актором. Поява багатополярного світу та вплив середніх держав, хактивістів та організованої злочинності створили більш непередбачуваний ландшафт загроз, де важко визначити відповідальних, а гібридні атаки стирають межі між державною та недержавною діяльністю…

Уряди посилюють контроль над кіберпростором шляхом більш суворого регулювання локалізації даних, посилення нагляду та зусиль з формування управління технологіями. Це створює складні проблеми з дотриманням вимог для транснаціональних компаній, оскільки нормативні акти, що базуються на суверенітеті, розходяться в різних юрисдикціях, що додає операційних труднощів і стратегічних ризиків. Експортний контроль над передовими технологіями фрагментує глобальний інноваційний ландшафт, підвищуючи ймовірність розділення цифрового світу з розбіжними технологічними стандартами.

Організації адаптуються, створюючи федеративні моделі безпеки, регіоналізуючи технологічні стеки та диверсифікуючи ланцюги поставок, але ці заходи супроводжуються вищими витратами і, інколи, зниженням стійкості. Ризик концентрації та залежність від ланцюгів поставок зараз є головними проблемами, оскільки геополітичні потрясіння можуть спричинити ланцюгові порушення. Гібридна війна, що поєднує кібератаки з фізичними та інформаційними операціями, ще більше ускладнює ризикову ситуацію.

Для підвищення стійкості організації впроваджують стратегії диверсифікації, моделі безпеки з нульовим рівнем довіри, проактивне планування на випадок кризових ситуацій та тіснішу співпрацю з національними органами безпеки. Лідери у сфері кібербезпеки визнають, що реактивні підходи вже не є достатніми; компанії повинні передбачати фрагментацію, інвестувати в стійкість та розуміти, що їхні рішення мають геополітичні наслідки. У сучасному взаємопов'язаному світі те, що відбувається в кіберпросторі, формує економіку, демократію та глобальний баланс сил, тому співпраця між бізнесом та урядами є необхідною для безпечного та стійкого цифрового майбутнього». ***(Ellie Winslow, Joanna Bouckaert. How cybersecurity can best navigate geopolitics to secure a resilient and open digital future***

// World Economic Forum (https://www.weforum.org/stories/2026/02/cybersecurity-and-geopolitics-the-challenges-to-build-resilience-in-a-fragmented-world/). 05.02.2026).

***

«Компанії з кібербезпеки Fortinet, NetScout і Qualys у своїх останніх квартальних звітах повідомили про кращі, ніж очікувалося, прибутки та доходи, що свідчить про стабільно високий попит на послуги з кібербезпеки на тлі розвитку штучного інтелекту…

Fortinet повідомила про 15% річне зростання доходу до 1,91 млрд доларів за четвертий квартал 2025 фінансового року, при цьому скоригований прибуток на акцію зріс до 81 цента. Дохід від реалізації продукції зріс на 20% до 691 млн доларів, а виставлені рахунки зросли на 18% до 2,37 млрд доларів. За весь рік дохід досяг 6,8 млрд доларів, що на 14% більше, а скоригований прибуток на акцію склав 2,76 долара. Fortinet очікує, що дохід у 2026 році складе від 7,5 до 7,7 млрд доларів. Після оприлюднення звіту акції компанії подорожчали приблизно на 2,5%...

NetScout опублікувала скоригований прибуток у розмірі 1 долар на акцію за третій квартал 2026 фінансового року, що перевищило очікування, хоча виручка дещо знизилася в порівнянні з аналогічним періодом минулого року і склала 250,7 млн доларів. Дохід від продажу продукції знизився, але дохід від надання послуг зріс. NetScout тепер прогнозує річний прибуток у розмірі від 1,15 до 1,23 долара на акцію та дохід від 835 до 870 мільйонів доларів. Незважаючи на перевищення прогнозів щодо прибутку, акції NetScout впали майже на 5%...

Qualys повідомила про скоригований прибуток у четвертому кварталі в розмірі 1,87 долара на акцію, що на 1,60 долара більше, ніж роком раніше, при доході в 175,3 мільйона доларів, що на 10% більше. За весь рік скоригований прибуток склав 7,07 долара на акцію при доході в 669,1 мільйона доларів, що на 10% більше. Qualys очікує, що у 2026 році дохід складе від 717 до 725 млн доларів, а скоригований прибуток — від 7,17 до 7,45 долара на акцію. Хоча прогноз прибутку був дещо нижчим за очікування аналітиків, прогноз доходу був вищим, і акції Qualys впали приблизно на 3% у післяторговельних торгах…

Загалом, результати підкреслюють стійкість сектору та зростаючу важливість кібербезпеки, оскільки організації інвестують у захист своїх цифрових активів». ***(Duncan Riley. Cybersecurity earnings season kicks off with beats from Fortinet, NetScout and Qualys // SiliconANGLE Media Inc. (https://siliconangle.com/2026/02/05/cybersecurity-earnings-season-kicks-off-beats-fortinet-netscout-qualys/). 05.02.2026).***

***

«Загрози кібербезпеці стають дедалі більш витонченими, що вимагає від організацій постійного посилення контролю та управління для захисту систем і даних. Однак постійний фінансовий тиск часто змушує керівників утримуватися від витрат або скорочувати їх, зберігаючи при цьому рівень захисту, що створює значні проблеми в умовах фіксованих витрат за контрактами та конкуренції за таланти…

Хороша новина полягає в тому, що організації можуть максимізувати вартість існуючих інвестицій у кібербезпеку без додаткових витрат. До типових обмежень належать перевищення бюджету, що призводить до часткової функціональності, плинність кадрів, що спричиняє дефіцит кваліфікованих фахівців, контроль, що залишається в режимі моніторингу через побоювання перебоїв у роботі, та перевантажені команди з обмеженими можливостями. Незважаючи на значні витрати на забезпечення відповідності вимогам, порушення продовжують траплятися, що підкреслює необхідність продемонструвати рентабельність інвестицій у поточні інструменти…

П'ять практичних кроків для максимізації вашої кіберстратегії:

Посильте контроль доступу та ідентифікації: Перегляньте такі інструменти, як Microsoft Active Directory, на наявність неактивних облікових записів, невикористаних привілеїв та старих тестових облікових записів — це швидкі перемоги, які зменшують ризик без додаткових витрат.

Посильте налаштування безпеки: Використовуйте безкоштовні ресурси, такі як рекомендації Австралійського центру кібербезпеки (ACSC) або критерії Центру інтернет-безпеки (CIS) для поетапного посилення захисту.

Відкрийте нові функції: постачальники часто додають нові можливості до існуючих продуктів; швидкий перегляд налаштувань або безкоштовна перевірка стану можуть виявити невикористаний потенціал рентабельності інвестицій.

Активуйте неактивні продукти: багато хто недостатньо використовує ліцензійні інструменти (наприклад, Microsoft 365 E5); увімкнення всіх функцій посилює захист і підтримує управління штучним інтелектом.

Використовуйте сервісні кредити: контракти часто включають кредити на перевірку стану або оптимізацію — попросіть постачальників максимально використати ці переваги…

Ці кроки оптимізують існуючі інструменти, усувають прогалини в захисті та узгоджують безпеку з пріоритетами бізнесу, зміцнюючи впевненість керівництва та стійкість навіть у складних економічних умовах». ***(Nick Kervin and Ashley Parkinson. Practical ways to maximise cyber security in lean times // BDO (https://www.bdo.com.au/en-au/insights/cyber-security/practical-ways-to-maximise-cyber-security-in-lean-times). 11.02.2026).***

***

«У міру посилення кіберзагроз організації часто інстинктивно розширюють свої засоби захисту, додаючи нові інструменти, що може ненавмисно призвести до «розростання інструментів» — накопичення непов'язаних або надлишкових продуктів, які створюють більше плутанини, ніж контролю. Ця фрагментація призводить до надмірного обсягу сповіщень, недовикористання платформ та ізольованих систем, що залишають критичні прогалини в захисті, змушуючи перевантажені команди керувати інформаційними панелями, а не усувати реальні загрози… Наслідки особливо гостро відчуваються в таких секторах, як нерухомість та фінансові послуги, де швидке зростання портфеля або складні регуляторні вимоги призводять до нескоординованого накладання інструментів, що спричиняє непослідовний захист, уповільнення

аудитів та марнування бюджетів. Розростання зазвичай виникає не через погане планування, а через термінові закупівлі без міжфункціональної узгодженості, що призводить до втрати організаціями прозорості та гнучкості.

Щоб вирішити цю проблему, експерти рекомендують чотириетапну стратегію раціоналізації систем безпеки та узгодження технологій із бізнес-цілями. Процес починається з комплексного аналізу архітектури безпеки та засобів контролю для виявлення надмірності та забезпечення відповідності стандартам, таким як NIST або HIPAA. Далі проводиться оцінка видимості мережі та хмари для усунення «сліпих зон» у гібридних середовищах, що забезпечує єдине виявлення загроз… Організації також повинні використовувати сторонні рішення з управління ризиками, щоб централізувати нагляд за постачальниками та зменшити необхідність дублювання контролю. Нарешті, економія коштів і часу, досягнута завдяки оптимізації, повинна бути реінвестована в довгострокові заходи з підвищення стійкості, такі як оновлення політик, проведення навчання з питань фішингу та вдосконалення планів реагування на інциденти, перетворюючи кібербезпеку на стратегічний фактор зростання». ***(Adam Wisnieski, Sridhar Alla. Is Your Cybersecurity Tool Stack Hurting Your Security? // MACIAS GINI & O'CONNELL LLP (https://www.mgocpa.com/perspective/cybersecurity-tool-sprawl/). 13.02.2026).***

***

«…Згідно з доповіддю ISACA «Стан кібербезпеки у 2025 році», 55% фахівців з кібербезпеки стикаються з проблемою нестачі персоналу та підвищенням рівня стресу, що є критичною вразливістю в умовах ескалації кібератак. Обмежені ресурси часто призводять до зниження пріоритетності сповіщень, затримок з виправленням вразливостей та ігнорування ризиків, пов'язаних із третіми сторонами, що створює накопичення некерованих вразливостей. Це особливо небезпечно для таких галузей, як біотехнології, де невеликі команди повинні захищати конфіденційну інтелектуальну власність та дотримуватися суворих стандартів відповідності… Щоб посилити захист без збільшення чисельності персоналу, організації повинні визначити пріоритетні області високого ризику за допомогою чіткого плану дій з кібербезпеки, узгодженого з такими рамками, як NIST CSF, посилити внутрішні команди цільовою зовнішньою підтримкою для виконання таких завдань, як управління вразливостями та реагування на інциденти, а також раціоналізувати набір засобів безпеки для зменшення складності та поліпшення видимості». ***(Adam Wisnieski, Sridhar Alla. How to Reduce Cyber Risk When Your Team Is Understaffed // MACIAS GINI & O'CONNELL LLP (https://www.mgocpa.com/perspective/reduce-cyber-risk-understaffed/). 18.02.2026).***

***

«У звіті «Глобальний прогноз у сфері кібербезпеки до 2026 року» Всесвітнього економічного форуму міститься попередження про те, що прискорення впровадження штучного інтелекту, геополітична фрагментація та поглиблення кібернерівності змінюють глобальний ландшафт ризиків. На

основі думок 800 лідерів у звіті зазначається, що хоча все більше організацій оцінюють безпеку штучного інтелекту перед його впровадженням, 87 % вважають вразливість, пов’язану зі штучним інтелектом, найшвидше зростаючою загрозою. Геополітика зараз визначає стратегію кібербезпеки для 91% великих організацій, хоча регіональна впевненість у захисті критичної інфраструктури різко варіюється: від 84% на Близькому Сході та в Північній Африці до лише 13% в Латинській Америці. Крім того, кібершахрайство залишається поширеним явищем, яке зачіпає 73% респондентів і підкреслює розбіжність у пріоритетах: генеральні директори зосереджуються на шахрайстві, а керівники служб інформаційної безпеки — на програмному забезпеченні для вимагання викупу…

З огляду на конкретну загрозу від програм-вимагачів, Федеральна комісія з питань зв'язку США (FCC) закликала телекомунікаційні компанії посилити захист після чотирикратного збільшення кількості атак з 2021 року. З огляду на вразливість малих і середніх провайдерів, FCC рекомендує впровадити архітектуру нульової довіри, сегментацію мережі та суворі плани реагування на інциденти, що включають повідомлення федеральних агентств. У корпоративних новинах Європейська комісія беззастережно схвалила придбання Google за 32 мільярди доларів компанії Wiz, що спеціалізується на кібербезпеці, а Індія запропонувала нові суворі стандарти безпеки, які можуть зобов'язати виробників смартфонів ділитися вихідним кодом з урядом. Нещодавні порушення також торкнулися голландської телекомунікаційної компанії Odido, яка оприлюднила дані з понад шести мільйонів облікових записів, та південнокорейського гіганта електронної комерції Coupang, де колишній інженер скористався недоліками в системі автентифікації. Нарешті, тривають заходи з забезпечення безпеки зимових Олімпійських ігор у Мілані-Кортіні, оскільки влада поспішає захистити об'єкти від нових кіберзагроз». ***(Akshay Joshi. The cyber threats to watch in 2026 – and other cybersecurity news // World Economic Forum (https://www.weforum.org/stories/2026/02/2026-cyberthreats-to-watch-and-other-cybersecurity-news/). 18.02.2026).***

***

«В останньому прогнозі Всесвітнього економічного форуму (WEF) щодо кібербезпеки наголошується на критичному «парадоксі кібербезпеки»: хоча цифрова взаємопов'язаність сприяє економічному зростанню, вона також створює безпрецедентний системний ризик через інфраструктуру, розроблену для більш довірливої епохи. Ця напруга посилюється фрагментацією геополітичного співробітництва та прискоренням як кібератак, так і кіберзахисту за допомогою штучного інтелекту, що перетворює кібербезпеку з IT-проблеми на основну відповідальність керівництва...

Ніде ця напруга не є такою очевидною, як у сучасному центрі безпеки (SOC), який бореться з обсягами сповіщень, що значно перевищують людські можливості. Традиційні SOC, розроблені для іншої епохи, не справляються зі складністю та швидкістю сучасних загроз, що призводить до виснаження аналітиків, непослідовних реакцій та небезпечних затримок у реагуванні, особливо вночі та у

вихідні дні — у найсприятливіший час, який зловмисники навчилися використовувати…

Для досягнення сучасної кіберстійкості необхідна фундаментальна переорієнтація, перехід від статичного виявлення на основі сигнатур до аналізу на основі поведінки та від ручного сортування до інтелектуальної автоматизації. Саме тут аналітик AI SOC стає важливим мультиплікатором сили, а не заміною людських експертів. Автономно сортуючи сповіщення, проводячи попередні розслідування та фільтруючи помилкові спрацьовування 24/7, аналітики AI SOC беруть на себе повторювану роботу з великим обсягом, яка перевантажує традиційні команди. Це дозволяє аналітикам-людям зосередитися на більш цінних видах діяльності, таких як пошук загроз та стратегічне зниження ризиків, скорочуючи час реагування з годин до хвилин та усуваючи прогалини в безпеці, що існують постійно…

Зрештою, вирішення парадоксу кібербезпеки є обов'язковим завданням для керівництва. Лідери повинні виходити з того, що ШІ буде визначати як атаки, так і захист, розробляти операції з урахуванням стійкості, а не досконалості, і перетворювати принципи цифрової довіри на вимірювані результати. Застосовуючи практичний ШІ, впроваджуючи ефективне управління та переосмислюючи операції з безпеки для світу, який характеризується швидкістю та невизначеністю, організації можуть перетворити цифрову довіру на довгострокову конкурентну перевагу». ***(Bill Tanner. The cybersecurity paradox: Digital growth outpaces legacy security // Intelligent CISO (https://www.intelligentciso.com/2026/02/25/the-cybersecurity-paradox-digital-growth-outpaces-legacy-security/). 25.02.2026).***

***

«У швидко розвиваючомуся середовищі кібербезпеки 2026 року характер загроз змінився: тепер вони спрямовані не на банки та технологічні компанії, а на критичну інфраструктуру, таку як лікарні, електромережі та виробничі підприємства, де простої можуть мати катастрофічні наслідки. Хакери все частіше використовують інструменти штучного інтелекту для складних атак, включаючи соціальну інженерію та дипфейки, випереджаючи можливості правових механізмів. Як результат, малі підприємства повинні впроваджувати комплексні політики кіберстрахування, які виходять за межі простої фінансової компенсації та включають проактивні заходи, такі як активна оцінка загроз, захист від шахрайства з використанням штучного інтелекту та надійний «регуляторний щит» для дотримання таких законів, як DPDP Act та GDPR… Ідеальна політика на 2026 рік передбачає модель «превентивного підходу» з моніторингом у режимі реального часу та командами швидкого реагування на інциденти, які можуть прибути на місце події протягом години, щоб пом'якшити наслідки кризи та захистити репутацію компанії. Зрештою, в епоху підвищених ризиків, пов'язаних із штучним інтелектом, та суворих нормативних вимог, розумне кіберстрахування вже не є розкішшю, а абсолютною необхідністю для забезпечення стійкості та виживання бізнесу». ***(Srinivasa Raghavendra Rao. Cyber Insurance Benchmarks for Small Businesses in 2026 // The Review Hive (https://thereviewhive.blog/cyber-insurance-for-small-businesses-in-2026/). 19.02.2026).***

***

«За словами Ніколь Квінн, віце-президента з питань політики та державних справ компанії Palo Alto Networks, кібербезпека стала національним пріоритетом, що впливає на економічну стабільність, довіру громадськості та цифрову безпеку, а не лише проблемою ІТ-галузі. Вона підкреслила, що штучний інтелект є «двосічним мечем»: кіберзлочинці використовують його для масштабування фішингу, шахрайства та шкідливого програмного забезпечення зі швидкістю машини, змушуючи захисників покладатися на системи на базі ШІ, які аналізують величезні потоки даних і запускають втручання людини лише в разі необхідності…

У той час як уряди все більше зосереджуються на регулюванні штучного інтелекту та цифрової безпеки, Квін зазначила, що законодавство часто відстає від технологій і повинно забезпечувати баланс між захистом та інноваціями за допомогою штучного інтелекту, безпечного за своєю конструкцією, та контрольованих систем поведінки. Вона підкреслила, що дискусії про кібербезпеку тепер доходять до залів засідань правління через ризики для бізнесу, але попередила, що людська помилка залишається основною вразливістю…» ***(Tanya Pandey. Cybersecurity a national priority as AI pushes threat landscape, digital adoption, says Palo Alto's Nicole Quinn // Bennett, Coleman & Co. Ltd. (https://economictimes.indiatimes.com/tech/artificial-intelligence/cybersecurity-a-national-priority-as-ai-pushes-threat-landscape-digital-adoption-says-palo-altos-nicole-quinn/articleshow/128680965.cms). 23.02.2026).***

***

«Ланцюги поставок стали однією з найбільш експлуатованих точок входу в сучасній кібервійні, що загрожує національній безпеці, критичній інфраструктурі та глобальній торгівлі. Гучні інциденти, такі як SolarWinds і атака на Colonial Pipeline, демонструють, як компрометація одного постачальника може поширитися на цілі галузі… Зловмисники, включаючи держави, злочинні угруповання та хактивістів, використовують слабку безпеку сторонніх розробників, доступ інсайдерів, неперевірений код та підроблене обладнання, тоді як нові технології, такі як штучний інтелект, 5G, Інтернет речей та квантові обчислення, одночасно підвищують ефективність та розширюють площу атаки. Майже 90% ІТ-фахівців вважають ланцюги постачання програмного забезпечення високоризиковими, проте більшість з них вважають, що нинішні засоби захисту є недостатніми…

Уряди та промисловість відреагували такими заходами, як указ президента США від 2019 року про ланцюги постачання ІКТ, ініціативи CISA та DoD, рамки NIST та все більш широке впровадження специфікацій програмного забезпечення (SBOM). Однак багаторівневі прогалини у видимості, застарілі системи та фрагментовані нормативні акти продовжують гальмувати прогрес. Щоб протистояти новим загрозам, організації повинні прийняти комплексні рамки ризиків, впровадити архітектури нульової довіри, використовувати виявлення на основі штучного інтелекту, вимагати прозорості від постачальників, диверсифікувати джерела постачання, готуватися до квантового шифрування та

надавати пріоритет стійкості над ідеальним запобіганням… Зрештою, кібербезпека ланцюгів постачання повинна стати питанням, яке турбує керівництво, оскільки конкурентна перевага та економічна стабільність все більше залежать від здатності швидко відновлювати та підтримувати довіру у взаємопов'язаному, технологічному світі». ***(Chuck Brooks. The Cybersecurity Challenges of the Supply Chain: Navigating Risks in a Hyper-Connected, Emerging-Tech World // Executive Mosaic Inc (https://www.govconwire.com/articles/chuck-brooks-govcon-expert-cyber-supply-chain-risks). 24.02.2026).***

***

«Глобальний збій кінцевих точок Windows у 2024 році, спричинений патчем CrowdStrike, висвітлив критичну прогалину в підготовленості організацій: здатність координувати дії в рамках взаємопов'язаної екосистеми. Хоча багато компаній зазнали труднощів, ті, що входять до Ради з питань стійкості бізнесу (BRC), відновилися швидше, використовуючи заздалегідь налагоджені відносини, безпечні канали та відпрацьовані сценарії дій — концепцію, яка отримала назву «колективна стійкість». Цей підхід виходить за межі традиційної операційної стійкості, яка зосереджується на підтримці роботи послуг однієї компанії, і забезпечує безперебійну роботу критично важливих послуг спільних постачальників і партнерів навіть у разі порушення їхньої роботи…

Настільні навчання, що імітують збій у роботі платіжної системи ACH, підкреслили необхідність таких змін, показавши, що спільні припущення постачальників часто виявляються помилковими в кризових ситуаціях, а треті сторони можуть бути не в змозі надати допомогу... Для досягнення колективної стійкості керівники повинні перейти від простого захисту до активної координації, налагодити безпечні канали зв'язку з ключовими постачальниками, визначити та контролювати мінімальні рівні життєздатних послуг (MVSL) для критично важливих послуг, а також ретельно відпрацьовувати дії в умовах порушення нормального функціонування за допомогою багатосторонніх навчань... Застосовуючи ці практики, організації можуть мінімізувати системний вплив, запобігти шкоді споживачам та забезпечити безперервність роботи в умовах дедалі більш взаємозалежного цифрового середовища». ***(Mark Orsi and Keri Pearlson. Cybersecurity Requires Collective Resilience // Harvard Business School Publishing (https://hbr.org/2026/02/cybersecurity-requires-collective-resilience). 18.02.2026).***

***

«У 2025 році активність венчурного капіталу в галузі кібербезпеки різко зросла, що було зумовлено переважною орієнтацією на рішення з безпеки на базі штучного інтелекту та рекордними злиттями і поглинаннями. За даними Momentum Cyber, інвестиції в галузь склали 119 млрд доларів, включаючи 400 угод злиття та поглинання на суму понад 96 млрд доларів і 820 раундів фінансування на загальну суму майже 21 млрд доларів, що майже втричі перевищує обсяг угод попереднього року. Лідерами за обсягом фінансування стали стартапи в галузі безпеки на базі штучного інтелекту з 144 угодами, за ними слідували компанії, що займаються ризиками та дотриманням нормативних вимог… Серед основних

придбань можна відзначити купівлю Google компанії Wiz за 32 мільярди доларів та придбання Palo Alto Networks компанії CyberArk за 25 мільярдів доларів, що відображає прагнення стратегічних покупців посилити портфелі продуктів та залучити найкращих фахівців. Венчурні капіталісти наголошують, що штучний інтелект змінює як поверхні атаки, так і операції з безпеки, створюючи можливості «AI-squared», оскільки компанії інвестують у захист систем штучного інтелекту та захист підприємств, що працюють на основі штучного інтелекту… Оскільки в січні 2026 року вже зафіксовано значний потік угод, інвестори вважають, що ця динаміка збережеться, розглядаючи кібербезпеку на основі штучного інтелекту як можливість покоління в умовах швидкозмінних загроз і попиту підприємств на стійкі, орієнтовані на результат рішення». ***(Robert Lemos. As Cybersecurity Firms Chase AI, VC Market Skyrockets // TechTarget, Inc. (https://www.darkreading.com/cybersecurity-analytics/cybersecurity-firms-chase-ai-vc-market-skyrockets). 24.02.2026).***

***

«…Нелюдські ідентичності (NHI) — облікові дані машин, ключі API, токени та дозволи, що дозволяють серверам, контейнерам, додаткам та агентам штучного інтелекту спілкуватися між собою — стали критично важливим, але часто недооціненим елементом сучасної кібербезпеки. У міру розширення організацій у хмарних, DevOps та AI-середовищах, ідентичності машин значно переважають за кількістю людських користувачів, що робить управління секретами та ідентичностями ключовим фактором зниження ризиків…

На відміну від традиційних облікових записів користувачів, NHI складаються як з секретного елемента (наприклад, ключа або токена), так і з пов'язаних з ним прав доступу. Неефективне управління життєвим циклом — застарілі облікові дані, надмірні дозволи, фрагментовані системи — створює серйозні ризики порушення безпеки. Ефективне управління NHI вимагає постійного виявлення, класифікації, моніторингу, ротації та виведення з експлуатації облікових даних машин. При правильному виконанні це зменшує ризики, покращує дотримання нормативних вимог, підвищує операційну ефективність, посилює прозорість та знижує витрати завдяки автоматизації.

Міграція до хмари та впровадження штучного інтелекту роблять це ще більш нагальним. Агенти штучного інтелекту та автоматизовані системи залежать від ідентичності машин для функціонування; у разі порушення їхньої цілісності вони можуть стати векторами швидких атак. Централізовані платформи управління NHI забезпечують контекстну видимість у різних середовищах, виявляють ненормальну поведінку та забезпечують дотримання єдиних політик. Вбудовування цих засобів контролю в конвеєри DevOps та робочі процеси SOC гарантує, що безпека вбудована в розробку та контролюється під час виконання…

Виклики залишаються — фрагментовані інфраструктури, швидко розвиваються екосистеми машин і міжкомандні силоси — але впровадження уніфікованих систем управління NHI заповнює прогалини між командами безпеки та НДДКР. У міру того, як кіберзагрози стають все більш автоматизованими та витонченими, організації, які проактивно захищають ідентичності та секрети

машин, будуть мати набагато кращі можливості для захисту даних, збереження довіри та захисту цифрових інфраструктур нового покоління». ***(Alison Mack. Why are cybersecurity experts optimistic about NHIDR // Techstrong Group Inc. (https://securityboulevard.com/2026/02/why-are-cybersecurity-experts-optimistic-about-nhidr/). 22.02.2026).***

***

«У міру того як кібератаки стають все більш витонченими, а централізовані системи залишаються вразливими до єдиних точок відмови, блокчейн стає додатковим інструментом для посилення кібербезпеки. Традиційне зберігання даних базується на централізованих серверах, які в разі порушення можуть оприлюднити величезні обсяги конфіденційної інформації. Блокчейн усуває цей ризик, забезпечуючи захищене від втручання децентралізоване ведення обліку, що дозволяє здійснювати прозорий аудит і зменшує ймовірність масштабного витоку даних. Він також підтримує децентралізовані системи ідентифікації (DID), що дозволяють користувачам пройти аутентифікацію без розкриття особистої інформації, і може підвищити безпеку пристроїв Інтернету речей та периферійних пристроїв шляхом перевірки цілісності пристроїв та передачі даних…

Хоча блокчейн не замінює традиційні протоколи безпеки, він може їх підсилити, особливо в поєднанні з новими технологіями, такими як штучний інтелект і докази з нульовим розкриттям інформації. У міру того як установи тестують блокчейн для забезпечення безпеки комунікацій, ланцюгів поставок і критичної інфраструктури, все більшого значення набувають питання продуктивності та масштабованості, такі як ті, що спостерігаються в мережах на зразок Solana. Зрештою, блокчейн еволюціонує від основи криптовалюти до фундаментального рівня сучасної стійкості кібербезпеки…» ***(William Jones. How Blockchain is Strengthening Cybersecurity in the Modern Age // Gannett Co., Inc. (https://www.usatoday.com/story/special/contributor-content/2026/02/20/how-blockchain-is-strengthening-cybersecurity-in-the-modern-age/88778791007/). 20.02.2026).***

***

«…Компанія Samsung SDS визначила п'ять основних загроз кібербезпеці, які, як очікується, будуть визначати пріоритети корпоративної безпеки в 2026 році: кібератаки на основі штучного інтелекту, програми-вимагачі, вразливості хмарних технологій, фішинг та порушення безпеки даних. На основі опитування 667 фахівців з IT та безпеки та аналізу останніх інцидентів компанія попереджає, що швидке впровадження генеративного штучного інтелекту та автономних агентів штучного інтелекту може призвести до надмірних привілеїв, несанкціонованих дій та витоку даних. Вона рекомендує впровадити захисні заходи для штучного інтелекту, включаючи моніторинг у реальному часі та затвердження людиною операцій з високим рівнем ризику…

У звіті також підкреслюється еволюція програм-вимагачів у «чотирикратне вимагання», що поєднує шифрування, витік даних, DDoS-атаки та шантаж, і

наголошується на необхідності впровадження багаторівневих систем відновлення та навчання співробітників. Ризики, пов'язані з хмарними технологіями, залишаються значними через неправильні налаштування та слабкий контроль доступу, що вимагає постійного моніторингу за допомогою хмарних засобів захисту. Фішинг продовжує слугувати основною точкою входу для більш масштабних вторгнень, тоді як запобігання витоку даних має поширюватися на сторонніх постачальників та ланцюги постачання, щоб забезпечити узгодженість безпеки в масштабах всієї екосистеми». ***(Lee Gyu-lee. Samsung SDS flags top 5 cybersecurity threats for 2026 // The Korea Times (https://www.koreatimes.co.kr/business/tech-science/20260223/samsung-sds-flags-top-5-cybersecurity-threats-for-2026). 23.02.2026).***

***

«…Керівник служби інформаційної безпеки розповідає, як завдання щодо скорочення витрат — зменшення поточних витрат на 10 %, компенсація інфляції та самофінансування нових ініціатив — змусило перейти від зростання за рахунок додавання до дисциплінованого розподілу капіталу. Замість того, щоб накопичувати інструменти та збільшувати штат, команда розглядала план дій з безпеки як портфель інвестицій, зіставляючи заходи контролю за вартістю та впливом на зменшення ризиків і перенаправляючи ресурси з малоефективних ініціатив на високоприбуткові…

Практичні кроки включали перегляд і модернізацію контрактів з постачальниками з урахуванням результатів, автоматизацію рутинних робочих процесів (сортування, звітність, виправлення) для звільнення аналітиків для виконання більш цінної роботи, скорочення неосновних адміністративних витрат, реструктуризацію команд і аутсорсинг у сфері ризиків, а не інструментів, а також консолідацію дублюючих платформ безпеки. Висновок: надлишок приховує марнотратство, але обмеження виявляють його. Ефективне лідерство в галузі кібербезпеки зараз залежить від вимірюваного зниження ризиків на кожен долар, прозорих компромісів та операційної дисципліни, а не від більших бюджетів…» ***(Marco Túlio Moraes. Discipline is the new power move in cybersecurity leadership // FoundryCo, Inc. (https://www.csoonline.com/article/4133280/discipline-is-the-new-power-move-in-cybersecurity-leadership.html). 18.02.2026).***

***

«Звіт VicOne про кібербезпеку в автомобільній галузі за 2026 рік показує, що кіберзагрози в автомобільній галузі вступили в так звану «еру перетину», коли автомобілі, хмарні платформи та корпоративні IT-системи функціонують як єдина взаємопов'язана система. У 2025 році кількість міжрегіональних та міжгалузевих кіберінцидентів зросла більш ніж утричі — до 161 із 610 зареєстрованих випадків. Причиною цього стали централізовані програмні платформи та системи оновлення через бездротовий зв'язок (OTA), які дозволяють одній уразливості поширюватися по всіх дочірніх компаніях та регіонах. Третина виявлених ризиків зараз безпосередньо впливає на системи, пов'язані з водіями, що підвищує їхню видимість та вплив на репутацію…

У звіті робиться висновок, що кіберризики в автомобільній галузі більше не є локальною технічною проблемою, а є викликом для управління, що охоплює IT, бек-енд, системи транспортних засобів та зовнішню інфраструктуру, таку як мережі зарядних станцій для електромобілів. Функції на основі штучного інтелекту та системи безперервного навчання прискорюють поширення ризиків, а дотримання таких нормативних актів, як UN R155 та ISO/SAE 21434, хоч і є корисним, але само по собі є недостатнім. VicOne стверджує, що кібербезпека повинна управлятися як відповідальність на рівні правління протягом усього життєвого циклу, а не за допомогою ізольованих, орієнтованих на виправлення контролюючих заходів, щоб вирішити проблему зростаючої складності програмно-визначених транспортних засобів та підключених екосистем…» ***(VicOne 2026 Automotive Cybersecurity Report Finds Cyber Incidents No Longer Stay Inside One Organization // indystar (https://www.indystar.com/press-release/story/33291/vicone-2026-automotive-cybersecurity-report-finds-cyber-incidents-no-longer-stay-inside-one-organization/). 11.02.2026).***

***

«Звіт Sophos «Активні супротивники 2026 року» показує, що слабкі місця в ідентифікації зараз є основною причиною кіберінцидентів, причому дві третини випадків пов'язані з компрометацією облікових даних, атаками методом грубої сили, фішингом і відсутністю багатофакторної автентифікації (MFA). У 59% розслідувань MFA була відсутня, що дозволило зловмисникам увійти в систему за допомогою викрадених облікових записів, а не використовувати недоліки програмного забезпечення. Хоча використання вразливостей (16%) і спроби брут-форсу (15,6%) залишаються поширеними, загальна тенденція показує, що зловмисники все частіше обходять периметральну захист, зловживаючи дійсними ідентифікаційними даними. Потрапивши всередину, зловмисники діють швидко — в середньому за 3,4 години досягають критично важливих систем, таких як Active Directory, — а середній час перебування в системі скоротився до трьох днів завдяки як швидшій діяльності зловмисників, так і покращеному виявленню в середовищах, що моніторяться MDR…

Програми-вимагачі залишаються серйозною загрозою: 88% корисних навантажень розгортаються поза робочим часом, а 79% витоків даних також відбуваються після закінчення робочого дня, що свідчить про те, що зловмисники навмисно атакують, коли команди безпеки не мають достатньої кількості персоналу. Екосистема програм-вимагачів фрагментувалася: у 2025 році було зафіксовано 51 активний бренд, що відображає вплив заходів правоохоронних органів, але збільшує непередбачуваність для захисників. Всупереч очікуванням, Sophos виявив, що генеративна штучна інтелігенція розширила масштаби фішингу та соціальної інженерії, але ще не змінила тактику зловмисників. У звіті також підкреслюється зростаюча проблема втрати телеметрії, особливо з брандмауерів з коротким терміном зберігання журналів, що ускладнює розслідування. Sophos рекомендує посилити безпеку ідентифікації за допомогою стійкої до фішингу багатофакторної автентифікації (MFA), зменшити вразливість сервісів, що мають вихід в Інтернет, забезпечити постійний моніторинг, зберігати журнали та

оперативно виправляти вразливості, щоб протидіяти новим загрозам…» ***(Identity Weaknesses Drive Two Thirds Of Cyber Incidents: Sophos // BW BUSINESSWORLD (https://www.businessworld.in/article/identity-weaknesses-drive-two-thirds-of-cyber-incidents-sophos-595130). 25.02.2026).***

***

«Нове дослідження Ради організацій малого бізнесу Австралії (COSBOA) виявляє постійні прогалини в кібербезпеці серед малих і середніх підприємств, особливо в секторі гостинності, де базові засоби контролю, такі як унікальні паролі, багатофакторна автентифікація (MFA) та хмарні резервні копії, все ще застосовуються непослідовно. Лише 47% підприємств сфери гостинності використовують унікальні паролі, 37% зберігають резервні копії в хмарі, а приблизно третина використовує MFA для електронної пошти — незважаючи на те, що фішинг, програми-вимагачі, компрометація ділової електронної пошти та порушення безпеки даних є поширеними загрозами. Ці висновки мають наслідки для страховиків, які все частіше враховують спостережувані заходи контролю та специфічні для сектору вразливості при встановленні цін та умов страхування…

Національні дані підтверджують ризики: Управління комісара з питань інформації Австралії зафіксувало 532 повідомлення про порушення безпеки даних у першій половині 2025 року, з яких 59% були пов'язані зі зловмисними атаками, а 37% — з людською помилкою. Середні збитки від кіберзлочинів, про які повідомили самі підприємства, сягнули 80 850 доларів на одне підприємство, а Австралійське управління зв'язку повідомило про зростання кількості інцидентів, включаючи різке збільшення кількості DDoS-атак та кампаній з викрадення облікових даних. Зловмисники використовують системи, підключені до Інтернету, та застосовують методи «життя за рахунок землі», які часто підсилюються інструментами штучного інтелекту…

В результаті, як страховики, так і малі та середні підприємства адаптуються до нових умов. Брокери використовують дані цього сектору для обговорення мінімальних стандартів безпеки та необхідності кіберстрахування, а майже 66% організацій планують збільшити витрати на кібербезпеку в 2026 році. Прогнозується, що глобальні премії за кіберстрахування будуть стабільно зростати, що свідчить про жорсткість ринку, де ретельна перевірка страхових ризиків, впровадження багатофакторної аутентифікації, практики резервного копіювання та готовність до інцидентів будуть все більше впливати на доступність страхового покриття та ціноутворення для малих підприємств». ***(Roxanne Libatique. Research finds cyber gaps in small hospitality businesses // KM Business Information Australia Pty Ltd (https://www.insurancebusinessmag.com/au/news/cyber/research-finds-cyber-gaps-in-small-hospitality-businesses-566542.aspx). 25.02.2026).***

***

«Інцидент безпеки — кібератака, яка успішно отримує доступ до ресурсів підприємства або ставить під загрозу фінанси, діяльність та репутацію організації — є майже неминучим для кожної організації, а серйозне порушення може потенційно призвести до банкрутства компанії. Для боротьби

з цією загрозою кожна організація потребує узгодженої стратегії реагування на інциденти (IR), яка є плановим підходом до виявлення та управління кібератаками з метою мінімізації ризиків та обмеження збитків, часу відновлення та витрат, пов'язаних з будь-яким інцидентом безпеки…

Основою будь-якої стратегії реагування на інциденти є добре розроблений план реагування на інциденти, який повинен слугувати докладним, авторитетним керівництвом від початкового виявлення інциденту до оцінки, сортування, локалізації та вирішення, і який повинен бути складений, перевірений та випробуваний шляхом введення в дію до настання кризової ситуації. Ключові етапи розробки цього плану включають встановлення політики високого рівня для керівництва процесом прийняття рішень під час інцидентів; формування та навчання спеціальної команди IR з чітко визначеними ролями; створення детальних інструкцій, що стандартизують процедури для конкретних сценаріїв; розробку плану комунікації, що координує діяльність керівників, юристів, фахівців з управління персоналом та комунікацій; проведення навчань, включаючи сесії для керівників, технічного персоналу та міжфункціональних команд, для відпрацювання ролей та тестування плану в реалістичних сценаріях. План також повинен містити вичерпний огляд ролей, обов'язків, типів інцидентів, мережевої інфраструктури, процедур виявлення та локалізації, протоколів ліквідації та відновлення, процесів повідомлення про порушення, завдань після інциденту, списків контактів, а також процесу тестування та перегляду, з рекомендаціями щодо офіційних переоцінок та щорічних переглядів.

Встановлені рамки безпеки від таких організацій, як NIST, SANS Institute, ISO, ISSA та ISACA, окреслюють шість етапів реагування на інциденти: підготовка (створення команди, політик та інструкцій); виявлення та ідентифікація (моніторинг та сортування подій безпеки); локалізація (запобігання погіршенню інцидентів); ліквідація (усунення загроз, включаючи шкідливе програмне забезпечення та зловмисні облікові записи); відновлення (відновлення нормальної роботи та усунення вразливостей); та винесені уроки (аналіз того, що сталося, та визначення можливостей для вдосконалення засобів контролю, політик та процедур)…» ***(Michelle Drolet. Building an Effective Incident Response Strategy to Combat Cyberattacks // (https://securityboulevard.com/2026/02/building-an-effective-incident-response-strategy-to-combat-cyberattacks/). 18.02.2026).***

***

«У звіті SecurityWeek про злиття та поглинання в галузі кібербезпеки за 2025 рік налічується 426 угод (334 з них — виключно в цій галузі), що на 5 % більше, ніж у 2024 році, і свідчить про повернення до зростання після двох років спаду, хоча цей показник все ще нижчий за піковий рівень 2022 року, який становив 455 угод. Вартість і складність угод зросли, оскільки ринок перейшов від буму «купуй все» 2021–2022 років до більш стратегічної міжнародної консолідації… Ландшафт стає все більш глобальним: США взяли участь у 288 з 426 угод (67%), що на 63% більше, ніж у 2023 році, але значно менше, ніж 80% у 2021 році; Великобританія зберегла своє друге місце з 64 угодами; Ізраїль повернув

собі третє місце з 34 угодами; а Ірландія та Швеція піднялися відповідно на 12 і 11 місце.

Були оприлюднені фінансові дані щодо 74 угод на загальну суму 92,5 млрд доларів (включаючи 84 млрд доларів за 63 операціями з чистою спеціалізацією), що на 82% більше, ніж у минулому році, завдяки запланованій Google покупці Wiz за 32 млрд доларів. Одинадцять угод перевищили 1 млрд доларів, серед яких можна виділити такі приклади, як Palo Alto Networks–CyberArk (25 млрд доларів) і Chronosphere (3,3 млрд доларів), ServiceNow–Armis (7,7 млрд доларів) і Veza (1 млрд доларів), Francisco Partners–Jamf (2,2 млрд доларів), Veeam–Securiti AI (1,7 млрд доларів) і Proofpoint–Hornetsecurity (1,8 млрд доларів). Зростання було забезпечено угодами в діапазоні від 100 до 999 млн доларів, що відображає перевагу покупців до зрілих, усталених об'єктів та стратегічну фазу масштабування, в якій середні спеціалізовані компанії об'єднуються в більші платформи; кількість оприлюднених угод на суму менше 100 млн доларів зменшилася до 26 (з 32). Активність MSSP (постачальники керованих рішень з безпеки) зросла до 125 угод (60 чисто спеціалізованих) з 119 у 2024 році, але залишається значно нижчою за темп 150+ у 2022–2023 роках, що свідчить про «нову норму», оскільки керовані послуги залишаються центральними для малих і середніх підприємств…

Тенденції в секторі вказують на перехід до стійкості та відповідності вимогам: GRC (Управління, ризики та дотримання вимог) досяг п'ятирічного максимуму в 82 угоди; захист даних зріс з 44 до 63; ідентифікація відновилася до 43; а безпека штучного інтелекту піднялася з 8 до 13. До сегментів, що охолонули, належать реагування на інциденти (з 38 до 25), придбання під керівництвом приватного капіталу (з 37 у 2023 році до 18), промислова/OT-безпека (з 16 до 9) та безпека додатків (з 31 до 26). Дві категорії залишилися стабільними: мережева безпека (близько 40 угод щорічно з 2022 року) та урядові підрядники (36–38 на рік, з 36 у 2025 році). Загалом, 2025 рік ознаменувався консолідацією в галузі управління, ризиків, дотримання вимог та безпеки, орієнтованої на дані, з переходом від реактивних інструментів до надійних платформ, що відповідають нормативним вимогам». ***(Eduard Kovacs. SecurityWeek Report: 426 Cybersecurity M&A Deals Announced in 2025 // (https://www.securityweek.com/securityweek-report-426-cybersecurity-ma-deals-announced-in-2025/). 25.02.2026).***

***

«Сучасна кібербезпека стикається з труднощами не через брак інструментів, а через те, що взаємопов'язані автоматизовані середовища концентрують ризики таким чином, що традиційні моделі безпеки не можуть їх стримати. В результаті кіберінциденти стають системними каскадами, а не поодинокими подіями. З огляду на 2026 рік, зловмисники будуть використовувати цю реальність, спираючись на швидкість і довірчі відносини, а не на нові експлойти, що вимагатиме фундаментальної зміни в оборонному мисленні…

Найбільш значним порушенням стане розширення «розриву в швидкості», коли автономні атаки ШІ будуть працювати зі швидкістю машини, скануючи вразливі місця і запускаючи корисні навантаження за лічені секунди — набагато

швидше, ніж можуть реагувати аналітики-люди. Це зробить традиційні засоби захисту, керовані людьми, застарілими, змушуючи організації впроваджувати автоматизовані засоби стримування та виявлення на основі ШІ, які реагують у режимі реального часу. Одночасно з цим, компрометація ланцюгів постачання стане найбільш руйнівним вектором атак, переходячи від націлювання на окремі організації до стратегій «атакувати одну, заразити багатьох». Зловмисники будуть непомітно ховатися всередині надійних сторонніх постачальників та інструментів автоматичного оновлення, роблячи ці порушення непомітними та важкими для виявлення, доки вони не поширяться по всій екосистемі…

Ці загрози посилюються небезпечною надмірною залежністю від систем оцінки відповідності та безпеки, які створюють помилкове відчуття захищеності. Хоча нормативні рамки та рейтинги постачальників можуть задовольняти страховиків, вони часто приховують критичні слабкі місця в ідентифікації та конфігурації, а це означає, що проходження оцінки не рівнозначне реальній безпеці. В кінцевому підсумку, стійкість у 2026 році буде визначатися не охопленням контролю або переліками перевірок, а здатністю швидко виявляти порушення та відновлювати роботу у взаємопов'язаних середовищах. Організації повинні відмовитися від припущення про запобігання і замість цього розробити програми безпеки, які передбачають можливі збої та постійно перевіряють захист». ***(Ross Filipek. When Cybersecurity Breaks at Scale: What 2026 Will Expose // THE FAST MODE (https://www.thefastmode.com/expert-opinion/47097-when-cybersecurity-breaks-at-scale-what-2026-will-expose). 16.02.2026).***

***

«Запобігання порушенням безпеки даних вимагає не тільки технічних засобів захисту, а й інтеграції кібербезпеки в систему управління ризиками підприємства (ERM). Однак, незважаючи на широке визнання фінансової важливості кібербезпеки, більшість організацій продовжують ізолювати її: дослідження APQC, проведене серед 5000 компаній, показує, що лише 41% мають значну інтеграцію кібербезпеки в ERM, а лише 23% поширюють єдині структури ризиків на постачальників і партнерів, навіть незважаючи на те, що треті сторони відіграють значну роль у великих порушеннях безпеки. Така невідповідність обмежує видимість, уповільнює прийняття рішень і перешкоджає проактивному зниженню ризиків. Там, де інтеграція є більш сильною, організації отримують більш повне уявлення про ризики, що дозволяє раніше виявляти їх, координувати реагування та швидше відновлюватися, перетворюючи кібербезпеку з оборонної функції IT на спільну відповідальність підприємства, вбудовану в процеси управління та бізнес-процеси на рівні вищого керівництва…

Фінансові керівники відіграють ключову роль у практичному впровадженні ERM. Коли кібербезпека залишається поза межами ERM, фінансовий відділ втрачає контроль над ризиками, що негативно позначається на координації. Включення кібербезпеки до постійного управління ERM (ради з питань ризиків, звітування перед правлінням) гарантує, що вона буде конкурувати за увагу та ресурси нарівні з фінансовими та операційними ризиками. Наполягання на фінансовому підході — як заходи контролю зменшують збитки, час простою або ризик втрати доходів —

допомагає узгодити інвестиції з рівнем прийнятного ризику, навіть за допомогою орієнтовних оцінок… Вбудовування засобів контролю та моніторингу в комплексні бізнес-процеси, особливо у сфері фінансів, закупівель та спільних послуг, дозволяє усунути ризики на етапі передачі повноважень, де вони виникають, а поширення нагляду ERM на постачальників, що мають значний вплив, забезпечує підзвітність, загальні стандарти та постійний моніторинг у всій екосистемі. Стійкість формується задовго до спрацьовування сигналізації: інтегроване управління виявляє проблеми раніше, відповідальність на рівні процесів уточнює підзвітність, а загальні показники покращують компроміси. Фінансові директори не повинні керувати кібербезпекою, але вони повинні забезпечити, щоб технічні знання впливали на рішення підприємства, посилюючи інтеграцію за допомогою управління, показників та міжфункціональної співпраці, щоб передбачати, реагувати та відновлюватися після збою з упевненістю». ***(Kelley Pruetz and Kristen Senz. What CFOs can do to close the cyber-ERM integration gap // TechTarget, Inc. (https://www.cfo.com/news/what-cfos-can-do-to-close-the-cyber-erm-integration-gap/811728/). 10.02.2026).***

***

«У звіті Tidal Cyber «Захист від загроз у 2025 році» керівникам служб інформаційної безпеки рекомендується перейти від реактивного виявлення на основі CVE та сигнатур до картографування та постійної перевірки реальної поведінки зловмисників, аргументуючи це тим, що щорічні оцінки та щоквартальні оновлення контролю не можуть відповідати темпам розвитку тактик, технік і процедур (TTP)… Дані показують, що TTP зараз є мінливими, а не стабільними: перехід Void Rabisu від фінансових злочинів до шпигунства ускладнює атрибуцію та робить захист, орієнтований на боротьбу з шахрайством, неефективним; Scattered Spider націлений на платформи співпраці SaaS і використовує рівні віртуалізації (наприклад, обхід пісочниці T1651), щоб вийти за межі традиційної сегментації та EDR; а ransomware Akira поєднує постійні процедури (такі як видалення тіньових копій на основі WMI) з незначними варіаціями виконання, які обходять статичні сигнатури, підкреслюючи необхідність поведінкового аналізу… Чотири макротренди посилюють ризики для підприємств: нульові дні стали товаром на нелегальних ринках, скорочуючи час на реагування до декількох днів і змушуючи зосередитися на поведінці після експлуатації; Соціальна інженерія на основі штучного інтелекту підсилила фішинг і вішинг за допомогою масштабного підроблення особи керівників; програмне забезпечення для вимагання викупу еволюціонувало в вимагання на основі важелів впливу (крадіжка даних, погрози розкриття інформації та регуляторний тиск), що обходить стратегії, орієнтовані на резервне копіювання; а геополітична розмитість стирає чіткі межі між злочинністю, хактивізмом і діяльністю держави, вимагаючи більш широких моделей загроз…

Технічний огляд висвітлює 300% зростання зловживання штучним інтелектом (T1588.007) зловмисниками для створення поліморфних корисних навантажень, автоматизації розвідки та налаштування ухилення від телеметрії захисників; складні тактики соціального інжинірингу, такі як Spearphishing Voice

(T1598.004) та Malicious Copy & Paste (T1204.004), використовують людську поведінку, а не технічні недоліки; а вразливість SaaS/ідентичності, особливо зловживання токенами OAuth, дозволи підключених додатків та облікові записи служб, забезпечують прихований постійний доступ, що вимагає глибокої інструменталізації IAM, шаблонів автентифікації та API SaaS… Дорожня карта звіту зосереджена на трьох змінах: перехід від «картографування технік» в ATT&CK до процедурної деталізації (конкретні інструменти, послідовності команд та умови середовища) для цільового виявлення та перевірки контролю; застосування постійної, орієнтованої на поведінку перевірки з регулярною емуляцією супротивника та створенням «фіолетової команди» (принаймні раз на місяць) для тестування реальних процедур; переосмислення периметра навколо ідентичності, SaaS та хмарних площин контролю за допомогою багатої телеметрії з журналів IdP, API SaaS, хмарних операцій та міжорендарської автентифікації (кінцева точка залишається важливою, але більше не є центром тяжіння).

У 2026 році стійкість буде залежати від адаптивності: впровадження процедурної видимості поведінки, інвестиції в телеметрію ідентичності/SaaS та постійне вдосконалення засобів захисту. Бюджети повинні надавати пріоритет аналітиці поведінки та видимості хмари, керівництво повинно прийняти, що ідеальна профілактика неможлива, а успіх буде на боці організацій, які відповідають темпу супротивників швидким виявленням та реагуванням, залишаючи відстаючих як приклади для вивчення, а не еталони». ***(Findings From The Tidal Cyber 2025 Threat-Led Defense Report // Techstrong Group Inc. (https://securityboulevard.com/2026/02/findings-from-the-tidal-cyber-2025-threat-led-defense-report/). 19.02.2026).***

***

«…Англомовна Вікіпедія заблокувала Archive.today та пов'язані домени (archive.is, archive.ph) з негайним вступом в силу після того, як слідчі виявили, що сервіс захоплював браузери відвідувачів через Captcha для проведення DDoS-атаки проти блогера Яні Патокалліо та маніпулював архівними сторінками, щоб дискредитувати його, змінюючи імена в знімках. Суперечка почалася після того, як Патокалліо повідомив про непрозорих операторів сервісу, які, як стверджується, використовували псевдоніми «Денис Петров» і «Маша Рабінович» та мали зв'язки з Росією, але переросла в те, що вікіпедисти назвали цифровим скандалом: зловживання апаратним забезпеченням читачів для атак і фальсифікації «незмінних» записів, що суперечить основному принципу Вікіпедії — перевірюваності…

Хоча деякі редактори стверджували, що Archive.today був корисним для обходу платних стін, спільнота дійшла висновку, що надійність джерела та безпека користувачів переважають зручність. Масштаби очищення великі — близько 695 000 посилань Archive.today на приблизно 400 000 сторінок — тепер заплановано видалити або замінити надійними альтернативами, такими як Internet Archive (archive.org) або Ghostarchive; редакторів закликали видалити посилання на архів, якщо оригінали залишаються в мережі. Цей епізод також висвітлює тривалу непрозорість власності сервісу (як повідомляється, навіть попри зусилля ФБР

викрити її через реєстратора Tucows) та практику залякування Патокалліо, включаючи фейкові профілі та відвертий контент, створений штучним інтелектом… Фонд Вікімедіа підтримав заборону як необхідний крок для захисту користувачів та цілісності контенту і заявив, що в разі потреби втрутиться безпосередньо. Наслідки цього рішення посилили заклики до створення архівної служби під управлінням Вікімедіа, перспективу якої Патокалліо назвав такою, що заслуговує на підтримку». ***(Stefan Krempl. Hundreds of thousands of links: Wikipedia bans Archive.today after cyberattack // heise medien (https://www.heise.de/en/news/Hundreds-of-thousands-of-links-Wikipedia-bans-Archive-today-after-cyberattack-11185344.html). 22.02.2026).***

***

«Новий звіт Proton AG показує, що, незважаючи на зростання інвестицій у кібербезпеку, малі та середні підприємства (МСП) продовжують стикатися зі значними кіберризиками: кожне четверте з них зазнало кібератаки або витоку даних протягом останнього року. Звіт про кібербезпеку МСП за 2026 рік, заснований на опитуванні 3000 керівників підприємств, показує, що, хоча рівень обізнаності та заходи з управління покращилися (92% МСП впровадили засоби захисту, а 74% МСП у Великобританії нещодавно провели оцінку ризиків), між витратами та реальним рівнем стійкості до ризиків залишається значна різниця, що пов'язано насамперед з людським фактором…

Дослідження показує, що майже 39% всіх інцидентів у сфері кібербезпеки пов'язані з проблемами, яких можна було б уникнути, такими як небезпечне спільне використання паролів (що залишається поширеним явищем навіть при використанні менеджерів паролів), непослідовне дотримання політик та різний рівень кваліфікації співробітників. Фінансові та операційні наслідки цих порушень є значними: більшість постраждалих малих та середніх підприємств повідомляють про збитки в розмірі від 7500 до 75 000 фунтів стерлінгів, що іноді перевищує їхній річний бюджет на кібербезпеку.

Додаткову складність створює швидке впровадження штучного інтелекту, яке приносить нові невизначеності, оскільки 30% підприємств, що використовують платформи ШІ, не довіряють постачальникам ШІ повністю захищати їхні власні дані, що створює прогалину в прозорості, яка може призвести до нових ризиків витоку даних. З позитивного боку, у звіті вказується, що кібербезпека еволюціонує від суто технічної функції до конкурентної переваги, причому дві третини малих і середніх підприємств заявляють, що надійні практики захисту даних зараз мають вирішальне значення для залучення нових клієнтів. У дослідженні робиться висновок, що для подолання розриву між уявленням про готовність і операційною стійкістю організації повинні вийти за межі простого впровадження інструментів і зосередитися на впровадженні безпечних моделей поведінки у свою повсякденну діяльність…» ***(SMBs Struggle to Translate Cybersecurity Investment into Real-World Resilience, Study Finds // IT Security Guru (https://www.itsecurityguru.org/2026/02/26/smbs-struggle-to-translate-cybersecurity-investment-into-real-world-resilience-study-finds/). 26.02.2026).***

***

«Кібербезпека переходить від захисту статичних цифрових периметрів до боротьби із загрозами, які мутують швидше, ніж традиційні засоби контролю можуть їх виявити, і «поліморфізм» — практика постійної зміни програмного забезпечення або криптографічної поведінки з метою уникнення аналізу — знаходиться в центрі цієї зміни. Поліморфне шкідливе програмне забезпечення більше не є винятковим випадком: згадані в тексті звіти про загрози свідчать, що воно з'являється в значній частині нових штамів, все частіше поширюється через зашифровані канали і часто поєднується з техніками упаковки/заплутування, які дозволяють обійти сканери на основі сигнатур і хеш-функцій… Штучний інтелект прискорює цю еволюцію, дозволяючи шкідливому програмному забезпеченню динамічно генерувати мутації, вчитися на невдалих спробах обійти захист і оптимізувати ухилення в режимі реального часу, що змушує захисників переходити до виявлення на основі поведінки, аналізу аномалій і кореляції телеметрії на основі штучного інтелекту, а не статичних правил…

Така ж логіка зараз застосовується в захисних цілях до криптографії. Хоча традиційне шифрування може бути математично надійним, його передбачувані реалізації (фіксовані алгоритми, статичні ключі, повторювані шаблони) можуть бути використані супротивниками за допомогою масштабної аналітики, і воно піддається ризикам «зібрати зараз, розшифрувати пізніше» у міру розвитку квантових обчислень… Запропонованим рішенням є «поліморфне шифрування» та ширша криптологічна гнучкість: постійна ротація ключів, перемикання або шарування алгоритмів та зміна криптографічних конфігурацій, щоб перехоплений шифрований текст став менш корисним, а аналіз шаблонів — складнішим. З цієї точки зору, постквантова криптографія є необхідною, але недостатньою сама по собі, якщо її застосовувати передбачуваними способами; поєднання PQC з адаптивними, поліморфними підходами позиціонується як більш стійкий шлях. У тексті також наводиться комерційний приклад (робота Ageos з поліморфного шифрування) як ілюстрація цієї тенденції, в якому стверджується, що криптографічні структури з низькою затримкою, що постійно змінюються, можуть допомогти захистити пристрої та організації від атак, посилених штучним інтелектом, та майбутніх атак з використанням квантових технологій». ***(Chuck Brooks. AI Polymorphic Threats Are Forcing A Rethink Of Cybersecurity // Forbes (https://www.forbes.com/sites/chuckbrooks/2026/02/21/ai-polymorphic-threats-are-forcing-a-rethink-of-cybersecurity/). 21.02.2026).***

***

«Фахівці з кібербезпеки стикаються з фундаментальним переходом від традиційної оборони до більш надійної концепції кіберстійкості, як детально описано експертами Integrity360 на 2026 рік. Ця еволюція визнає неминучість порушень і підкреслює здатність організації передбачати, протистояти, відновлюватися після атак і адаптуватися до них, що зараз закріплено в таких правових рамках, як Закон ЄС про цифрову операційну стійкість. Це вимагає від організацій зосередитися на таких показниках, як максимально допустимий час

простою та цілі щодо часу відновлення, причому проактивна підготовка є ключовим фактором виживання…

У 2026 році загрози стануть значно складнішими через низку факторів, що збігаються. По-перше, штучний інтелект має потужний вплив, що дозволяє проводити дуже переконливі кампанії соціального інжинірингу та розробляти шкідливі програми (наприклад, «Bad GPT»), які уникнуть традиційних засобів виявлення. Організаціям настійно рекомендується встановити чіткі правила використання штучного інтелекту та інструменти управління для контролю ризиків, пов'язаних як із санкціонованим, так і з «тіньовим» використанням штучного інтелекту…

По-друге, геополітика змінює цифрову сферу, а національні держави, такі як Росія, Іран, Китай і Північна Корея, вдосконалюють свої методи, зокрема шляхом компрометації ланцюгів постачання та крадіжки інтелектуальної власності. Групи хактивістів додають ще один рівень ризику, націлюючись на приватні підприємства на основі символічних асоціацій, що означає, що компанії можуть опинитися під перехресним вогнем міжнародних напружень.

По-третє, національна критична інфраструктура та операційні технології (OT) все частіше стають об'єктом атак, причому кількість атак з використанням програм-вимагачів на ці сектори зросте приблизно на 80% до 2025 року. Ці середовища є привабливими цілями через відставання інвестицій у кібербезпеку, високі витрати на простої, що стимулюють швидку виплату викупу, та вразливості, такі як відсутність сегментації мережі — критична проблема, оскільки понад 70% порушень OT походять із підключених IT-систем…

Нарешті, зловмисники все частіше обходять захист кінцевих точок, щоб безпосередньо атакувати хмарні ідентичності, що вимагає переходу до розширеної видимості у всьому технологічному середовищі, включаючи хмару, додатки та системи ідентифікації. Щоб бути готовими, організації повинні підвищити кіберстійкість до рівня відповідальності правління, розробити захист на основі розвідки, впровадити надійну сегментацію мережі між IT та OT і розширити виявлення за межі кінцевих точок. Основний висновок на 2026 рік полягає в тому, що виживання залежить не від досконалого запобігання, а від ретельної підготовки до того, щоб витримати і відновитися після неминучих успішних атак». ***(Patricia Rodrigues. Cybersecurity in 2026: From Protection to Resilience // Sync NI (https://syncni.com/article/14861/cybersecurity-in-2026-from-protection-to-resilience). 25.02.2026).***

***

«Порти, термінали та логістичні центри перетворилися на критично важливі центри обробки даних, де порушення роботи операційних систем, таких як TOS і PCS, може спричинити катастрофічний ефект доміно в усьому ланцюжку поставок, що призведе до зупинки митного оформлення, штрафних санкцій за порушення договорів і втрати довіри клієнтів. Кібербезпека більше не є проблемою IT-відділу, а питанням виживання на ринку. Логістичний сектор стикається зі сплеском спроб фішингу, коли злочинці видають себе за ділових партнерів, щоб маніпулювати комерційною документацією, такою як рахунки-

фактури та пакувальні листи. Навіть незначна зміна, така як зміна номера банківського рахунку, може призвести до серйозних митних та фінансових наслідків, що робить суворі процедури перевірки документів необхідними для безпеки…

Загроза посилюється через все частіше використання дезінформації, часто за допомогою штучного інтелекту, що може спричинити хаос у комунікації та сприяти кібератакам. Ця ескалація ризиків тепер регулюється Директивою ЄС NIS 2, яка встановлює нові зобов'язання з кібербезпеки для сектору транспорту та логістики, включаючи аналіз ризиків, безпеку ланцюгів постачання та повідомлення про інциденти. Директива вимагає вжиття таких заходів, як багатофакторна автентифікація, криптографія та регулярні аудити безпеки, опосередковано поширюючи ці вимоги на менші суб'єкти господарювання в ланцюгах постачання великих операторів…

Щоб захиститися від цих загроз, оператори повинні надавати пріоритет кібербезпеці, навчаючи співробітників розпізнавати фішинг, впроваджуючи процедури подвійної перевірки документів, обмежуючи доступ до конфіденційних даних та регулярно оновлюючи системи. У сучасному цифровому світі обізнаність співробітників та проактивні заходи безпеки є настільки ж важливими, як і знання нормативних вимог, оскільки вони мають фундаментальне значення для забезпечення безперервності бізнесу та операційної стійкості». ***(Joanna Porath. Cybersecurity in transport and logistics: one fake email can halt the supply chain // Trans.INFO (https://trans.info/en/cybersecurity-logistics-457004). 23.02.2026).***

***

«Кібербезпека стала одним із пріоритетних напрямків для венчурних інвестицій, набувши стратегічного значення в умовах, коли на перший план виходять питання оборони, штучного інтелекту та національної стійкості. Хоча кібербезпека не така «ефектна», як оборонні технології, орієнтовані на апаратне забезпечення, наприклад дрони, вона зараз визнається критично важливою сферою конфлікту, необхідною для забезпечення цифрової основи всього, від супутникових систем до критичної інфраструктури. Недавні кібератаки на європейські аеропорти та посилення взаємозв'язку інфраструктури, такої як електростанції, посилили політичну та інвестиційну увагу до стійкості, створивши значні можливості для стартапів у цій сфері…

Інвестори виявляють великий інтерес до таких сфер, як засоби протидії обману (наприклад, іспанська компанія CounterCraft), надійне шифрування для національної безпеки (наприклад, британська компанія Sitehop), аналіз дезінформації (наприклад, лондонська компанія Refute) та безпека систем штучного інтелекту на периферії. Стратегічна цінність кібербезпеки ще більше підтверджується венчурними фондами «Smart Money», які, за даними CB Insights, підтримують значну частину майбутніх «єдинорогів» і вважають кібербезпеку найбільш ймовірним джерелом виходу з інвестицій у найближчому майбутньому. Державне фінансування також зростає: наприклад, Великобританія виділяє мільйони на підтримку кіберстартапів та малих і середніх підприємств у рамках

своєї промислової стратегії, визнаючи значний потенціал цього сектору в плані генерування доходів та зростання зайнятості…

Серед венчурних капіталістів, які активно інвестують у цю сферу, є DataTribe, яка використовує свій багатий досвід, набутий як у Кремнієвій долині, так і в розвідувальному співтоваристві, для створення та фінансування компаній, що займаються кібербезпекою на початковому етапі, через свою програму Foundry, а також M12, венчурний фонд Microsoft, очолюваний керуючим партнером Тоддом Гремом. Грем, який має досвід роботи як у стартапах, так і у великих постачальниках інфраструктури, таких як Cisco та VMware, зосереджується на кібербезпеці, інструментах для розробників та хмарній інфраструктурі, приділяючи особливу увагу загрозам, пов'язаним з людським фактором, та революційним стратегіям виходу на ринок». ***(VCs Investing In Cybersecurity In 2026 // TechRound (https://techround.co.uk/cybersecurity/vcs-investing-cybersecurity/). 25.02.2026).***

***

«На Мюнхенській конференції з безпеки та Мюнхенській конференції з кібербезпеки 2026 року, що проходили під гаслом «Під руйнуванням» і зібрали близько 2000 учасників, серед яких було приблизно 60 глав держав і понад 200 міністрів, лідери дійшли одностайної думки: кібербезпека стала основним компонентом національної безпеки. Дискусії на обох заходах відображали занепокоєння тим, що після закінчення холодної війни порядок, заснований на правилах, руйнується «кулею для знесення будівель», і на горизонті не видно чіткої системи, яка могла б його замінити. Міністр закордонних справ Індії описав майбутній період як «сутінкову зону», в якій в одних місцях можуть діяти правила, а в інших — «закон джунглів»… Ця невизначеність також вплинула на трансатлантичні відносини: американські чиновники висловили бажання налагодити партнерство, але закликали Європу переглянути частину своїх цифрових правил та ширшу політичну програму, тоді як європейські лідери наголошували на цифровому суверенітеті, правах людини та зобов'язаннях щодо верховенства права і наполягали, що «MAGA не є нашою програмою», залишаючи самі відносини в тій самій невизначеності…

Гібридний конфлікт у цифрову епоху став ще однією гарячою темою, і багато доповідачів перейшли від «впровадження норм» до «обходу норм», оскільки супротивники ігнорують існуючі правила; посилилися заклики до більшого ризику, більш рішучих кібератак і навіть асиметричних «хакерських ударів у відповідь», незважаючи на проблеми з атрибуцією та ризик ескалації. Штучний інтелект розглядався як прискорювач і дестабілізатор: спікери попереджали про його використання в дронах і автономних системах, проводили паралелі з ранніми гонками ядерних озброєнь і ставили під сумнів, чи потрібен світу «цифровий кубинський момент», перш ніж з'являться серйозні обмеження… Хоча глобальні ініціативи з управління штучним інтелектом розширюються — панелі ООН та поточні саміти «Блетчлі-процесу» — Мюнхен не дав чіткої відповіді на питання, як можна домовитися про обов'язкові обмеження та забезпечити їх дотримання. Постійною проблемою була «цілісність даних»: як стверджував Брюс Шнайер, маніпулювання навчальними даними та інформаційними потоками може стати

небезпечнішим за крадіжку, оскільки системи штучного інтелекту не можуть надійно відрізнити правду від неправди, що може спричинити реальну шкоду в таких сферах, як транспорт, охорона здоров'я та дипломатія…

Конференції також натякнули на більш широкі структурні зміни в управлінні Інтернетом та кібердипломатії. Хоча співпраця з галузевими та технічними експертами була в принципі підтверджена, багато урядових спікерів висловилися за більш ієрархічні, вертикальні моделі в ім'я «цифрового суверенітету», при цьому громадянське суспільство було порівняно відсунуте на другий план. Ця тенденція була підкріплена ознаками фрагментації в багатосторонніх форумах, орієнтованих на розбудову потенціалу та права: вихід США з таких організацій, як GFCE, Європейський центр гібридних загроз та Коаліція за свободу в Інтернеті, був розкритикований як удар по колективній обороні проти глобальних кіберзагроз. Загалом, Мюнхен показав світ, який рухається від співпраці, керованої нормами кіберпорядку, до суперечливої, державно-орієнтованої конкуренції, де штучний інтелект, наступальні кіберзаходи та послаблення багатосторонньої довіри можуть штовхнути цифрову дипломатію у все більш бурхливі води». ***(Wolfgang Kleinwächter. Munich Cybersecurity Conference 2026: Moving Into the Twilight Zone // CircleID (https://circleid.com/posts/munich-cybersecurity-conference-2026-moving-into-the-twilight-zone). 23.02.2026).***

***

«Розширення браузера додають зручності — блокувальники реклами, менеджери паролів, бічні панелі штучного інтелекту та інструменти продуктивності — але вони також створюють зростаючу та недостатньо контрольовану поверхню для атак, оскільки постійно працюють з підвищеними правами доступу всередині браузера. Після надання доступу користувачем розширення може читати та змінювати сторінки, відстежувати активність у вкладках, отримувати доступ до сеансів та взаємодіяти з додатками SaaS, і воно може продовжувати робити це непомітно завдяки автоматичним оновленням, які користувачі рідко перевіряють. Тому зловмисні розширення не потребують використання вразливостей програмного забезпечення; вони можуть «законно» діяти в рамках моделі дозволів браузера, щоб викрадати облікові дані, перехоплювати сеанси, стежити за користувачами, вводити вміст і здійснювати шахрайство або корпоративне шпигунство…

Останні дослідження показують, що зараз це є масштабованою загрозою. Malwarebytes повідомило про кампанії в середині 2025 року, коли розширення в офіційних магазинах Chrome і Edge — часто з позитивними відгуками і навіть перевіркою платформи — пізніше були перетворені на зброю за допомогою оновлень, перетворивши надійні інструменти на шпигунське програмне забезпечення, яке вплинуло на мільйони людей. Інші випадки стосувалися розширень, що маскувалися під інструменти штучного інтелекту для підвищення продуктивності, які збирали розмови з таких сервісів, як ChatGPT і DeepSeek, а також дані про перегляди, ризикуючи розкриттям власницького коду, досліджень і конфіденційних ділових обговорень. Тривалі кампанії, такі як «DarkSpectre», демонструють модель «сплячого агента»: розширення можуть залишатися

нешкідливими протягом багатьох років, щоб створити велику базу встановлень, а потім стати шкідливими після зміни власника або розробника та тихого оновлення, що робить кількість завантажень, рейтинги та тривалість існування ненадійними сигналами безпеки. Це фактично перетворює розширення на ризик для ланцюга постачання на рівні браузера, який набагато менше контролюється, ніж традиційне програмне забезпечення…

Зменшення ризиків є скоріше практичним, ніж абсолютним: встановлюйте менше розширень, видаляйте невикористовувані, перевіряйте розширення та оновлення (особливо зміни у власності), ретельно вивчайте запити на дозвіл, відокремлюйте роботу від особистого перегляду веб-сторінок, а в організаціях ставитеся до розширень як до керованого програмного забезпечення — інвентаризація, політика та постійний перегляд. Посилення виявлення та реагування за допомогою керованого XDR може ще більше зменшити оперативне навантаження, але головний урок полягає в тому, що довіру до розширень необхідно постійно переоцінювати, оскільки «безпечне вчора» може стати «компрометованим сьогодні». ***(Tony Burgess. The hidden cybersecurity risk lurking in your browser extensions // Barracuda Networks, Inc. (https://blog.barracuda.com/2026/02/25/hidden-cybersecurity-risk-browser-extensions). 25.02.2026).***

***

«Кіберзагрози стають дедалі більш витонченими та частими, часто використовуючи людські слабкості, а не лише технічні недоліки. Медіапсихологія, яка вивчає, як люди сприймають та обробляють цифрову інформацію, пропонує важливі уявлення про те, чому люди піддаються кіберманіпуляціям, та надає основу для розробки більш безпечних систем. П'ять ключових психологічних теорій є особливо важливими для розуміння цих вразливостей…

По-перше, теорія переконання пояснює, як зловмисники використовують такі сигнали, як авторитет, терміновість і дефіцитність у фішингових повідомленнях, наприклад, в електронних листах, що імітують листи від IT-відділів із темою «Необхідно вжити заходів негайно», щоб змусити користувачів підкоритися. По-друге, зловмисники використовують обмеженість людської уваги і створюють когнітивну плутанину за допомогою стратегічного багатозадачності, оскільки дослідження показують, що користувачі в два рази частіше клікають на фішингові посилання, коли вони когнітивно перевантажені… По-третє, вони використовують когнітивні упередження, такі як упередження підтвердження (використання очікувань, наприклад, затримки доставки посилок) та упередження оптимізму (переконання, що людина навряд чи стане жертвою), щоб зробити свої обмани більш ефективними. По-четверте, емоційне збудження використовується для обходу аналітичного мислення; наприклад, засновані на страху заклики в тривожних спливаючих повідомленнях спонукають користувачів виконувати шахрайські запити. Нарешті, зловмисники маніпулюють соціальною ідентичністю та впливом групи, імітуючи стилі внутрішньої комунікації довірених груп, що

зменшує підозру та збільшує ймовірність відповіді, як це було в разі порушення безпеки Національного комітету Демократичної партії у 2016 році…

Розуміння цих психологічних принципів є зараз фундаментальним для кібербезпеки, оскільки воно впливає на розробку більш стійких систем і підкреслює важливість освіти. Експерти з кібербезпеки повинні враховувати медіапсихологію у своїх технічних розробках, а професійні організації, такі як Товариство медіапсихології та технологій, активно вивчають ці застосування, щоб краще захищати споживачів у дедалі складнішому цифровому світі». ***(Bernard J. Luskin. The Importance of Media Psychology in Cybersecurity // Sussex Publishers, LLC (https://www.psychologytoday.com/gb/blog/the-media-psychology-effect/202602/the-importance-of-media-psychology-in-cybersecurity/amp). 26.02.2026).***

***

«Недавнє дослідження Zero100 показує, що кібербезпека стала головним питанням для великих підприємств: понад третина операційних директорів (COO) компаній з мільярдним оборотом вважають кіберінциденти «найбільшою загрозою для безперебійної роботи» у 2026 році, яка перевершує геополітичну нестабільність, потрясіння в торговельній політиці та порушення робочого процесу. Ці інциденти також сприймаються як «найшвидші потрясіння», з якими, на думку підприємств, їм доведеться зіткнутися. Хоча генеральні директори рекламують штучний інтелект як двигун продуктивності для акціонерів, настрої всередині компаній є більш стриманими; операційні директори розділилися в думках щодо того, чи допоможе штучний інтелект кібербезпеці, чи зашкодить їй: 50% вважають, що він може поліпшити зменшення ризиків, а 43% побоюються, що він погіршить ситуацію… Крім того, менше ніж один з п'яти керівників операційної діяльності вірить, що штучний інтелект зможе втілити в життя амбітні плани, які обіцяють. Ця обережна позиція підтверджується останніми звітами про загрози, такими як висновок Google від травня 2025 року про те, що групи кіберзлочинців активно атакують американські роздрібні компанії. У відповідь на це багато компаній збільшують інвестиції в передові технології, такі як біометрія, токенізація та системи моніторингу на основі штучного інтелекту, щоб виявляти та запобігати все більш витонченим кібератакам». ***(Jeena Sharma. Most businesses view cybersecurity as a bigger threat than tariffs or geopolitical instabilities // Morning Brew Inc. (https://www.retailbrew.com/stories/2026/02/24/most-businesses-view-cybersecurity-as-a-bigger-threat-than-tariffs-or-geopolitical-instabilities). 25.02.2026).***

***

«Трансформація портів з аналогових хабів у складні цифрові екосистеми призвела до зближення інформаційних технологій (IT) та операційних технологій (OT), що кардинально змінило архітектуру ризиків глобальних морських операцій. Ця інтеграція, підвищуючи ефективність, розширила поверхню морських атак настільки, що компрометація корпоративної мережі може призвести до фізичних наслідків, таких як зупинка терміналів, несправності при вивантаженні вантажів, посадка на мілину або системний

параліч ланцюга поставок, як продемонстрували атака NotPetya на Maersk у 2017 році та кібератака на Transnet у Південній Африці у 2021 році. Як наслідок, Allianz Risk Barometer 2026 та Міжнародна асоціація портів і гаваней (IAPH) зараз визнають кібербезпеку найважливішим глобальним бізнес-ризиком, причому 62% портів ставлять її вище за природні катастрофи та зміну клімату… На цьому тлі постає нагальне юридичне питання щодо того, чи є Міжнародний кодекс з охорони суден і портових споруд (ISPS), який був розроблений після 11 вересня 2001 року для боротьби з фізичним тероризмом, структурно пристосованим до цього конвергентного середовища загроз. Хоча ліберальне тлумачення ризик-орієнтованої структури Кодексу та рекомендацій частини B дозволяє включати «комп'ютерні системи та мережі» до оцінок безпеки, відсутність чітких, обов'язкових до виконання вимог щодо кібербезпеки часто призводить до того, що навчання та планування обмежуються традиційними фізичними парадигмами…

Міжнародні регуляторні заходи стають дедалі більш розбіжними, оскільки країни переходять від простого тлумачення до чіткого законодавчого регулювання. Сполучені Штати Америки запровадили обов'язкові плани з кібербезпеки та зобов'язання щодо звітності через Остаточне правило Берегової охорони 2025 року, тоді як Директива NIS2 та Закон про кібербезпеку Європейського Союзу класифікують порти як надзвичайно важливі об'єкти, що підлягають суворому управлінню та нагляду. Аналогічно, такі країни, як Італія та Велика Британія, посилюють вимоги щодо звітності про інциденти та інтегрують кібербезпеку в системи управління безпекою… На багатосторонньому рівні, хоча Міжнародна морська організація (IMO) включила кіберстійкість до системи управління безпекою суден, її інструменти залишаються переважно рекомендаційними та орієнтованими на судна; проте, наразі розробляється комплексна Стратегія цифровізації морського транспорту на 2027 рік. На додаток до цих зусиль, IAPH взяла на себе провідну роль, виступаючи за «кібербезпеку за замовчуванням» та управління на виконавчому рівні, підкреслюючи, що кібербезпека є відповідальністю вищого рівня, а не лише функцією IT…

У Південній Африці впровадження Кодексу ISPS через Правила торгового судноплавства (морська безпека) виявляє значні структурні недоліки, оскільки внутрішня нормативно-правова база не визнає цифрову інфраструктуру як захищений об'єкт безпеки і не вимагає залучення спеціалізованих кіберфахівців до оцінки ризиків. Ця прогалина в законодавстві ускладнюється роздвоєною моделлю управління, в якій відповідальність за нагляд за кібербезпекою чітко не розподілена, а зобов'язання щодо обміну інформацією не передбачають обов'язкового механізму повідомлення про кіберінциденти… Для усунення цих вразливостей та підтримки програми прискореної модернізації портів Південної Африки необхідні цілеспрямовані реформи на трьох рівнях: внесення змін до нормативних актів з метою чіткого визнання цифрових активів та стандартів навчання, створення механізму координації кібербезпеки в морському секторі або спеціалізованої групи CSIRT, а також включення нагляду за кібербезпекою до структури виконавчих органів портових адміністрацій. Зрештою, у міру поступової цифровізації портових екосистем, глобальна морська спільнота більше не може покладатися на інтерпретаційні розширення застарілих інструментів безпеки;

натомість для забезпечення безперервності міжнародної торгівлі необхідні чіткі, гармонізовані та обов'язкові до виконання регуляторні зобов'язання». ***(From physical security to cyber resilience: Reassessing the ISPS code and port governance in South Africa // Clyde & Co LLP (https://www.clydeco.com/en/insights/2026/02/from-physical-security-to-cyber-resilience-reassis). 24.02.2026).***

***

«…Нове дослідження з щорічного звіту Darktrace про загрози на 2026 рік виявляє фундаментальні зміни в ландшафті кіберзагроз, оскільки хакери все частіше відмовляються від традиційних програмних експлойтів на користь компрометації ідентичності та зловживання обліковими даними. Ця тенденція найбільш виражена в Америці, де майже 70% інцидентів зараз починаються з викрадених або зловживаних облікових записів, що дозволяє зловмисникам «увійти» в систему, а не «зламати» її. Зловживаючи довіреними з'єднаннями в хмарних системах, додатках SaaS та ланцюгах постачання, кіберзлочинці можуть діяти відкрито, використовуючи законні дозволи, про що свідчать гучні випадки порушення безпеки в таких організаціях, як JLR, Marks & Spencer та Salesforce. У звіті підкреслюється зростаюча увага до цілей з високою вартістю, зазначаючи, що понад 8,2 мільйона фішингових електронних листів — більше чверті всієї фішингової активності в 2025 році — були спрямовані саме на VIP-персон…

В Європі хмарні та електронні поштові акаунти стали основними точками входу, на які припадає 58% інцидентів, випередивши традиційні порушення мережевої безпеки. Ці атаки, спрямовані на ідентифікацію, часто переростають у складні подвійні або потрійні кампанії з вимагання. Ця зміна супроводжується зростанням фішингу за допомогою штучного інтелекту, що призвело до значного збільшення нових технік соціального інжинірингу та довгих і складних повідомлень. Крім того, фішинг за допомогою QR-кодів зріс на 28%, причому зловмисники використовують такі передові методи, як «сплішинг» (розподіл QR-коду на два зображення) і «вкладання» (вбудовування шкідливих кодів у легітимні), щоб обійти традиційні інструменти сканування посилань. Щоб протидіяти цим адаптивним загрозам, експерти з безпеки наголошують на необхідності переходу від статичного контролю периметра до поведінкової безпеки, яка розуміє контекст і наміри, що дозволяє виявляти найменші аномалії в законній діяльності облікового запису». ***(Tom Quinn. 70% of Cyber-attacks Begin With Logins, Not Break-Ins // DIGIT (https://www.digit.fyi/70-of-cyber-attacks-begin-with-logins-not-break-ins/). 27.02.2026).***

***

«Кіберризики в роздрібній торгівлі перетворилися з вузької проблеми IT на системну проблему ланцюга поставок, але багато роздрібних торговців все ще думають занадто обмежено. Кібератаки 2025 року на M&S, Co-op і Harrods підкреслили цю зміну: те, що спочатку виглядало як збій IT, швидко перетворилося на відключення офлайн-систем, порушення платежів, порожні полиці і, у випадку M&S, очікуваний збиток у розмірі 300 млн фунтів стерлінгів від операційного прибутку. Як стверджує партнер TLT Ед Хейс, роздрібні торговці часто не можуть

відобразити всі цифрові «точки входу» у свій бізнес, оскільки нетехнічні команди регулярно підписують контракти на нові платформи з низькою вартістю без кіберзахисту, тихо створюючи інтеграції в основні системи… З часом ці невеликі, часто малодосвідчені постачальники стають «прихованими воротами» для зловмисників, як це було видно під час атаки на американського постачальника програмного забезпечення Blue Yonder, яка поширилася на декількох роздрібних продавців, таких як Starbucks. Ще більш підступними є компрометації надійних IT-постачальників, коли шкідливе програмне забезпечення поширюється через звичайні оновлення, що робить справжню «наскрізну видимість» нереальною.

У таких умовах «достатня» безпека означає жорсткі периметри, мінімальний доступ, відсутність підключень сторонніх осіб без офіційного схвалення IT-відділу та припущення, що постачальники рано чи пізно зазнають невдачі, тому необхідні ручні обхідні шляхи, надмірність, вторинні постачальники та системи резервного копіювання. Однак ці заходи суперечать тиску з боку витрат та культурі керівництва, яке все ще розглядає IT як центр витрат, а заходи безпеки — як перешкоду: фінансові директори не хочуть платити за потужності, які «можуть ніколи не бути використані», користувачі не сприймають багатофакторну автентифікацію, а багато організацій задовольняються «паперовою відповідністю» стандартам, таким як PCI DSS або ISO 27001, рідко використовуючи права на аудит або тестуючи плани відновлення в реальних умовах. Реальний вплив кіберінцидентів на бізнес — чи то порожні полиці, про які широко повідомляють соціальні мережі, чи то витік конфіденційних даних клієнтів або дітей, чи то просто «фактор роздратування» від паралізованої логістики, як у випадку з втратами Maersk від NotPetya — стає повністю зрозумілим лише після того, як щось зламається…

Хейс скептично ставиться до того, що нові закони, такі як британський законопроект про кібербезпеку та стійкість, самі по собі змінять поведінку, коли старі норми вже давно не виконуються. Натомість він очікує, що зміни будуть стимулювати заохочення та тиск з боку ланцюга поставок: великі роздрібні мережі вже посилюють договірні вимоги, що, ймовірно, змусить дрібніші агентства об'єднуватися, оскільки дотримання вимог буде для них занадто дорогим... Хейс наполягає, що штучний інтелект повинен доповнювати, а не замінювати людське судження. Якби він створював роздрібну компанію з нуля, жоден постачальник не отримав би доступ до системи без кіберзатвердження, кількість постачальників була б жорстко скорочена, права на аудит активно використовувалися б, а стійкість ретельно відпрацьовувалася б, а не вважалася само собою зрозумілою...» ***(Yasmeen Louis. Not just an IT problem: What are retailers still getting wrong about supply chain cyber security? // Retail Gazette (https://www.retailgazette.co.uk/blog/2026/02/retail-cyber-security/). 26.02.2026).***

***

«Світова морська галузь наразі стикається з нестабільною та швидкозмінною ситуацією у сфері кіберзагроз, де гіперпідключеність, необхідна для інтелектуальних суден, фактично подвоїла площу атаки на цей сектор. У 2025 році кількість кіберінцидентів у морській галузі зросла на 103%

порівняно з попереднім роком, а основними загрозами для безпеки на морі стали програми-вимагачі, DDoS-атаки та зараження шкідливим програмним забезпеченням. Ця криза розгортається в різних регіонах з різною динамікою: на Близькому Сході часто використовується підробка GPS-сигналів, щоб створити привід для захоплення суден; в Азії «кіберпірати» зламують мережі судноплавства, щоб провести розвідку для точних ударів по цінних вантажах; а в Європі військові електронні перешкоди зробили відключення GPS щоденною причиною аварій у Балтійському та Чорному морях. Крім того, великі глобальні транспортні вузли, такі як Роттердам і Лос-Анджелес, стали головними цілями для програм-вимагачів, оскільки паралізація операційної системи одного терміналу може спричинити затор, який дестабілізує весь глобальний ланцюг поставок…

Еволюція цих атак відбувається за двома основними напрямками: прямі спроби захопити фізичний контроль над суднами та атаки на ланцюги постачання, спрямовані на паралізацію більш широкої морської екосистеми. Прямі атаки на судна часто використовують вразливості систем супутникового зв'язку (VSAT) — як це було в 2025 році під час атаки Lab Dookhtegan, яка паралізувала 180 суден, — або використовують підробку GPS/GNSS, щоб навмисно змусити судна зіткнутися або сісти на мілину, як це було в інциденті з MSC Antonia в Червоному морі. Ще більш смертоносними є прямі атаки на системи операційних технологій (OT); наприклад, встановлення трояна віддаленого доступу на поромі Fantastic за допомогою USB-накопичувача, зараженого шкідливим програмним забезпеченням, продемонструвало, як застарілі операційні системи та погана сегментація мережі можуть дозволити зловмисникам дистанційно захопити ключові інженерні системи та дані карт ECDIS, що призведе до повної втрати контролю над судном…

Одночасно атаки на ланцюги поставок націлені на основи галузі, де державні групи та злочинні організації, такі як RansomHub, компрометують субпідрядників, щоб викрасти секрети морського проектування або креслення з верфей. Крім окремих верфей, атаки програм-вимагачів на операційні системи терміналів (TOS) виявилися здатними зупинити контейнерні операції на цілих континентах, викликавши глобальний економічний хаос через стрибки цін на нафту та інфляцію. Парадоксально, але перехід до автономної навігації та дистанційного обслуговування перетворив «надійні» сервери оновлення програмного забезпечення та інструменти управління на небезпечні вектори атак, де одне порушення може одночасно розповсюдити шкідливий код на десятки тисяч суден. У міру поглиблення інтеграції супутникового зв'язку та систем OT морські кіберзагрози переходять від простої крадіжки даних до руйнівних втручань, що спричиняють катастрофічні фізичні та економічні наслідки». ***(Maritime cyber incidents jumped 103% in 2025 // safety4sea (https://safety4sea.com/maritime-cyber-incidents-jumped-103-in-2025/). 24.02.2026).***

***

«Звіт Upstream Security «Глобальна кібербезпека в автомобільній галузі та галузі інтелектуальної мобільності в 2026 році», в якому проаналізовано 494 публічно повідомлені інциденти в 2025 році, виявляє структурну зміну ризиків, а не безпосередню кризу споживання. Частка атак з використанням

програм-вимагачів подвоїлася до 44 % від загальної кількості інцидентів, при цьому 92 % атак було здійснено дистанційно, а 67 % було спрямовано на телематичні та хмарні системи, що підкреслює, що основною мішенню атак зараз є серверна інфраструктура, API та платформи дистанційного управління, а не фізичне втручання в роботу транспортних засобів…

Хоча абсолютна кількість інцидентів залишається незначною порівняно з глобальною автомобільною промисловістю, зростаюча концентрація на віддалених хмарних векторах викликає занепокоєння щодо масштабованості. Сучасні автомобілі та автопарки все більше покладаються на стандартизоване програмне забезпечення, хмарні сервіси та системи дистанційного управління, створюючи дуже однорідну поверхню для атак. Колишній глава Національного кібердиректорату Ізраїлю, Ігаль Унна, попереджає, що одна-єдина вразлива слабкість може швидко вплинути на мільйони автомобілів: «Це все однакові машини без захисту, з однаковою підключеністю. Це пандемія, яка тільки чекає на спалах»…

У звіті підкреслюється, що хоча поточні інциденти ще не призвели до системного збою, автомобільний сектор перебуває у перехідній фазі, коли швидка цифровізація, що стимулюється бездротовими оновленнями, панелями управління автопарком та підключеними послугами, випереджає рівень зрілості захисних заходів. Експерти наголошують, що серйозний інцидент, який спричинить фізичну шкоду або широкомасштабні порушення, може кардинально змінити увагу громадськості та регуляторних органів, подібно до того, як минулі трагедії трансформували авіаційну безпеку. З огляду на те, що зловмисники використовують штучний інтелект для прискорення розвідки та експлуатації, галузь стикається з дедалі більшим тиском щодо посилення стійкості до наступної ескалації». ***(Zachy Hennessey. “The automotive industry will eventually wake up to cyber attacks. It's a pandemic that's just waiting for an outbreak.” // CTech (https://www.calcalistech.com/ctechnews/article/rk5e4rdobx). 22.02.2026).***

***

Сполучені Штати Америки та Канада

«У відповідь на зростаючу загрозу кібератак, ФБР у Цинциннаті розпочало операцію «Winter SHIELD» — кампанію, що закликає громадян і підприємства застосовувати проактивний підхід до цифрової безпеки. Ініціатива передбачає 10-крокoвий посібник, детально описаний на веб-сайті ФБР, що охоплює такі основні питання, як оновлення програмного забезпечення та регулярне резервне копіювання даних. Основне повідомлення є чітким: кожен є потенційною мішенню, і кіберзлочини — це питання «коли», а не «чи»…

Операція «Winter SHIELD» («Зимовий щит») підкреслює, що ці кроки не є просто рекомендаціями, а є фундаментальними основами надійної кіберзахисту. Кампанія заохочує перехід від реактивної до проактивної кібербезпеки, підкреслюючи, що як окремі особи, так і організації відіграють вирішальну роль у стримуванні кіберзлочинців. Інформаційна кампанія ФБР поєднує технічні поради

з рекомендаціями щодо поведінки, спрямованими на формування культури пильності та стійкості. Озброюючи громадськість знаннями та практичними кроками, операція «Winter SHIELD» є стратегічним заходом, спрямованим на зміцнення цифрової оборони країни в епоху, коли кіберзагрози є постійними і все більш витонченими». ***(Trevor Wang. FBI Cincinnati Launches Operation Winter SHIELD to Strengthen Cybersecurity Nationwide // SFist LLC (https://hoodline.com/2026/02/fbi-cincinnati-launches-operation-winter-shield-to-strengthen-cybersecurity-nationwide/). 04.02.2026).***

***

«…Новий законопроект у Конгресі США пропонує дозволити президенту Дональду Трампу уповноважувати приватні американські компанії з кібербезпеки переслідувати кіберзлочинців у всьому світі, відроджуючи історичну концепцію «каперських листів і репресалій». Традиційно ці листи використовувалися для надання приватним кораблям права атакувати ворожі судна під час війни, а тепер вони надаватимуть приватним фірмам повноваження переслідувати іноземні кіберзлочинні підприємства, особливо шахрайські ферми в Південно-Східній Азії, які використовують примусову працю для обману американців…

Законопроект, поданий представником Девідом Швейкертом, визначає масштабні шахрайські дії, спрямовані проти американців, як «акт війни» і має на меті надати США більші можливості кіберзахисту за менших витрат. Прихильники порівнюють цей підхід із програмами винагороди за виявлення вразливостей, стверджуючи, що він допоможе виявляти та припиняти злочинні операції, які щороку приносять мільярдні збитки вразливим американцям. Законопроект дозволить виконавчій владі видавати цільові доручення приватним компаніям, що потенційно вирівняє умови для менших кібербезпекових фірм у конкуренції за державні контракти.

Однак критики попереджають, що делегування приватним компаніям повноважень міжнародних правоохоронних органів у сфері кібербезпеки може спровокувати негативну реакцію інших країн, які стурбовані порушенням суверенітету та ризиком зловмисних дій. Прихильники заперечують, що законопроект містить регуляторні запобіжні заходи для запобігання зловживанням і що загроза кіберзлочинності зростає надто швидко, щоб традиційні зусилля уряду могли встигати за нею. Дебати точаться навколо того, чи є приватизація кіберзахисту сміливим і необхідним кроком, чи ризикованим заходом, який може ускладнити міжнародні відносини та нагляд…» ***(Cody Combs. Modern-day privateers: Could the US soon allow private companies to wage its cyber wars? // The National (https://www.thenationalnews.com/future/technology/2026/02/02/cybercrime-bill-marque-reprisal-warfare/). 02.02.2026).***

***

«Національний директор з кібербезпеки Шон Кернкросс закликав лідерів галузі співпрацювати з адміністрацією Трампа, щоб допомогти зменшити регуляторне навантаження в сфері кібербезпеки та підтримати

ключове законодавство з кібербезпеки в Конгресі. Виступаючи на заході Ради з інформаційних технологій, Кернкросс підкреслив бажання адміністрації співпрацювати з галуззю, а не нав'язувати правила зверху вниз, протиставляючи цей підхід прагненню попередньої адміністрації до посилення регулювання кібербезпеки в приватному секторі…

Кернкросс спеціально закликав представників галузі виступити за продовження дії Закону про обмін інформацією з питань кібербезпеки 2015 року, який забезпечує правовий захист компаніям, що обмінюються даними про кіберзагрози, але нещодавно втратив чинність і продовжувався лише на короткий термін. Адміністрація хоче продовжити дію закону на 10 років і вважає, що голос представників галузі має вирішальне значення для переконання Конгресу в необхідності вжити відповідних заходів.

Він закликав представників галузі надавати відгуки щодо проблемних питань у сфері регулювання та процесів обміну інформацією, пообіцявши, що адміністрація вислухає їх і докладе зусиль для вирішення цих питань. Кернкросс також наголосив на майбутній стратегії адміністрації у сфері кібербезпеки, зазначивши, що участь галузі відіграла ключову роль у її розробці. На завершення він запросив до постійного діалогу, підкресливши, що адміністрація прагне співпрацювати з галуззю для зміцнення національної кібербезпеки…» ***(Tim Starks. Sean Cairncross' cybersecurity agenda: less regulation, more cooperation // cyberscoop (https://cyberscoop.com/sean-cairncross-industry-cut-cybersecurity-regulations-renew-cisa/). 03.02.2026).***

***

«З початком 2026 року урядові підрядники стикаються з швидко мінливою ситуацією в галузі кібербезпеки, яка формується під впливом важливих регуляторних подій та посилення федерального контролю у 2025 році. Найбільш значущим досягненням стало завершення розробки Сертифікації моделі зрілості кібербезпеки (CMMC) 2.0, яка робить дотримання CMMC обов'язковим, підлягаючим аудиту та безпосередньо пов'язаним з правом на укладення контрактів. Нові положення Додатку до Федеральних правил оборонних закупівель (DFARS) тепер вимагають певних рівнів CMMC для укладення контрактів, а їх поетапне впровадження триватиме до кінця 2020-х років…

Ініціатива Міністерства юстиції США щодо боротьби з кібершахрайством (CCFI) також посилилася: у 2025 році було укладено дев'ять угод за Законом про неправдиві заяви (FCA), пов'язаних з кібербезпекою, на загальну суму 52 мільйони доларів. Міністерство юстиції зосередилося на неправдивих заявах щодо заходів контролю кібербезпеки, неповному впровадженні заходів захисту та нерозкритті відомих прогалин. Примітно, що заходи з забезпечення дотримання законодавства поширилися на приватні інвестиційні компанії та окремих менеджерів, підкресливши, що дотримання вимог кібербезпеки є тепер критично важливим обов'язком підрядників, який підлягає примусовому виконанню.

Модернізація хмарної безпеки просунулася вперед із впровадженням FedRAMP 20x, спрямованого на оптимізацію хмарних авторизацій за рахунок підвищення рівня автоматизації та співпраці. Ініціатива, яка реалізується поетапно,

обіцяє пришвидшення процесу затвердження та підвищення ефективності безперервного моніторингу, а її повне впровадження очікується до 2027 року.

Виконавчі дії адміністрації Трампа ще більше сформували ситуацію, включаючи наказ від червня 2025 року, що підтверджує федеральні пріоритети в галузі кібербезпеки, та нові меморандуми Управління з питань управління та бюджету (OMB) щодо використання та придбання штучного інтелекту (ШІ)…

На розгляді перебуває кілька справ, пов'язаних з Федеральним регламентом закупівель (FAR) та DFARS, які стосуються таких питань, як повідомлення про кіберзагрози, стандартизація вимог до кібербезпеки, безпека програмного забезпечення ланцюгів постачання та контрольована некласифікована інформація (CUI). Також триває оновлення положень DFARS, включаючи правила захисту захищеної оборонної інформації та впровадження вимог оцінки NIST SP 800-171…

У перспективі підрядники повинні залишатися проактивними та поінформованими, щоб управляти ризиками та зберігати право на участь у федеральних контрактах. Прихильність федерального уряду до безпеки даних та боротьби з кіберзагрозами є очевидною, і розуміння цих змін у законодавстві є необхідним для дотримання вимог та отримання конкурентних переваг на федеральному ринку». ***(Townsend L. Bourne, Nikole Snyder, Sidney Howe. What a Year! Cybersecurity Recap and 2026 Forecast for Government Contractors // Sheppard (https://www.sheppard.com/insights/blogs/what-a-year-cybersecurity-recap-and-2026-forecast-for-government-contractors). 03.02.2026).***

***

«5 січня 2026 року Адміністрація загальних служб (GSA) опублікувала оновлений посібник з політики для підрядників щодо захисту контрольованої некласифікованої інформації (CUI), що стало першим оновленням з 2022 року. Новий посібник GSA CUI відповідає останнім федеральним нормам, включаючи програму CMMC Міністерства оборони, і сигналізує про посилення контролю та офіційних вимог до оцінки підрядників, які працюють з CUI за контрактами цивільних агентств…

Основні моменти оновленого посібника включають:

Застосовність: Посібник широко застосовується до будь-якого підрядника, який зберігає CUI у своїх системах відповідно до контракту GSA. Однак він стає обов'язковим лише в тому випадку, якщо на нього конкретно посилаються в тендерах або контрактах, що вимагає координації та затвердження з боку головного спеціаліста з інформаційної безпеки (CISO) GSA.

Вимоги до безпеки: Посібник оновлює базові вимоги до контролю безпеки з NIST SP 800-171 Ревізія 2 до Ревізії 3, що робить GSA першою великою агенцією, яка вимагає дотримання нового стандарту. Підрядники повинні проактивно переглянути та спланувати впровадження Ревізії 3, навіть якщо деякі з них все ще повинні дотримуватися Ревізії 2…

Оцінка третьої сторони: Підрядники повинні пройти незалежну оцінку третьої сторони на відповідність вимогам, аналогічну FedRAMP та вищим рівням CMMC. Оцінювачі повинні бути акредитовані FedRAMP або затверджені GSA OCISO.

Вимоги «Showstopper»: У Посібнику перелічено критичні заходи безпеки, які, якщо не будуть належним чином впроваджені, автоматично унеможливлять затвердження системи…

План дій та етапи (POA&M): Підрядники можуть використовувати POA&M для виконання невиконаних вимог безпеки, але на відміну від CMMC, у Посібнику не вказано термін закриття для некритичних засобів контролю.

GSA як рецензент: Підрядники повинні подати комплексний пакет документів на затвердження, включаючи звіти про оцінку та супровідні документи, до команди безпеки GSA для розгляду та затвердження CISO, що є процесом, більш суворим, ніж CMMC, і схожим на FedRAMP…

Постійний моніторинг: підрядники повинні щоквартально, щорічно та раз на три роки подавати результати роботи, такі як сканування вразливостей, оновлені плани безпеки та тести на проникнення, щоб забезпечити відповідність вимогам.

Повідомлення про інциденти: про всі інциденти, що впливають на конфіденційність, цілісність або доступність, необхідно повідомляти протягом години, відповідно до процедур FedRAMP…

Переглянутий посібник GSA CUI підкреслює прихильність федерального уряду до суворого, стандартизованого дотримання вимог кібербезпеки підрядниками. Компанії, що працюють з CUI за контрактами GSA, повинні звертати увагу на ці вимоги в нових тендерах і почати переглядати та впроваджувати заходи контролю NIST SP 800-171 Revision 3. У міру посилення федерального контролю за кібербезпекою підрядників розуміння та дотримання специфічних для агентства практик безпеки даних буде мати вирішальне значення для збереження права на укладення контрактів та управління ризиками». ***(Townsend L. Bourne, Nikole Snyder, Sidney Howe. GSA Signals Enhanced Focus on Contractor Cybersecurity Practices: What You Need to Know About GSA's New CUI Guide // Sheppard (https://www.sheppard.com/insights/blogs/gsa-signals-enhanced-focus-on-contractor-cybersecurity-practices-what-you-need-to-know-about-gsas-new-cui-guide). 06.02.2026).***

***

«Нові правила кібербезпеки США в рамках програми сертифікації зрілості кібербезпеки (CMMC) Міністерства оборони змушують невеликих постачальників оборонної продукції переглянути свою участь через високі витрати на дотримання вимог та оперативну невизначеність. Впроваджена для захисту контрольованої несекретної інформації, ця система вимагає від підрядників проходження самооцінки, а незабаром і більш суворих аудитів. Однак тривалі затримки з проведенням аудитів, нечіткі визначення захищеної інформації та плутанина з впровадженням зробили дотримання вимог обтяжливим, особливо для малих підприємств, які становлять 88% ланцюга поставок в аерокосмічній галузі… Багато постачальників стикаються з витратами в сотні тисяч доларів, що змушує деяких з них розглядати можливість повного виходу з ринку оборонної промисловості, що може призвести до ослаблення промислової бази. Лідери галузі попереджають, що зменшення конкуренції серед дрібних постачальників може посилити виробничі проблеми, а міжнародні компанії стикаються з додатковими

ускладненнями через суперечливі глобальні закони про захист даних. Незважаючи на тиск з боку уряду з метою збільшення обсягів виробництва в оборонній галузі та диверсифікації постачальників, додаткові витрати на дотримання вимог можуть підірвати стійкість ланцюгів поставок». ***(Allison Lampert and Mike Stone. New cybersecurity rules for US defense industry create barrier for some small suppliers // Reuters (https://www.reuters.com/business/aerospace-defense/new-cybersecurity-rules-us-defense-industry-create-barrier-for-some-small-2026-02-20/). 20.02.2026).***

***

«Уряд США все частіше використовує Закон про неправдиві заяви (FCA) для боротьби з шахрайством у сфері кібербезпеки, про що свідчить рекордний обсяг відшкодувань за FCA у розмірі 6,8 млрд доларів за 2025 фінансовий рік, з яких 52 млн доларів припадає на угоди, пов'язані з кібербезпекою. З моменту запуску Ініціативи щодо цивільного кібершахрайства в 2021 році Міністерство юстиції (DOJ) посилило увагу до федеральних підрядників та отримувачів грантів, які неправдиво заявляють про дотримання стандартів кібербезпеки…

Заступник помічника генерального прокурора Бренна Дженні підкреслила, що це правозастосування надає пріоритет відповідальності за обманні дії, а не покаранню жертв порушень, підкреслюючи необхідність для організацій узгодити свої фактичні заходи безпеки з заявленою відповідністю. У зв'язку зі збільшенням кількості позовів від інформаторів (qui tam) Міністерство юстиції закликає компанії створити надійні структури управління, перевірити свої заходи контролю та підтримувати чіткі внутрішні канали повідомлення про порушення, щоб проактивно усувати потенційні прогалини. Для зменшення ризиків організації повинні сформувати міжфункціональні команди, які будуть займатися постійною оцінкою, розумінням вимог дотримання нормативних вимог та скоординованим реагуванням на інциденти…» ***(Ji Won Kim. The DOJ's civil cyber-fraud initiative lives on: Insights from cybersecurity enforcement through the False Claims Act // Norton Rose Fulbright (https://www.dataprotectionreport.com/2026/02/the-dojs-civil-cyber-fraud-initiative-lives-on-insights-from-cybersecurity-enforcement-through-the-false-claims-act/). 11.02.2026).***

***

«Міністерство війни США визнало компанію Anthropic, що займається розробкою штучного інтелекту, загрозою національній безпеці в ланцюжку поставок. Міністр оборони Піт Хегсет оголосив, що федеральний уряд припинить використання її технологій, дотримуючись публічної вимоги президента Дональда Трампа. Цей драматичний розрив став наслідком протистояння щодо контракту на суму 200 мільйонів доларів, підписаного в липні, в якому Anthropic вимагала письмових гарантій, що її моделі штучного інтелекту не будуть використовуватися для повністю автономної зброї або масового внутрішнього спостереження за американцями — обмеження, яким Пентагон «рішуче опирався». Коли встановлений Пентагоном термін, протягом якого Anthropic мала погодитися на необмежене використання військовими «всіх законних цілей», минув без укладення

угоди, Хегсет оголосив, що відносини компанії з федеральним урядом «назавжди змінилися»…

Директива Хегсета, опублікована на X, також має на меті заборонити будь-яким військовим підрядникам, постачальникам або партнерам вести комерційну діяльність з Anthropic, що компанія назвала «юридично необґрунтованим» і «небезпечним прецедентом». У своїй відповіді Anthropic заявила, що намагалася вести переговори в дусі доброї волі, підтримує законне використання в цілях національної безпеки і оскаржить «безпрецедентне» рішення в суді. Компанія стверджує, що міністр оборони не має законних повноважень (посилаючись на 10 USC 3252) поширювати заборону за межі контрактів Міністерства оборони, і запевнила своїх індивідуальних та комерційних клієнтів, що доступ до її продуктів, включаючи модель штучного інтелекту Claude, залишається незмінним. Крок адміністрації Трампа був охарактеризований як захоплення влади і, як очікується, матиме далекосяжні негативні наслідки для американської галузі штучного інтелекту, що потенційно змусить таких великих інвесторів, як Nvidia, Amazon і Google, відмовитися від інвестицій в Anthropic». ***(Jai Hamid. US Pentagon designates Anthropic a supply chain risk to national security – What's really going on? // Cryptopolitan (https://www.cryptopolitan.com/us-pentagon-anthropic-national-security/). 28.02.2026).***

***

«Массіллон оновлює свою програму кібербезпеки відповідно до нових стандартів штату Огайо, які вимагають від місцевих органів влади прийняття офіційної політики в галузі кібербезпеки. Міська рада розглянула 19-сторінкову пропозицію, спрямовану на захист даних споживачів, фінансових записів, інтелектуальної власності та інших критично важливих активів, і незабаром очікується голосування. Оновлення є результатом нещодавнього перегляду політики, проведеного разом із постачальником програмного забезпечення міста, компанією Talix, і доповнює щорічне навчання з кібербезпеки, яке вже є обов'язковим для співробітників… Згідно з новим законом штату, муніципалітети повинні визначити критично важливі функції, оцінити ризики кібербезпеки, створити плани відновлення інфраструктури у разі збою та дотримуватися обов'язкової процедури повідомлення про інциденти, пов'язані з кібербезпекою або програмним забезпеченням-вимагачем, включаючи повідомлення Департаменту громадської безпеки штату Огайо та державного аудитора. У пропонованій політиці Массіллона також чітко зазначено, що місто не буде виконувати вимоги про виплату викупу». ***(Massillon cybersecurity plan aims to protect consumer data, records // Gannett Co., Inc. (https://www.indeonline.com/story/news/local/2026/02/23/massillon-council-considers-cybersecurity-measures-to-safeguard-data/88821193007/). 23.02.2026).***

***

«У звіті про дотримання вимог за 2026 рік Канадська організація з регулювання інвестицій (CIRO) закликає дилерів посилити кібербезпеку, посилити нагляд та забезпечити точність реєстрації. Кіберризик залишається

«ключовим бізнес-ризиком» після власного порушення CIRO, спричиненого фішингом, у серпні минулого року, і регулятор проведе навчальні вправи з кібербезпеки в 2026 році, щоб поділитися отриманим досвідом. Компаніям рекомендується забезпечувати постійне навчання персоналу та впроваджувати багатофакторну автентифікацію, оскільки співробітники часто є найслабшою ланкою. У міру впровадження дилерами інструментів штучного інтелекту CIRO буде перевіряти відповідні операційні заходи контролю під час перевірок відповідності…

Окрім технологічних аспектів, у звіті висвітлюються недоліки, виявлені під час нещодавніх перевірок, спрямованих на реформування клієнтоорієнтованих процесів (CFR): політика повинна бути індивідуальною, детальною та реалістичною, а не просто повторювати правила. Дилери повинні покращити нагляд за зовнішньою діловою діяльністю, контролювати несанкціоновані канали комунікації та посилити розкриття інформації про конфлікти інтересів. Помилки в реєстрації, такі як неправильні юридичні назви у формі 33-109F4, продовжують спричиняти затримки. Нарешті, CIRO просуває гармонізовану систему безперервної освіти, а поправки до другої фази очікуються в найближчі місяці…» ***(CIRO addresses cybersecurity, AI, CFR gaps and more // Newcom Media Inc. (https://www.investmentexecutive.com/news/ciro-addresses-cybersecurity-ai-cfr-gaps-and-more/). 17.02.2026).***

***

«Агентство з кібербезпеки та безпеки інфраструктури США (CISA) перебуває, за повідомленнями, у скрутному становищі, а законодавці з обох партій та лідери галузі попереджають, що його здатність виконувати свою основну місію значно знизилася, і воно не готове до кризи. Згідно з розслідуванням Cyberscoop, CISA втратила приблизно третину свого персоналу протягом першого року адміністрації Трампа, що змусило її скоротити ключові програми, такі як ініціатива проти викрадення даних та заходи щодо забезпечення безпеки розробки програмного забезпечення. Ці втрати персоналу, серед яких є кілька членів команди агентства з безпеки виборів, ускладнюються переведенням сотень інших співробітників CISA для підтримки заходів адміністрації щодо боротьби з імміграцією…

Джерела пов'язують цей спад з сукупністю факторів, серед яких скорочення бюджету, триваюче часткове припинення роботи уряду, що почалося 14 лютого, та відсутність постійного директора з моменту вступу Трампа на посаду. Наразі CISA працює з приблизно 38% штату, що ще більше ускладнює її функціонування. Дехто звинувачує в цьому адміністрацію Трампа та Конгрес, інші вказують на проблеми з керівництвом, пов'язані з виконуючим обов'язки директора Мадху Готтумуккалою. У відповідь Готтумуккала заявив, що, незважаючи на виклики, CISA залишається непохитною у своєму прагненні захищати федеральні мережі від зловмисних кіберзагроз». ***(Zack Whittaker. US cybersecurity agency CISA reportedly in dire shape amid Trump cuts and layoffs // TechCrunch Media LLC. (https://techcrunch.com/2026/02/25/us-cybersecurity-agency-cisa-reportedly-in-dire-shape-amid-trump-cuts-and-layoffs/). 25.02.2026).***

***

«Агентство з кібербезпеки та безпеки інфраструктури (CISA) стикається з постійною невизначеністю щодо керівництва після переведення його виконуючого обов'язки директора Мадху Готтумуккала на нову посаду «директора зі стратегічної реалізації» Міністерства внутрішньої безпеки США. Нестабільний термін повноважень Готтумуккала ознаменувався хвилею звільнень співробітників, ретельним розслідуванням Конгресу щодо повідомлень про те, що він не пройшов тест на поліграфі та неправильно поводився з конфіденційними документами, а також закриттям уряду, в результаті якого дві третини співробітників CISA були відправлені у відпустку. Деякі критикували його стиль керівництва як неефективний і невідповідний місії агентства…

Нік Андерсен, виконуючий обов'язки заступника директора CISA з питань кібербезпеки, тепер буде виконувати обов'язки директора CISA. Нинішні та колишні чиновники сподіваються, що Андерсен, який обіймав високі посади в сфері кібербезпеки в першій адміністрації Трампа, зможе стабілізувати роботу агентства в умовах значного тиску, спричиненого зміною керівництва, закриттям уряду та геополітичною напруженістю, яка може спровокувати заходи відплати проти інфраструктури США…

Тривала відсутність затвердженого Сенатом директора CISA посилює ці виклики, оскільки агентство в значній мірі покладається на партнерські відносини для очолювання кіберзахисту країни на федеральному, штатному та місцевому рівнях, а також в організаціях критичної інфраструктури. Кандидат президента Дональда Трампа на цю посаду, Шон Планкі, користується широкою повагою, але його призначення затримується в Сенаті з причин, не пов'язаних з його кваліфікацією. Член Комітету з питань внутрішньої безпеки Палати представників Бенні Томпсон (демократ від штату Міссісіпі) висловив глибоку стурбованість станом CISA, зазначивши, що її персонал був «знекровлений», а її місія – ослаблена, і заявив, що з нетерпінням чекає на співпрацю з Андерсеном, щоб повернути агентство «на правильний шлях». ***(Justin Doubleday. CISA leadership shakeup comes amid 'pressure' moment for cyber agency // Hubbard Radio Washington DC, LLC (https://federalnewsnetwork.com/cybersecurity/2026/02/cisa-leadership-shakeup-comes-amid-pressure-moment-for-cyber-agency/). 27.02.2026).***

***

«Двопартійна група сенаторів наполягає на оновленні федеральних нормативних актів щодо кібербезпеки в галузі охорони здоров'я, а Комітет Сенату з питань охорони здоров'я, освіти, праці та пенсій проголосував 22 голосами проти 1 за просування Закону про кібербезпеку та стійкість у галузі охорони здоров'я. Законопроект, який тепер передається на розгляд Сенату в повному складі, має на меті посилити стійкість сектора шляхом опублікування рекомендацій з кібербезпеки для сільських медичних закладів та поліпшення координації між федеральними агентствами. Він також спрямований на впровадження затриманих оновлень до Правил безпеки HIPAA, які зобов'язують організації, що підпадають під дію HIPAA, застосовувати багатофакторну

автентифікацію, шифрування та проводити регулярні аудити, включаючи тестування на проникнення…

Законодавство враховує занепокоєння сектора охорони здоров'я щодо високої вартості впровадження пропонованих вимог HIPAA, пропонуючи гранти та навчання для практик з обмеженими ресурсами з метою поліпшення їхніх можливостей щодо запобігання кібератакам та реагування на них. Сенатор Марк Уорнер (Демократична партія, штат Вірджинія) підкреслив, що кібератаки на систему охорони здоров'я не тільки ставлять під загрозу дані, але й порушують надання медичної допомоги та ставлять під загрозу життя людей. Хоча доля більшості законодавчих актів Конгресу є невизначеною, експерти з питань політики вважають, що цей законопроект має розумні шанси на успіх, як окремий захід або як частина більш широкого пакету, з огляду на широке визнання необхідності посилення кібербезпеки в галузі охорони здоров'я в умовах нещодавніх масштабних атак. Якщо законопроект буде прийнятий, передбачається, що він помірно покращить стан безпеки організацій охорони здоров'я». ***(Marianne Kolbasuk McGee. Senate Health Cyber Bill Clears Committee Hurdle // Information Security Media Group, Corp. (https://www.govinfosecurity.com/senate-health-cyber-bill-clears-committee-hurdle-a-30880). 27.02.2026).***

***

Країни ЄС та Великобританія

«Під час нещодавніх дебатів у Європейському парламенті атака програм-вимагачів на Управління охорони здоров'я Ірландії (HSE) у 2021 році, яка коштувала державі понад 102 мільйони євро, була названа яскравим прикладом зростаючих кіберзагроз, з якими стикається критична цивільна та військова інфраструктура ЄС. Експерти та депутати Європейського парламенту на слуханнях Комітету з питань безпеки та оборони (SEDE) попередили, що Європа зараз стикається з систематичними гібридними операціями, в яких кібератаки на важливу інфраструктуру поєднуються з дезінформаційними кампаніями та політичним тиском…

Учасники дискусії, серед яких були Фердинанд Герінгер з FTI Consulting та директор Європейського центру компетенції з кібербезпеки Лука Тальяретті, наголосили, що загрози еволюціонували від поодиноких інцидентів до атак «змішаної реальності», посилаючись не тільки на хакерську атаку на HSE, а й на інциденти, що вплинули на інфраструктуру Великої Британії та Франції. Вони також висловили занепокоєння щодо вразливості морських вітрових електростанцій, дронів та розумних автомобілів, які можуть збирати конфіденційні дані та потенційно розкривати схеми руху транспорту навколо критично важливих об'єктів.

Пауліна Узнанська з відділу Китаю Центру східних досліджень порівняла розумні автомобілі зі «смартфонами на колесах», попередивши, що вони становлять значну загрозу для національної безпеки та критичної інфраструктури.

Вона закликала держави-члени ЄС вжити негайних заходів для захисту своїх доріг та об'єктів.

У відповідь Міністерство юстиції Ірландії зазначило, що тривають зусилля з посилення стандартів кібербезпеки для операторів вітрових електростанцій та усунення загроз від дронів і підключених до мережі транспортних засобів. Збройні сили також інвестують у системи протидії дронам для захисту великих заходів та критичної інфраструктури. Дебати підкреслили нагальну потребу у скоординованому підході ЄС до захисту від дедалі більш витончених і комплексних кіберзагроз…» ***(Neil Michael. MEPs discuss HSE ransomware attack during 'frightening' debate // Examiner Echo Group Limited (https://www.irishexaminer.com/news/politics/arid-41786618.html). 02.02.2026).***

***

«20 січня 2026 року Європейська комісія запропонувала новий комплексний пакет заходів з кібербезпеки, спрямований на посилення стійкості ЄС та його спроможності протистояти новим кіберзагрозам. Пакет включає зміни до Закону ЄС про кібербезпеку, Директиви NIS2 та Європейської системи сертифікації кібербезпеки (ECCF).

Основні зміни до Закону про кібербезпеку включають створення Рамки безпеки ланцюга постачання ІКТ для вирішення проблем безпеки в критичній інфраструктурі, спрощення та вдосконалення процесів сертифікації кібербезпеки, адміністративне спрощення для зменшення непотрібного навантаження відповідно до NIS2, а також посилення ролі ENISA, Агентства ЄС з кібербезпеки, з вимогою до держав-членів призначити по два офіцери зв'язку…

Запропоновані поправки до Директиви NIS2 уточнюють сферу застосування та визначення для таких секторів, як охорона здоров'я, електроенергетика, воднева енергетика та хімічна промисловість, а також встановлюють чіткі правила для виробників електроенергії потужністю понад 1 МВт. Малі підприємства середньої капіталізації будуть визначені як важливі суб'єкти, що зменшить навантаження на дотримання вимог, тоді як мікро- та малі постачальники послуг DNS будуть виключені. Пакет запроваджує максимальну гармонізацію управління ризиками та повідомлення про інциденти, підкріплену європейськими системами сертифікації, та класифікує постачальників європейських цифрових ідентифікаторів та бізнес-гаманців як важливі суб'єкти, на яких поширюються зобов'язання з кібербезпеки.

Комісія також розробить керівні принципи для гармонізації запитів щодо інформації про безпеку ланцюгів постачання та запровадить нові правила повідомлення про випадки використання програм-вимагачів, згідно з якими певні суб'єкти господарювання будуть зобов'язані повідомляти CSIRT та національним органам влади про деталі таких випадків, включаючи виплати викупу. ENISA буде підтримувати транскордонний аналіз ризиків та спільні наглядові заходи для суб'єктів господарювання, що здійснюють діяльність у декількох державах-членах.

Оновлений ECCF розширить свою сферу застосування, щоб охопити ІКТ-продукти, послуги, керовані послуги безпеки та загальний стан кібербезпеки, підтримуючи дотримання NIS2 та інших законів ЄС. Він запровадить чіткі терміни,

покращене управління та гармонізовані інструменти дотримання вимог, а ENISA буде відповідати за підтримку та розробку схем сертифікації…

Пакет буде представлений Європейському парламенту та Раді для затвердження. Після прийняття переглянутий Закон про кібербезпеку набуде чинності негайно, а держави-члени матимуть один рік для імплементації оновленої Директиви NIS2 у національне законодавство». ***(European Commission Announces New Cybersecurity Package // National Law Forum, LLC (https://natlawreview.com/article/european-commission-announces-new-cybersecurity-package). 03.02.2026).***

***

«Польща готова переглянути поправки до закону про Національну систему кібербезпеки на тлі зростаючого тиску з боку США з метою блокування участі китайських технологічних компаній, таких як Huawei і ZTE, у проектах з розвитку критичної цифрової інфраструктури. Законопроект, який чекає на підпис президента Кароля Навроцького, вважається одним з найважливіших законопроектів поточного парламентського терміну. Він розширить регулювання кібербезпеки на такі сектори, як управління ІКТ, стічні води, розподіл продуктів харчування, поштові послуги та хімічне виробництво, а також надасть владі повноваження призначати певні технологічні компанії «постачальниками високого ризику», фактично виключаючи їх з державних тендерів…

Експерти вважають, що цей крок може завадити китайським компаніям брати участь у розвитку цифрової інфраструктури Польщі. Посилення вимог до кібербезпеки пов'язане з тим, що в 2025 році в Польщі було зафіксовано 272 000 інцидентів, пов'язаних з кібербезпекою, що більш ніж удвічі перевищує показник попереднього року, що підкреслює необхідність зміцнення Національної мережі кібербезпеки.

Американські чиновники постійно висловлюють занепокоєння щодо китайських технологій у дискусіях із польськими колегами, закликаючи Польщу наслідувати приклад США і заборонити обладнання Huawei та ZTE у федеральних мережах. Тим часом Китай, як повідомляється, чинить власний тиск, натякаючи, що відновлення експорту польської птиці до Китаю може залежати від рішення президента щодо цього закону.

Президент Навроцький зараз стоїть перед стратегічним рішенням: приєднатися до Вашингтона і ризикнути економічними санкціями з боку Пекіна, або піти на поступки китайським інтересам і потенційно поступитися питаннями національної безпеки…» ***(Melike Pala. Poland weighs cybersecurity law amid US, China tech pressure // Anadolu Ajansı (https://www.aa.com.tr/en/europe/poland-weighs-cybersecurity-law-amid-us-china-tech-pressure/3821710#). 05.02.2026).***

***

«3 лютого 2026 року Комітет з питань публічних законопроектів Великої Британії розпочав розгляд законопроекту про кібербезпеку та стійкість (мережеві та інформаційні системи), який є значним оновленням британської

системи регулювання кібербезпеки з часу прийняття Регламенту NIS 2018 року. У зв'язку зі зростанням масштабів і складності кіберзагроз, законопроект спрямований на модернізацію підходу Великобританії до захисту критичної інфраструктури, посилення регуляторного нагляду та вдосконалення системи повідомлення про інциденти. Запропонований у листопаді 2025 року, законопроект є ключовою частиною більш широкої стратегії уряду щодо кіберстійкості і, як очікується, набуде чинності до кінця 2026 року…

Центральною особливістю законопроекту є розширення сфери регулювання, що включає нові суб'єкти до визначення «операторів основних послуг». До них тепер належать центри обробки даних, контролери великих навантажень (наприклад, ті, що керують інтелектуальними приладами та електромобілями), постачальники керованих послуг та постачальники, які мають вирішальне значення для надання основних послуг.

Законопроект також надає регуляторним органам розширені повноваження для створення більш передбачуваного та ефективного середовища дотримання вимог. Регуляторні органи зможуть вимагати більш частого повідомлення про інциденти, відшкодування витрат, обміну інформацією та накладати більш високі штрафи. Державний секретар отримує нові повноваження встановлювати стратегічні пріоритети для регуляторних органів, керувати діями в інтересах національної безпеки та оновлювати Регламент NIS за допомогою вторинного законодавства…

Вимоги щодо повідомлення про інциденти посилюються: обов'язкове первинне повідомлення про значні інциденти має надходити протягом 24 годин, а детальний звіт — протягом 72 годин, причому це прямо стосується і атак програм-вимагачів. Відповідальність за повідомлення клієнтів про інциденти перекладається безпосередньо на постачальників послуг…

Підприємства, які наразі підпадають під дію Регламенту NIS, повинні провести аналіз прогалин, щоб визначити нові зобов'язання, такі як переглянуті процедури повідомлення про інциденти та готовність до цілодобового інформування. Розширення сфери застосування означає, що деякі компанії, які раніше не підпадали під регулювання, тепер можуть бути включені, особливо як критично важливі постачальники, що вимагає від них перегляду контрактів, оновлення політики кібербезпеки та підготовки до взаємодії з регуляторними органами сектору.

Процес проходження законопроекту буде ретельно відстежуватися на шляху до отримання королівської згоди, оскільки він матиме значний вплив на підхід Великобританії до управління кіберризиками та захисту критичної інфраструктури». ***(Emma Thompson and Beverley Flynn. UK Cyber Security and Resilience Bill under scrutiny // Stevens & Bolton LLP (https://www.stevens-bolton.com/insights/102mgn2/uk-cyber-security-and-resilience-bill-under-scrutiny/). 04.02.2026).***

***

«Нормативно-правова база щодо штрафів за кіберзлочини в регіоні ЕМЕА різко розширилася, що робить страхування таких штрафів нагальною

проблемою для організацій. Згідно зі спільним звітом Aon та A&O Shearman, джерела кіберштрафів зростають, а правозастосування стає більш рішучим і багаторівневим. Нові закони та рамки, такі як Закон ЄС про цифрову операційну стійкість (DORA), Директива NIS2 та майбутній законопроект Великобританії про кібербезпеку та стійкість, посилюють тиск на компанії з метою досягнення більшої кіберстійкості…

З цими регуляторними змінами пов'язані більш високі штрафи та санкції для компаній, керівників та членів правління, які не забезпечують дотримання вимог. Однак питання про те, чи можна застрахувати кіберштрафи, залишається дуже специфічним для кожної юрисдикції. Багато країн обмежують або забороняють страхування кримінальних або адміністративних штрафів, а там, де страхування доступне, воно зазвичай обмежується тим, що «страхується згідно із законом», виключаючи умисні або грубі недбалість.

Негрошові санкції, такі як накази про припинення обробки даних, обов'язкові аудити, призупинення діяльності або анулювання ліцензій, також стають все більш поширеними і можуть бути настільки ж руйнівними, як і фінансові санкції. Зростає відповідальність керівництва, оскільки до ради директорів та вищого керівництва висуваються підвищені вимоги щодо нагляду, інвестицій та готовності до мінімізації кіберризиків.

У звіті підкреслюється, що в міру посилення правозастосування організації повинні розуміти правовий контекст та обмеження страхування в кожній юрисдикції. Проактивна співпраця між юридичними, ризиковими та страховими командами є необхідною для орієнтування в цьому складному та мінливому середовищі, управління ризиками та випередження змін у законодавстві…» ***(Charlie Weston Simons, Steven Hadwin, Laurie-Anne Ancenys, Dalila Korchane, Hippolyte Marquetty, Nicole Wolters Ruckert, Marleen Huisman. Insurability of cyber fines: Navigating a complex and evolving risk landscape // A&O Shearman (https://www.aoshearman.com/en/insights/insurability-of-cyber-fines-navigating-a-complex-and-evolving-risk-landscape). 04.02.2026).***

***

«Після проведення громадських консультацій уряд Великої Британії оприлюднив пропозиції щодо боротьби з ескалацією загрози від програм-вимагачів, які, як очікується, залишатимуться одним з головних кіберризиків до 2026 року через зростання кількості атак із використанням штучного інтелекту, програм-вимагачів як послуги та вразливості ланцюгів постачання… Уряд реалізує три ключові законодавчі заходи: (1) цільова заборона виплат викупу за програмне забезпечення-вимагач для органів державного сектору та операторів критичної національної інфраструктури (CNI), яка отримала значну підтримку (72%) і буде розвиватися далі щодо сфери застосування та екстериторіальності; (2) режим запобігання виплатам, який вимагає від усіх інших жертв повідомляти про інциденти владі перед здійсненням виплат, пропозиція, яка викликала неоднозначну реакцію, але буде реалізована з уточненням порогів для повідомлення; та (3) обов'язковий режим повідомлення про інциденти, який вимагає від усіх організацій повідомляти уряд про атаки протягом 72 годин, захід,

який підтримали 63% респондентів… Ці ініціативи, поряд із майбутнім законопроектом про кібербезпеку та стійкість, свідчать про зміну, в результаті якої реагування на кіберінциденти стає основним питанням управління та дотримання вимог, а не лише технічним питанням». ***(Curtis McCluskey. The UK's Ransomware Strategy: What the UK Government's Response Signals // Goodwin Procter LLP (https://www.goodwinlaw.com/en/insights/publications/2026/02/alerts-technology-dpc-the-uks-ransomware-strategy). 12.02.2026).***

***

«Місцеві органи влади стикаються з посиленням ризику кібератак, які можуть паралізувати роботу основних державних служб — від надання житлових субсидій до вивезення сміття — та поставити під загрозу конфіденційні дані громадян. Хоча майбутній британський законопроект про кібербезпеку та стійкість має на меті модернізувати системи захисту та запровадити більш суворі стандарти для ланцюгів постачання, місцеві ради можуть негайно посилити свою обороноздатність, вживши п'ять практичних заходів…

Застосовуйте постійний моніторинг третіх сторін: замість того, щоб покладатися на щорічні анкети, використовуйте автоматизовані інструменти для сканування всієї екосистеми постачальників (включаючи четверті сторони) на предмет вразливостей, прострочених сертифікатів та порушень у режимі реального часу.

Використовуйте інформацію про загрози: підпишіться на канали, такі як Служба раннього попередження NCSC (Національний центр кібербезпеки), щоб отримувати сповіщення про кампанії з використанням програм-вимагачів та шкідливого програмного забезпечення, характерні для певного сектору, та передавати ці показники безпосередньо в системи захисту…

Приєднуйтесь до регіональних кіберкластерів: співпрацюйте з групами, що підтримуються UKC3 (UK Cyber Cluster Collaboration), щоб обмінюватися даними про інциденти, координувати взаємодопомогу та отримувати доступ до талантів університетів, ефективно примножуючи обмежені ресурси.

Стандартизуйте звітність про інциденти: відійдіть від несистематичних ручних процесів, автоматизувавши робочі процеси та привівши їх у відповідність до структури реагування на кіберінциденти NCSC, щоб відповідати майбутнім, більш жорстким нормативним строкам.

Прийміть підхід «припустити порушення»: визнайте, що компрометація є неминучою, і зосередьтеся на постійній пильності, тестуванні та готовності, щоб мінімізувати вплив, коли захист врешті-решт буде обійдено…

Впроваджуючи ці практики вже зараз, ради можуть сформувати культуру стійкості, яка захищає критично важливі послуги незалежно від законодавчих термінів». ***(Renata Vincoletto. Five easy wins to strengthen cyber resilience in local government // techUK (https://www.techuk.org/resource/five-easy-wins-to-strengthen-cyber-resilience-in-local-government.html). 24.02.2026).***

***

«Уряд Великобританії розпочинає кампанію, спрямовану на впровадження малим та середнім бізнесом програми Cyber Essentials, після того як дослідження виявило, що половина малих та середніх підприємств зазнала кібератак протягом минулого року, а збитки від цих атак оцінюються в 14,7 млрд фунтів стерлінгів на рік (близько 0,5% ВВП), а середня вартість значних інцидентів становить майже 195 000 фунтів стерлінгів кожен. Незважаючи на широку обізнаність про фінансові ризики та ризики для репутації, а також зростання загроз, спричинене швидким розвитком технологій та штучного інтелекту, багато компаній залишаються вразливими і шукають рекомендацій та кіберстрахування…

Останнє довгострокове дослідження DSIT Cyber Security Longitudinal Survey підкреслює нагальність проблеми: 82% підприємств повідомили про ті чи інші форми кібератак протягом останнього року, а управління постачальниками залишається ключовою слабкою ланкою, оскільки видимість інцидентів у ланцюжку поставок є обмеженою. Паралельне дослідження, проведене консалтинговою компанією ISO Be Certified, свідчить про те, що побоювання щодо кібербезпеки також можуть гальмувати інновації: 42% з 700 керівників малих і середніх підприємств назвали це головним перешкодою для цифрової трансформації в 2026 році, хоча 55% все ще вважають цифровізацію пріоритетом для зростання (особливо в IT та фінансових послугах)…

Недостатній рівень кваліфікації та підготовки ускладнює ситуацію, оскільки багато респондентів зазначають, що їхнім працівникам бракує цифрових навичок для безпечного впровадження нових технологій. МСП просять про підтримку: 18 % хочуть отримати субсидії на навчання з цифрової трансформації, а 15 % шукають фінансування для найму персоналу, який би керував змінами. Cyber Essentials може допомогти задовольнити ці потреби завдяки структурованим рекомендаціям та безкоштовним підготовчим ресурсам (хоча сама оцінка є платною). Національний центр кібербезпеки наголошує, що зловмисники націлюються на слабкі місця, а не на розмір компанії, і закликає підприємства діяти негайно: замість того, щоб відкладати плани модернізації, малі та середні підприємства повинні інвестувати в навички та навчання, щоб безпечно впроваджувати нові технології, зберігаючи постійну пильність щодо нових загроз». ***(Katie Scott. SMEs urged by Government to "lock the door" against cybercriminals // Marketing VF Ltd (https://startups.co.uk/news/cyber-essentials-scheme/). 24.02.2026).***

***

«У зв'язку з щоденним зростанням кіберзагроз, статус Великобританії як цифрово розвиненої країни зробив її головним об'єктом для витоків даних і програм-вимагачів, що призвело до гострого дефіциту кваліфікованих фахівців і зробило кібербезпеку критично важливим пріоритетом для таких секторів, як фінанси, охорона здоров'я та державне управління. Цей дисбаланс між попитом і пропозицією відкриває перспективні кар'єрні можливості для тих, хто володіє відповідними знаннями… Щоб досягти успіху, кандидати повинні оволодіти конкретними технічними навичками, включаючи основи мережевих технологій (такі як TCP/IP та аналіз трафіку), програмування для автоматизації

(Python або Bash) та хмарну безпеку для таких платформ, як AWS та Azure. Роботодавці також надають пріоритет володінню навичками етичного хакерства, реагуванню на інциденти за допомогою інструментів SIEM, таких як Splunk, та здатності управляти ідентифікацією та доступом…

Однак теоретичних знань недостатньо; роботодавці активно шукають кандидатів, які можуть застосувати свої навички в реальних ситуаціях. Отже, структуровані програми навчання, що пропонують практичні лабораторні заняття та наставництво, такі як ті, що надаються edept, стають необхідними для подолання розриву між академічними концепціями та готовими до роботи знаннями. Ці програми дозволяють навіть тим, хто не має технічної підготовки, отримати практичний досвід, необхідний для вступу в цю галузь, як правило, протягом 6–12 місяців. Зрештою, поєднання безперервного навчання з практичним застосуванням дає змогу майбутнім фахівцям досягти довгострокової стабільності в високооплачуваній галузі, яка є життєво важливою для цифрової економіки Великої Британії». ***(Kapil Joshi. Which Skills Required for High-Demand Cyber Security Jobs in UK // Printline Media Pvt. Ltd. (https://theprint.in/brandit/which-skills-required-for-high-demand-cyber-security-jobs-in-uk/2858541/). 19.02.2026).***

***

«Оскільки економіка Литви, яка швидко переходить на цифрові технології, спирається на електронні підписи, цифрові медичні записи та централізовану електронну ідентифікацію, уряд запустив національну програму, координовану Агентством з інновацій Литви, щоб перетворити академічні дослідження на готові до виходу на ринок рішення в галузі кібербезпеки та зміцнити цифрову стійкість країни. Її флагманська місія «Безпечне та інклюзивне електронне суспільство» вартістю 24,1 млн євро, очолювана Каунаським технологічним університетом спільно з Вільнюським технологічним університетом, Університетом імені Миколи Ромеріса та такими компаніями, як NRD Cyber Security, Elsis PRO, Transcendent Group Baltics та BPTI (разом з Infobalt та національним центром компетенції з кіберзлочинності), пілотує інструменти в державних установах та критичній інфраструктурі: інтелектуальні будівлі, що самостійно навчаються, засоби захисту на основі штучного інтелекту від шахрайства у сфері фінансових технологій та порушення безпеки даних, датчики виявлення загроз для промислових об'єктів, управління гібридними загрозами для громадської безпеки та освіти, моделі штучного інтелекту для виявлення скоординованої дезінформації та автоматизовані платформи збору інформації про загрози…

Дослідники попереджають, що GenAI зруйнувала захист, заснований на шаблонах: LLM тепер створюють реалістичні, багатомовні, персоналізовані фішингові атаки в великих масштабах, а злочинці організовують мультимодальні набори — моделі класу GPT (та їхні клони, такі як FraudGPT), клонування голосу (ElevenLabs, VALL-E) та інструменти для створення дипфейків (StyleGAN, Stable Diffusion, DeepFaceLab, Wav2Lip) — для створення ідентичностей, відео «живості» та синтетичних KYC, з агентами ШІ, що автоматизують реєстрацію та відповіді на виклики; адаптивні кампанії навіть перемикають канали та використовують

клоновані голоси в режимі реального часу. Незважаючи на ці загрози, Литва просунулася в глобальних індексах (Індекс ефективного управління Чендлера (CGGI) 25-те місце; готовність уряду до штучного інтелекту 33-тє місце, 2025 рік), оновила свою стратегію штучного інтелекту на 2021–2030 роки, щоб надати пріоритет кіберзахисту на основі штучного інтелекту, і за допомогою Національного центру кібербезпеки (NKSC) зменшила кількість випадків використання програм-вимагачів у п'ять разів з 2023 по 2024 рік, поглиблюючи співпрацю з NATO, ENISA та партнерами з ЄС… Чиновники наголошують, що забезпечення надійного, інклюзивного цифрового суспільства зараз залежить від стабільної співпраці науки та бізнесу, захисту на основі штучного інтелекту та постійної освіти населення». ***(Safe and Inclusive E-Society: How Lithuania Is Bracing for AI-Driven Cyber Fraud // The Hacker News (https://thehackernews.com/2026/02/safe-and-inclusive-esociety-how.html). 16.02.2026).***

***

«…Кібербезпека зараз є невід'ємною частиною стратегічного ландшафту Європи, але ефективне кіберзапобігання залишається недосяжним, оскільки класична теорія запобігання погано підходить для цифрової сфери. На відміну від традиційних військових контекстів з чіткими порогами та передбачуваною ескалацією, кіберпростір характеризується поступовими, неоднозначними та постійними операціями, спрямованими на використання правових сірих зон та політичної нерішучості. Європа особливо вразлива: її економіка та державні служби глибоко цифровізовані, а повноваження з питань безпеки та реагування роздроблені між національними та європейськими інституціями, що робить окремі інциденти занадто незначними для колективного відплати, але сукупно підриває довіру та згуртованість…

Політика відображає цю напругу — стримування застосовується, але рідко реалізується, червоні лінії залишаються неявними, а атрибуція випереджає домовленості щодо наслідків — на тлі структурної невідповідності між національним цивільним управлінням кібербезпекою та логікою військового альянсу, що лежить в основі стримування (наприклад, навмисна двозначність НАТО щодо статті 5). Як результат, Європа покладається на стримування шляхом відмови — підвищення стійкості за допомогою таких механізмів, як NIS2 та DORA, — що знижує прибутки зловмисників, але не накладає на них витрат; каральні заходи обмежуються нерівномірними наступальними можливостями та скоординованими санкціями або публічними атрибуціями, ефективність яких залежить від послідовності.

Залежність від неєвропейських постачальників хмарних послуг та послуг безпеки, нерівномірна видимість та повільне, фрагментоване прийняття рішень ще більше послаблюють стримуючий ефект. Шлях уперед полягає в тому, щоб розглядати стримування як процес: зменшувати вигоди шляхом відмови, підвищувати витрати за допомогою скоординованих, заздалегідь сигналізованих відповідей та інтегрувати кібербезпеку в більш широке планування ескалації з використанням рутинних сигналів, кризового управління та міждоменної

координації, скорочуючи розрив між стратегічними амбіціями Європи та оперативним виконанням…» ***(John Allen, and Alexandr Burilkov. Cyber Deterrence Without Illusions: Europe's Escalation Dilemma // Center for the National Interest (https://nationalinterest.org/feature/cyber-deterrence-without-illusions-europes-escalation-dilemma). 24.02.2026).***

***

«Сучасні автомобілі тепер функціонують як мобільні комп'ютери, виконуючи понад 100 мільйонів рядків коду та генеруючи безперервні потоки даних — від стану двигуна та заряду акумулятора до геолокації та поведінки водія — за допомогою сотень датчиків. Цей вибух даних про транспортні засоби та користувачів підвищує безпеку, комфорт та ефективність, але також створює нові ризики кібератак, шпигунства та порушень конфіденційності, змушуючи автомобільний сектор поєднувати необхідний обмін даними для надання послуг (технічне обслуговування, допомога водієві, інформаційно-розважальні системи) з конфіденційністю та безпекою…

В Європі управління є складним, оскільки існує кілька режимі, що перетинаються: GDPR, Закон про кіберстійкість та, з вересня 2025 року, Закон ЄС про дані, а також численні національні та галузеві правила. Закон про дані покликаний збільшити потоки даних B2C, B2B та B2G, надаючи користувачам — споживачам та підприємствам — права на доступ до даних, що генеруються підключеними продуктами, такими як автомобілі, та на передачу їх третім сторонам за їхнім вибором, що сприятиме посиленню конкуренції та появі нових послуг, які виходять за межі того, що сьогодні контролюють виробники. Однак таке «відкриття» даних створює напругу у сфері кібербезпеки, захисту комерційної таємниці та запатентованих технологій, порушуючи практичні питання щодо безпечного шифрування, безпеки життєвого циклу транспортних засобів, які залишаються на дорогах протягом ~15 років, та меж промислової таємниці…

Закон про дані також спрямований на зміцнення європейського цифрового суверенітету шляхом зменшення залежності від неєвропейських хмарних провайдерів та введення обов'язкової хмарної портативності для полегшення міграції та зменшення залежності від одного постачальника. Однак екстериторіальні закони, такі як американський CLOUD Act та FISA, все ще можуть надавати іноземним державам доступ до європейських даних, навіть якщо вони зберігаються в Європі, що означає, що повна імунітет є важкодосяжним. Як показує нещодавнє рішення канадського суду щодо французької компанії OVHCloud, компанії, що ведуть діяльність у третіх країнах, все ще можуть стикатися з вимогами про розкриття інформації. Тому реалістичним шляхом є мінімізація ризиків: уточнення того, як перетинаються правила, спрощення зобов'язань, де це можливо, та розробка технічних і організаційних заходів безпеки, що дозволяють законно обмінюватися даними без шкоди для безпеки або конфіденційності». ***(Thomas Le Goff. What the future holds for cybersecurity in connected vehicles // Polytechnique Insights (https://www.polytechnique-insights.com/en/columns/digital/the-challenge-of-cybersecurity-for-connected-vehicles/). 24.02.2026).***

***

«Президент Польщі Кароль Навроцький підписав урядський законопроект про посилення національної системи кібербезпеки, який забороняє «високоризиковим» постачальникам, особливо з країн, що не входять до НАТО, таких як Китай, доступ до секторів, що мають вирішальне значення для функціонування держави. Закон, який впроваджує директиву ЄС NIS 2, отримав рідкісну міжпартійну підтримку, але викликав гнів бізнес-груп, стурбованих високими витратами на дотримання вимог, що спонукало президента одночасно передати законопроект на розгляд до Конституційного трибуналу (ТК)…

Законодавство створює категорію постачальників «високого ризику» — позначення, яке може базуватися на походженні постачальника або контролі з боку країни, що не є членом НАТО, — яким буде заборонено постачати товари або послуги до таких життєво важливих секторів, як енергомережа, поштові послуги, хімічне та харчове виробництво. Китайська компанія Huawei була названа ймовірною мішенню, через що законопроект неофіційно отримав назву «Lex Huawei». Державні організації, які вже використовують продукцію цих постачальників з високим ризиком, матимуть сім років на її вилучення, що бізнес-організації назвали «експропріацією» через відсутність компенсації…

Президент Навроцький наголосив на різкому зростанні кількості кібератак проти Польщі — країни ЄС, яка, згідно з останнім звітом Microsoft, є найбільш уразливою для таких атак — і заявив, що цифрова безпека є нині важливою складовою національної оборони. Міністр цифрових справ привітав закон як «важливий крок до підвищення безпеки», але розкритикував рішення президента про передачу справи до Конституційного суду, заявивши, що на нього вплинули «іноземні лобісти» і що це створить невизначеність для бізнесу. Закон набуде чинності в очікуванні розгляду ТК, хоча чинний уряд не визнає рішення суду, вважаючи його нелегітимним через незаконне призначення суддів попередньою адміністрацією». ***(Poland tightens cybersecurity rules targeting non-NATO suppliers // Notes From Poland (https://notesfrompoland.com/2026/02/21/poland-tightens-cybersecurity-rules-targeting-non-nato-suppliers/). 21.02.2026).***

***

«Агентство Європейського Союзу з кібербезпеки (ENISA) опублікувало оновлену методологію проведення навчань з кібербезпеки, яка пропонує структуровану комплексну систему для організацій та урядів по всій Європі з метою підвищення їхньої кіберстійкості. Розроблена для фахівців з кібербезпеки та організаційних планувальників, ця методологія слугує комплексним планом для планування, проведення та оцінки навчань з метою перевірки оперативних навичок, процедур реагування на інциденти та, що найважливіше, дотримання основних європейських нормативних актів, таких як NIS2 та Закон ЄС про кібербезпеку…

Методологія ENISA базується на таких основних принципах, як структуроване планування, нарощування потенціалу, гнучкість для адаптації до різних організаційних потреб та сприятлива екосистема ресурсів, що включає

практичний набір шаблонів і контрольних списків, узгоджених з Європейською рамкою навичок у сфері кібербезпеки. Вона поділяє вправи на шість критичних етапів — від концептуалізації до оцінки після вправи — і включає такі ключові компоненти, як детальний план вправи, план оцінки з чіткими цілями щодо можливостей, план комунікацій, перелік основних сценаріїв подій (MSEL) для моделювання кризових ситуацій та звіт після завершення дій (AAR) для забезпечення постійного вдосконалення…

Застосовуючи цю структуру, організації можуть скоротити час на підготовку, перетворити результати навчань на практичні поліпшення та продемонструвати готовність до дотримання нормативних вимог. Відповідність методології встановленим стандартам та акцент на співпраці спільноти через семінари та експертні форуми гарантують, що навіть складні навчання на національному рівні можуть скористатися спільним досвідом, що в кінцевому підсумку сприятиме формуванню культури постійного вдосконалення та зміцненню колективної позиції Європи в галузі кібербезпеки». ***(ENISA's Updated Cybersecurity Methodology Aligns with NIS2 and EU Cybersecurity Act // Cyble Inc. (https://cyble.com/blog/enisa-cybersecurity-exercise-methodology/). 26.02.2026).***

***

«Уряд Великобританії запустив нову службу моніторингу вразливостей (VMS), призначену для захисту державного сектора від кіберзагроз, стверджуючи, що вона може виявляти та усувати критичні слабкі місця в шість разів швидше, ніж попередні методи. У відповідь на нещодавні атаки на такі важливі служби, як Національна служба охорони здоров'я (NHS) та Агентство з надання правової допомоги, VMS спеціально націлена на вразливі місця в системі доменних імен (DNS), щоб запобігти викраденню даних або відключенню служб зловмисниками. Якщо раніше вразливі місця в DNS залишалися непоміченими протягом майже двох місяців, то ця служба скоротила цей термін до восьми днів, постійно скануючи 6000 органів державного сектора на наявність приблизно 1000 різних типів вразливостей…

Завдяки автоматизації виявлення та наданню адміністраторам практичних рекомендацій, VMS досягла 84% поліпшення часу виправлення проблем, пов'язаних з доменом, та зменшила кількість критичних вразливостей на 75%. На додаток до цього технічного впровадження, уряд також запровадив програму «Кіберпрофесія» для набору та підготовки елітних талантів. Ця ініціатива, очолювана Національним центром кібербезпеки (NCSC) та Міністерством науки, інновацій та технологій, включає центр кіберресурсів для оптимізації набору персоналу, спеціальну кіберакадемію та програму стажування. Програма, яка базується переважно на північному заході країни з метою використання цифрової екосистеми Манчестера, спрямована на створення структурованих кар'єрних шляхів та формування стійкої робочої сили, здатної захистити державні служби від дедалі більш досконалих цифрових загроз». ***(Tom Quinn. New Gov Cyber Tool Cuts Attack Fix Times by 84% // DIGIT (https://www.digit.fyi/new-gov-cyber-tool-cuts-attack-fix-times-by-84/). 26.02.2026).***

***

«Міжнародне дослідження компанії Exabeam показує, що хоча 93% британських та ірландських організацій збільшують свої бюджети на кібербезпеку на 2026 рік (68% з них очікують двозначного зростання), керівники служб безпеки намагаються стратегічно узгодити та обґрунтувати ці інвестиції перед своїми правліннями. Штучний інтелект займає парадоксальне місце в плануванні бюджету: він одночасно є основним фактором збільшення фінансування (51%), першою інвестицією, яку, ймовірно, скоротять у разі жорсткості бюджетів (43%), і найскладнішою статтею витрат, яку важко обґрунтувати перед зацікавленими сторонами (28%). Хоча керівники служб безпеки впевнені в цінності ШІ, існує значна розбіжність у демонстрації цієї цінності керівництву; 26% респондентів з Великобританії та Ірландії називають головним викликом відсутність розуміння з боку правління зв'язку між кібербезпекою та стійкістю бізнесу…

Ця «розбіжність у демонстрації цінності» виникає через невідповідність між технічними показниками безпеки та мовою прийняття бізнес-рішень. Хоча команди використовують операційні дані та дані про результати, традиційні показники, такі як середній час вирішення проблеми (MTTR), часто не дозволяють чітко визначити вимірюване зниження ризику або довгостроковий вплив на бізнес. Експерти вважають, що оскільки середовища, що підтримуються штучним інтелектом, роблять швидкість майже автоматичною, акцент повинен бути перенесений на доведення того, як штучний інтелект усуває умови, що сприяють виникненню інцидентів… Регіональні відмінності ще більше підкреслюють різноманітність стратегій: Саудівська Аравія повідомляє про 75% поліпшення операцій з безпеки завдяки ШІ, порівняно з 43% у Великобританії та Ірландії, що відображає поєднання агресивних національних цифрових ініціатив та більш обережного європейського масштабування. Зрештою, стійкість поточного збільшення бюджету залежить від здатності керівників служб безпеки розробляти нові, орієнтовані на результат рамки, які перетворюють технічні характеристики ШІ на мову стійкості бізнесу та чіткої окупності інвестицій». ***(Elizabeth Greenberg. AI Accountability Drives Cybersecurity Budgets in 2026 // DIGIT (https://www.digit.fyi/ai-accountability-drives-cybersecurity-budgets-in-2026/). 24.02.2026).***

***

«Згідно з проектом закону, з яким ознайомилося агентство Reuters, Німеччина планує розширити повноваження правоохоронних органів для боротьби з кіберзагрозами, що є важливим кроком у напрямку зміцнення кіберзахисту країни. Запропонований закон надає силовим структурам право втручатися в роботу ІТ-систем, включаючи їх відключення та видалення даних, навіть на іноземних серверах.

Цей захід, спричинений повномасштабним вторгненням Росії в Україну в 2022 році, є частиною ширшої стратегії зміцнення збройних сил і розвідувальних агентств Німеччини, що базується на історичних чутливих моментах. Міністр внутрішніх справ Олександр Добріндт наголосив на необхідності підготовки країни

до іноземних кібератак, які, як часто підозрюють, походять з Росії, хоча Москва заперечує ці звинувачення.

Законопроект передбачає, що втручання в приватні системи, як правило, вимагає судового рішення, яке в екстрених випадках може бути отримане ретроспективно. Він також вимагає співпраці від постачальників цифрових послуг, передбачаючи штрафи за невиконання. Важливо, що Федеральне управління з інформаційної безпеки буде займатися «полюванням на загрози» з метою проактивного пом'якшення потенційних кіберзагроз». ***(Germany Bolsters Cyber Defense with New Law // Devdiscourse (https://www.devdiscourse.com/article/technology/3820357-germany-bolsters-cyber-defense-with-new-law). 27.02.2026).***

***

Австралія та Нова Зеландія

«Недавній сплеск вимог від групи хакерів-вимагачів Qilin привернув пильну увагу австралійських кіберстраховиків та менеджерів з управління ризиками, оскільки ця фінансово мотивована операція RaaS з кінця січня розмістила на своєму даркнет-сайті чотири регіональні австралійські підприємства — три в Західній Австралії та одне в Квінсленді. Хоча Qilin заявляє про значну крадіжку даних, включаючи 40 ГБ від Mount Barker Co-operative, відсутність перевірених доказів та непрацюючі посилання на витік даних підкреслюють тактику створення невизначеності для чинення тиску. Дослідження показують, що Qilin, яка розширилася з 45 жертв у 2022 році до понад 800 у 2025 році, зазвичай перебуває в мережах у середньому 19 днів, що дає достатньо часу для розвідки та викрадення даних перед шифруванням….

Ця діяльність відбувається на тлі більш широкої ескалації кіберзагроз в Австралії, при цьому Австралійський центр кібербезпеки (ACSC) повідомляє про 16% зростання кількості дзвінків на гарячу лінію та значне збільшення зловмисної діяльності в мережі та фінансових втрат, особливо для великих організацій. Страховики наголошують на критичній важливості перших 48 годин реагування на інцидент, закликаючи організації заздалегідь домовитися про доступ до технічних та юридичних експертів, оскільки інциденти з програмним забезпеченням-вимагачем все частіше супроводжуються складним витоком даних та регуляторними зобов'язаннями… Рішення про виплату викупу супроводжуються юридичними обмеженнями відповідно до законів про санкції та обов'язковими вимогами щодо подання звітності до ASD (Австралійське управління зв'язку) та OAIC (Офіс австралійського комісара з питань інформації). Отже, готовність — завдяки перевіреним планам реагування та чіткості страхового покриття — має першочергове значення для подолання юридичних, репутаційних та фінансових наслідків таких кампаній з вимагання викупу». ***(Roxanne Libatique. Qilin ransomware activity adds pressure on Australian insurers // KM Business Information Australia Pty Ltd (https://www.insurancebusinessmag.com/au/news/cyber/qilin-ransomware-activity-adds-pressure-on-australian-insurers-566534.aspx). 25.02.2026).***

***

«Компанія Emergence Insurance (Австралія) оновила свою політику захисту від кіберзагроз (CEP) для австралійських малих і середніх підприємств, випустивши формулювання CEP-005.1. Цей крок був обумовлений тим, що кіберзагрози залишаються головним ризиком для місцевих організацій. Згідно з глобальним опитуванням Aon з управління ризиками 2025 року, 93% австралійських респондентів зараз розглядають кіберзагрози як ризик для підприємства, що вимагає офіційного нагляду, що відображає перехід від суто технічних проблем до системних порушень у роботі бізнесу. Цей контекст підкріплюється даними OAIC (Офіс австралійського комісара з питань інформації) за перше півріччя 2025 року, які зафіксували 532 випадки порушення безпеки даних — переважно внаслідок зловмисних атак (59 %), але з помітним зростанням кількості людських помилок (37 %) — що вплинули на такі сектори, як охорона здоров'я, фінанси та державне управління…

Оновлення CEP-005.1, розроблене на основі відгуків брокерів та досвіду розгляду страхових випадків, передбачає ключові вдосконалення покриття, включаючи обмеження «будь-якого одного інциденту», повне покриття системних збоїв та не пов'язаних з IT випадкових перебоїв у роботі, а також розширену опціональну секцію щодо кримінальних фінансових втрат, що охоплює крадіжку фізичних товарів… Окрім цих фінансових захисних заходів, Emergence продовжує включати набір послуг з управління ризиками без додаткових витрат, таких як віртуальний CISO, аналіз загроз та моніторинг даркнету. Команда реагування на інциденти страхової компанії також надає підтримку в розслідуванні та координації, що виходить за межі лімітів та надлишку полісу, забезпечуючи практичну підтримку страхувальникам. Ці зміни відображають те, як страхові компанії адаптують продукти до мінливого профілю кіберризиків, де середня вартість порушення безпеки даних оцінюється в 4,26 мільйона доларів». ***(Roxanne Libatique. Emergence updates cyber policy wording for Australian SMEs // KM Business Information Australia Pty Ltd (https://www.insurancebusinessmag.com/au/news/cyber/emergence-updates-cyber-policy-wording-for-australian-smes-565467.aspx). 16.02.2026).***

***

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

«Гонконг активізує свої зусилля, щоб стати «фортецею» проти все більш складних кібератак і витончених шахрайських схем, усвідомлюючи, що технологічний прогрес повинен йти рука в руку з надійною кібербезпекою. Секретар з питань інновацій, технологій та промисловості Сун Дон підкреслив на недавньому симпозіумі, що захист міста від цифрових загроз є необхідною умовою для сталого розвитку технологій…

Останні звіти підкреслюють нагальність цієї місії. Кількість повідомлень про витоки даних, що надійшли до органу з нагляду за захистом персональних даних

Гонконгу, у 2025 році зросла на 21% порівняно з попереднім роком, а кількість випадків хакерських атак — на 33%. Рада з продуктивності Гонконгу також повідомила про рекордну кількість кібератак, попередивши, що розвиток штучного інтелекту (ШІ) робить фішинг-атаки більш переконливими та збільшує ризик витоку конфіденційних даних, особливо з огляду на те, що генеративні та агентивні інструменти ШІ стають все більш поширеними.

Дослідження Ради виявило більш ніж трикратне збільшення випадків, пов'язаних із вразливими комп'ютерними системами, що було спричинено активними перевірками, які виявили поширені прогалини в системі безпеки. Оскільки Гонконг прагне стати міжнародним центром інновацій та технологій, комплексні заходи з кібербезпеки мають вирішальне значення для захисту від хакерських атак та витоку даних…

Уряд реагує на це шляхом підвищення обізнаності, забезпечення професійної підготовки та вдосконалення управління державними інформаційними системами шляхом співпраці, навчань та захисних заходів. 1 січня набув чинності новий закон про захист критичної інфраструктури, який встановлює більш суворі вимоги до операторів у восьми основних секторах. Очікується, що це законодавство сприятиме поширенню культури обізнаності про кібербезпеку та зменшенню ризиків.

Сун Дон закликав усі сектори суспільства до співпраці, наголосивши, що інновації та технології можуть приносити користь суспільству лише тоді, коли вони побудовані на надійній основі». ***(Hong Kong's innovation goals must go hand in hand with cybersecurity // South China Morning Post Publishers Ltd. (https://www.scmp.com/opinion/comment/article/3342327/hong-kongs-innovation-goals-must-go-hand-hand-cybersecurity). 06.02.2026).***

***

«Згідно з «Дослідженням ризиків FICCI-EY 2026», порушення кібербезпеки стали головним предметом занепокоєння керівників індійських організацій: 51% опитаних назвали це головним ризиком, за яким слідують зміни в потребах клієнтів (49%) і геополітичні події (48%). На основі даних, отриманих від 137 керівників вищої ланки, зокрема з секторів технологій та професійних послуг, у звіті підкреслюється, що технологічні ризики тепер нерозривно пов'язані з безперебійністю діяльності. Значна частина респондентів (61%) вважає, що швидкі цифрові зрушення впливають на їхню конкурентну позицію, а така ж частка респондентів вважає кібератаки та порушення безпеки даних серйозними загрозами для фінансів та репутації. Крім того, понад половина опитаних керівників вказали на крадіжку даних та шахрайство з боку інсайдерів як на значні ризики, а майже половина визнали, що їм важко протидіяти дедалі більш витонченим кіберзагрозам…

Штучний інтелект (ШІ) представляє подвійний виклик для індійських компаній: 60% опитаних побоюються, що недостатнє впровадження нових технологій завадить оперативній ефективності, а 54% стурбовані тим, що ризики, пов'язані з ШІ, включаючи етичні та управлінські питання, не управляються ефективно. Окрім технологій, серйозну загрозу становить динаміка робочої сили:

64% респондентів стурбовані нестачею талановитих кадрів і прогалинами в кваліфікації, а 59% вказують на слабке планування наступності. Також поширені регуляторні та операційні виклики: 40% організацій намагаються встигати за змінами в нормативно-правовій сфері, а 54% залишаються стурбованими порушеннями в ланцюгах постачання…» ***(Cybersecurity breaches emerge as top risk for India Inc: FICCI-EY Survey // THG PUBLISHING PVT LTD. (https://www.thehindubusinessline.com/info-tech/cybersecurity-breaches-emerge-as-top-risk-for-india-inc-ficci-ey-survey/article70607018.ece). 08.02.2026).***

***

«…У відповідь на нещодавні масштабні порушення безпеки даних у телекомунікаційному, роздрібному та фінансовому секторах, Національна асамблея Південної Кореї та урядові органи просувають законодавчі поправки до Закону про мережі та Закону про захист персональних даних (PIPA) з метою посилення кібербезпеки та захисту даних. Закон про мережі, який контролюється Міністерством науки та інформаційно-комунікаційних технологій (MSIT), та PIPA, який управляється Комісією з захисту персональних даних (PIPC), оновлюються з метою посилення управління безпекою, вдосконалення систем управління інформацією та забезпечення ефективного реагування на інциденти. Основні зміни включають розширення ролі та повноважень головних спеціалістів з інформаційної безпеки (CISO) та головних спеціалістів з конфіденційності (CPO), обов'язкову сертифікацію ISMS-P до середини 2027 року та запровадження регулярних оцінок рівня безпеки. Поправки також встановлюють більш суворі зобов'язання щодо повідомлення про інциденти та інформування користувачів, а також посилюють покарання за невиконання коригувальних наказів…

Одночасно MSIT визначив пріоритетність реагування на хакерські атаки в приватному секторі у своєму робочому плані на 2026 рік, а PIPC окреслив цільові політики розслідування на наступний рік. Підприємствам рекомендується проактивно оцінювати свої регуляторні зобов'язання з урахуванням розміру та обсягу даних, посилювати свої системи управління безпекою та інвестувати в спеціалізований персонал і бюджети. Компанії також повинні оновлювати свої посібники з реагування на інциденти, щоб відповідати новим законодавчим вимогам, та встановлювати надійні внутрішні процеси для оперативного реагування на регуляторні розслідування. Удосконалюючи процедури прийняття рішень та впроваджуючи системи управління після інцидентів для запобігання їх повторенню, організації можуть краще орієнтуватися в мінливому регуляторному середовищі та зменшувати ризики суворих санкцій…» ***(Sun Hee Kim, Na Ray Kim, Sang Ho Bae, Syng Hyok Choi and Hye Jin Yun. Legislative and Regulatory Trends in Data Protection and Cybersecurity // Yulchon LLC (https://www.yulchon.com/en/resources/publications/newsletter-view/42836/page.do). 09.02.2026).***

***

«31 січня 2026 року Міністерство громадської безпеки Китаю опублікувало проект Закону про запобігання та боротьбу з кіберзлочинністю

для громадського обговорення, що стало наслідком приєднання країни до Конвенції ООН про боротьбу з кіберзлочинністю. Запропонований закон, який базується на існуючих нормативних актах у сфері кібербезпеки та безпеки даних, значно розширює обов'язки та відповідальність підприємств, зокрема операторів мереж та обробників даних. Він передбачає такі заходи, як створення спеціальних органів з попередження кіберзлочинності, ведення детальних записів про інциденти та впровадження надійних технічних заходів безпеки, таких як маркування даних та можливість їх відстеження, особливо для контенту, створеного за допомогою штучного інтелекту…

Важливо, що законопроект спрямований на боротьбу з транскордонною кіберзлочинністю, надаючи правову основу для дій проти закордонних суб'єктів, включаючи технічне блокування, заморожування активів та обмеження інвестицій і в'їзду. Він також запроваджує багаторівневу систему відповідальності з покараннями, що варіюються від штрафів і призупинення діяльності до кримінального переслідування. Міжнародним підприємствам рекомендується проактивно переглянути свої системи забезпечення відповідності, щоб привести їх у відповідність до цих підвищених регуляторних вимог до закінчення періоду консультацій 2 березня 2026 року…» ***(Jonathan Chu and Anqi Qin. China releases draft law on preventing cybercrime for public comment // CMS (https://cms-lawnow.com/en/ealerts/2026/02/china-releases-draft-law-on-preventing-cybercrime-for-public-comment). 12.02.2026).***

***

«З 1 січня 2026 року змінений Закон Китаю про кібербезпеку (CSL) вносить істотні зміни до покарань, екстериторіального правозастосування та управління штучним інтелектом, зберігаючи при цьому основні зобов'язання операторів та внутрішню юрисдикцію без змін. Затверджені в жовтні 2025 року, ці зміни є першою значною реформою з моменту прийняття закону в 2017 році…

Зміни посилюють інструментарій правозастосування. Тепер органи влади можуть накладати штрафи за загальні порушення кібербезпеки (наприклад, за невиконання вимог щодо реєстрації даних безпеки) у розмірі від 10 000 до 50 000 юанів без попереднього попередження або доведеного збитку. За серйозні порушення, пов'язані з масовим витоком даних або невиправленням проблем, штрафи різко зростають — до 2 мільйонів юанів для підприємств і 200 000 юанів для фізичних осіб. Аналогічно, невиконання вимог щодо припинення незаконного поширення інформації або усунення дефектів безпеки продукції тепер може спричинити штрафи, що досягають 10 мільйонів юанів у «особливо серйозних» випадках, таких як виведення з ладу критично важливих функцій інфраструктури.

Важливо, що поправки розширюють повноваження з виконання законів за межі Китаю. Тепер влада може застосовувати санкції до іноземних юридичних або фізичних осіб, діяльність яких ставить під загрозу не тільки критичну інформаційну інфраструктуру Китаю, а й кібербезпеку країни в цілому. Це може стосуватися обробки даних за кордоном або ІТ-послуг, що впливають на китайські мережі…

Крім того, закон закріплює нові цілі політики в галузі управління ШІ, обіцяючи державну підтримку досліджень і розробок у сфері ШІ та інфраструктури, одночасно посилюючи етичне регулювання та моніторинг ризиків. З огляду на ці зміни, транснаціональним компаніям рекомендується терміново переглянути свої програми дотримання вимог, щоб зменшити підвищений ризик негайних штрафів та розширення сфери застосування заходів примусу». ***(Philip Ruan, Jena M. Valdetero and Andrea Maciejewski. China's Amended Cybersecurity Law Takes Effect // Greenberg Traurig, LLP. (https://www.gtlaw.com/en/insights/2026/2/chinas-amended-cybersecurity-law-takes-effect). 12.02.2026).***

***

«Сінгапур планує ввести в дію Закон про цифрову інфраструктуру (DIA) пізніше цього року, щоб встановити більш суворі вимоги до енергоефективності та кібербезпеки для центрів обробки даних та основних постачальників хмарних послуг. Законодавство встановить обов'язкові стандарти енергоефективності (PUE) як для існуючих, так і для майбутніх об'єктів, оскільки потужність центрів обробки даних країни, яка вже перевищує 1,4 гігавата, як очікується, буде швидко зростати з підвищенням навантаження на штучний інтелект. Старший державний міністр Тан Кіат Хоу підкреслив, що сталий розвиток є надзвичайно важливим з огляду на обмеженість ресурсів Сінгапуру, і що стандарти будуть скориговані відповідно до міжнародних критеріїв, одночасно поступово підвищуючи ефективність усього парку центрів обробки даних…

Окрім екологічних цілей, DIA встановить базові зобов'язання щодо кібербезпеки, стійкості та управління ризиками для основних операторів, включаючи обов'язкове повідомлення про інциденти, з метою захисту основних цифрових послуг, таких як банківські та цифрові системи ідентифікації. Цей крок ґрунтується на дорожній карті Сінгапуру щодо зелених центрів обробки даних і сигналізує про перехід від рекомендаційних вказівок до обов'язкового регуляторного нагляду, щоб забезпечити стійкість, надійність та безпеку цифрової інфраструктури країни в умовах прискорення попиту, зумовленого розвитком штучного інтелекту». ***(Nurdianah Md Nur. Singapore plans legislation to impose energy, cybersecurity standards on data centres and major cloud providers // The Edge Publishing Pte Ltd. (https://www.theedgesingapore.com/digitaledge/digital-economy/singapore-plans-legislation-impose-energy-cybersecurity-standards-data). 24.02.2026).***

***

«Збройні сили Філіппін (AFP) запевнили громадськість, що активно посилюють свої можливості кіберзахисту в умовах більш складної та динамічної загрози в 2026 році, спричиненої ескалацією геополітичної напруженості в Західно-Філіппінському морі. Речниця AFP полковник Франсель Маргарет Паділья, міжнародно визнана експертка з кібербезпеки та перша філіппінка, яка отримала нагороду «Жінка року в галузі кібербезпеки» у 2023 році, наголосила, що ці напруження поширюються на кіберпростір, де постійні загрози,

включаючи вторгнення в мережі, псування веб-сайтів та кампанії з дезінформації, значною мірою пов'язані з діячами з Китаю…

Вона зазначила, що Філіппіни є частиною більш широкої глобальної тенденції, коли державні та недержавні суб'єкти використовують кіберпростір для просування своїх стратегічних інтересів, підкресливши, що сучасні загрози безпеці щодня еволюціонують і впливають на всіх. Щоб протидіяти цим ризикам, Кіберкомандування Збройних сил Філіппін посилює захисні заходи, покращує обмін інформацією про загрози з партнерськими агентствами та співпрацює з вітчизняними та міжнародними зацікавленими сторонами для захисту критичної інформаційної інфраструктури». ***(Michael Punongbayan. AFP strengthening cyber defenses // Philstar Global Corp. (https://www.philstar.com/headlines/2026/02/21/2509389/afp-strengthening-cyber-defenses). 21.02.2026).***

***

«Південна Корея значно посилює свої системи кібербезпеки та захисту персональних даних у відповідь на серію масштабних порушень у телекомунікаційному, роздрібному та фінансовому секторах. Запропоновані поправки до Закону про мережі та Закону про захист персональних даних (PIPA) мають на меті покращити управління, реагування на інциденти та правозастосування…

Основні зміни включають розширення повноважень керівників служб інформаційної безпеки (CISO) та керівників служб конфіденційності (CPO) з прямим підпорядкуванням раді директорів та наглядом за ресурсами, обов'язкові комітети з кібербезпеки для великих провайдерів, більш суворі критерії сертифікації ISMS та чітку відповідальність генерального директора за захист даних. Терміни повідомлення про інциденти будуть скорочені до 24 годин, визначення порушень буде розширено, щоб включити зміну або пошкодження даних, а штрафи будуть різко збільшені — до 3% річного доходу відповідно до Закону про мережі та, можливо, до 10% відповідно до PIPA за серйозні або повторні порушення, хоча можуть застосовуватися знижки за підтверджені інвестиції в заходи захисту…

Регулюючі органи — Міністерство науки та інформаційно-комунікаційних технологій (MSIT) та Комісія з захисту персональних даних (PIPC) — оголосили про агресивні пріоритети у сфері правозастосування на 2026 рік: проактивні розслідування, швидке покарання для рецидивістів та фокус на секторах з високим ризиком і чутливих типах даних. Зміни в ситуації вимагають від організацій переоцінки структур управління, планів реагування на інциденти та програм дотримання вимог, щоб відповідати підвищеним очікуванням щодо прозорості, підзвітності та стійкості». ***(Charmian Aw, Paul Otto, Ciara O'Leary. South Korea considers updates to data and cyber laws // Hogan Lovells (https://www.hoganlovells.com/en/publications/south-korea-considers-updates-to-data-and-cyber-laws). 25.02.2026).***

***

«Завдяки процвітаючій екосистемі, що налічує понад 500 компаній, та потужній підтримці уряду, Ізраїль продовжує зміцнювати свої позиції світового лідера в галузі кібербезпеки у 2026 році. Спираючись на глибокий кадровий резерв експертів з національної безпеки та потужну інфраструктуру досліджень і розробок, сектор продемонстрував виняткові фінансові результати та стійкість до економічних і геополітичних негараздів. Про це свідчить рекордний обсяг залучених капіталовкладень, який у 2025 році досяг найвищого за всю історію рівня в 8,27 млрд доларів — це майже 110% річне зростання, яке перевищило попередній пік, встановлений у 2021 році. Крім того, загальна вартість виходу з ринку для цього сектора стрімко зросла до приблизно 72,6 млрд доларів у 2025 році, що на 1500% більше, ніж у 2024 році, хоча основною стратегією виходу з ринку залишається придбання, і лише невелика частина компаній виходить на біржу…

Здатність сектора перевищувати свої можливості є очевидною: хоча компанії з кібербезпеки становлять лише близько 7% технологічної екосистеми Ізраїлю, вони залучили 36% загальних інвестицій у технологічний сектор у 2024 році, зібравши 3,8 млрд доларів — суму, що еквівалентна 40% загального обсягу ринку США. Цей приплив капіталу сприяв створенню зрілого середовища, в якому 31% кіберкомпаній розширилися до більш ніж 50 співробітників, а концентрація компаній, що знаходяться на стадії зростання, більш ніж удвічі перевищує показники інших секторів. Провідні компанії в різних галузях, такі як гіганти хмарної безпеки Wiz і Orca Security та інноватори в галузі безпеки даних Cyera і Deep Instinct, використовують цю силу для розширення своєї міжнародної присутності в Європі, Азії та Америці.

Ця глобальна експансія ще більше підкреслюється стратегічними міжнародними партнерствами, такими як співпраця з Федеральним міністерством внутрішніх справ Німеччини з метою розробки «кіберкупола» для національної оборони. Використовуючи послуги з виходу на ринок для проникнення на високотехнологічні ринки, такі як США та Китай, «Стартап-нація» успішно експортує свій досвід у сфері кібербезпеки у великих масштабах, забезпечуючи постійне зростання та відіграючи важливу роль у захисті цифрових екосистем у всьому світі…» ***(Dmytro Spilka. Israel's World-Leading Cybersecurity Sector is Scaling at an Unprecedented Pace // The Times of Israel (https://blogs.timesofisrael.com/israels-world-leading-cybersecurity-sector-is-scaling-at-an-unprecedented-pace/). 08.02.2026).***

***

«Рада з кібербезпеки ОАЕ (CSC) успішно запобігла організованим кібератакам терористичного характеру, спрямованим на дестабілізацію цифрової інфраструктури країни та порушення роботи основних служб. Ці атаки, що включали спроби проникнення в мережу, використання програм-вимагачів та систематичні фішингові кампанії, зокрема, використовували штучний інтелект для розробки складних засобів нападу, що свідчить про якісну зміну

методів терористів… Підкреслюючи, що захист осіб, даних та критично важливих послуг є головним пріоритетом, Рада наголосила на своїй цілодобовій системі національної оборони, яка працює у співпраці з вітчизняними та міжнародними партнерами для забезпечення стійкості та швидкого відновлення. Підтверджуючи свою прихильність до захисту цифрової сфери, Рада закликала громадськість повідомляти про будь-які підозрілі дії через офіційні канали для збереження національної безпеки та інституційної безперервності». ***(UAE Cybersecurity Council announces systematic terrorist cyberattacks targeting vital sectors thwarted // SyndiGate Media Inc. (https://www.aninews.in/news/world/middle-east/uae-cybersecurity-council-announces-systematic-terrorist-cyberattacks-targeting-vital-sectors-thwarted20260222064555/). 22.02.2026).***

***

«…За словами глави Національного кібердиректорату Ізраїлю (INCD) Йосі Караді, за останні роки Ізраїль зазнав крадіжки вражаючих двох петабайтів (двох квадрильйонів байтів) даних, що еквівалентно приблизно 100-кратному обсягу цифрового контенту всієї Національної бібліотеки Ізраїлю. Цей безпрецедентний масштаб хакерських атак, який в основному приписують іранській розвідці, свідчить про різке зростання кіберзагроз, а Ізраїль зараз посідає третє місце серед країн світу за кількістю атак. У 2025 році в країні відбувся 35-відсотковий сплеск фішингових атак і 170-відсоткове збільшення кібероперацій, спрямованих на маніпулювання громадською думкою…

INCD також попередив про сотні складних атак, що відбулися з середини 2025 року і були спрямовані проти урядовців, співробітників служб безпеки, науковців та представників ЗМІ. Щоб посилити захист, Караді наполягає на прийнятті нового комплексного закону про кібербезпеку, який зобов'яже постачальників критичної інфраструктури та урядові установи дотримуватися 63 конкретних стандартів кібербезпеки, багато з яких базуються на рекомендаціях NIST, а також вимагатиме повідомлення INCD про серйозні інциденти в режимі реального часу. Запропонований законопроект, поданий у січні, планується винести на перше читання в Кнесеті в березні, перед початком передвиборчої кампанії». ***(YONAH JEREMY BOB. Hackers stole 2 quadrillion bytes of data from Israelis in recent years, cyber chief tells 'Post' // Jpost Inc. (https://www.jpost.com/israel-news/defense-news/article-887153). 18.02.2026).***

***

«Туреччина значно посилює свої національні можливості в галузі кібербезпеки завдяки амбітній програмі навчань та стратегічних ініціатив, викладених у Програмі діяльності Міністерства транспорту та інфраструктури на 2025 рік та Стратегічному плані на 2024-2028 роки. Цього року країна проведе 11 національних та міжнародних навчань з кібербезпеки, а до 2026 року планує провести 12, а до 2028 року – 13, з метою підвищення стійкості, вдосконалення процедур реагування та підвищення обізнаності в державному та приватному секторах…

Ці зусилля зосереджені на забезпеченні безпеки електронних комунікацій та критичної інфраструктури інформаційних технологій, визначенні чітких політик і стратегій, координації заходів з кіберзахисту, виявленні та захисті критичної інфраструктури, а також створенні центрів швидкого реагування. Ключовим пріоритетом є розробка внутрішніх інструментів та рішень у сфері кібербезпеки, а також посилення нагляду, створення нормативно-правової бази для операторів кібербезпеки та проведення широкомасштабних навчальних та інформаційних кампаній. Інтегруючи ці заходи, Туреччина прагне створити більш надійну, скоординовану та самодостатню національну екосистему кіберзахисту, здатну ефективно протидіяти новим загрозам». ***(Türkiye to strengthen cybersecurity shield with new drills // Hürriyet Daily News (https://www.hurriyetdailynews.com/turkiye-to-strengthen-cybersecurity-shield-with-new-drills-219197). 22.02.2026).***

***

Країни Африки

«…Незважаючи на значні витрати на різні платформи кібербезпеки, південноафриканські організації продовжують стикатися зі зростаючим числом порушень і загроз від програм-вимагачів, оскільки основною проблемою є не брак інструментів, а неефективне їх використання. Команди з безпеки перевантажені сповіщеннями та даними, але при цьому не можуть визначити пріоритетність ризиків і діяти рішуче через обмежені бюджети та брак кваліфікованих кадрів. Оскільки зловмисники автоматизують свої дії та націлюються на хмарні системи та системи ідентифікації, компаніям необхідно отримувати більшу віддачу від існуючих інвестицій, а не додавати нові інструменти…

Уніфіковані платформи, такі як Command Platform від Rapid7, покликані вирішити цю проблему шляхом консолідації даних про вразливість, хмару, ідентичність та виявлення в практичні висновки, що відображають реальні шляхи атак, дозволяючи командам зосередитися на невеликому наборі проблем, які дійсно знижують ризики для бізнесу. Швидші, інтегровані можливості реагування додатково допомагають невеликим командам SOC локалізувати інциденти до їх ескалації… Однак однієї лише технології недостатньо; для забезпечення належного налаштування платформ та їх відповідності пріоритетам бізнесу необхідна місцева підтримка та консультаційна допомога, така як та, що надається компанією Trinexia South Africa. В кінцевому рахунку, успіх у сфері кібербезпеки зараз залежить не від кількості інструментів, а від вимірюваного зниження ризиків, швидшого реагування та чіткої відповідності між кіберризиками та бізнес-результатами». ***(South Africa's cybersecurity challenge is not a tool problem // NewsCentral Media (https://techcentral.co.za/south-africas-cybersecurity-challenge-is-not-a-tool-problem/277882/). 19.02.2026).***

***

«Швидко зростаюча цифрова економіка Нігерії випереджає пропозицію талановитих фахівців у галузі кібербезпеки, що призводить до зростання кількості випадків використання програм-вимагачів, витоків даних та фішингу з використанням штучного інтелекту в банківській сфері, телекомунікаціях та критичній інфраструктурі. Експерти попереджають, що ці загрози становлять ризик як для фінансової стабільності, так і для IT-сектору. Незважаючи на офіційну структуру, очолювану NITDA та Національним координаційним центром з кібербезпеки під керівництвом Радника з національної безпеки, кількість та складність інцидентів зростає, оскільки злочинці впроваджують автоматизацію та штучний інтелект швидше, ніж багато організацій можуть модернізувати свої системи захисту…

Серйозний дефіцит кваліфікованих кадрів — за оцінками, до 2024 року буде потрібно понад 15 000 додаткових фахівців — стимулював активність приватного сектора в сфері послуг безпеки (наприклад, Layer3, Digital Encode, Cyberfleet) та навчання (NIIT, Utiva, New Horizons, Fibertrain), тоді як дослідження Абайомі Тітілола Олутімехіна показує, що лише дотримання нормативних вимог не запобігає атакам, і закликає до впровадження програм на основі розвідки та ширшого використання штучного інтелекту для виявлення та управління ризиками… Вразливість є гострою проблемою в децентралізованих фінансах, де зловживання смарт-контрактами та атаки з використанням флеш-позик підкреслюють необхідність ретельних аудитів та стандартів безпеки, передбачених на етапі проектування. Аналітики дійшли висновку, що стійкість Нігерії буде залежати від більш суворого дотримання політики, прискореного розвитку навичок та більш адаптивних, інтелектуальних засобів захисту, що відповідають мінливому ландшафту загроз». ***(Chisom Michael. Expert warns as cyber threats rise, skills gap widens in Nigeria // BUSINESSDAY MEDIA LTD (https://businessday.ng/news/article/expert-warns-as-cyber-threats-rise-skills-gap-widens-in-nigeria/). 07.02.2026).***

***

«Ринок кібербезпеки Марокко переходить у фазу сталого зростання, що зумовлено стратегією країни «Цифрове Марокко 2030», посиленням регулювання та підвищенням обізнаності про кіберризики. Mordor Intelligence оцінює вартість цього сектору в 144,6 млн доларів США у 2025 році і прогнозує його зростання з 157,1 млн доларів США у 2026 році до 238,1 млн доларів США у 2031 році, що відповідає середньорічному темпу зростання (CAGR) на рівні 8,67% у період з 2026 по 2031 рік… Digital Morocco 2030 має на меті позиціонувати Марокко як панафриканський цифровий хаб завдяки безпечному підключенню, впровадженню гібридної хмари та захисту критичної інфраструктури, а також безпечним цифровим посвідченням особи в масштабах країни та створенню 240 000 робочих місць у сфері технологій. Перші пілотні проекти в Касабланці, Рабаті та Марракеші свідчать про те, що управління ідентифікацією та доступом, управління хмарними ключами та моніторинг відповідності стануть основними складовими безпеки…

У 2025 році «рішення» з кібербезпеки (такі як брандмауери та інструменти ідентифікації) принесли 63,5% доходу ринку, але очікується, що найшвидше зростатимуть послуги з управління безпекою (15,23% CAGR), оскільки організації передають моніторинг, виявлення та реагування на інциденти на аутсорсинг. Розгортання хмарних технологій також прискорюється (17,42% CAGR), що відображає широке впровадження гібридних хмар; за прогнозами, до 2031 року лише витрати на хмарні засоби безпеки досягнуть близько 84,6 млн доларів США. Наразі великі підприємства домінують у витратах (71,8% ринку в 2025 році), хоча малі та середні підприємства розширюються швидше (15,67% CAGR). За секторами лідирують банківські та фінансові послуги (25,1% доходу в 2025 році) через суворі вимоги до дотримання нормативних вимог, тоді як найшвидше зростає вертикальний ринок охорони здоров'я (16,74% CAGR), де витрати на кібербезпеку, як очікується, зростуть з 12,45 млн доларів США в 2026 році до 26,9 млн доларів США до 2031 року в міру розширення цифрових медичних послуг та підвищення важливості безпеки даних пацієнтів». ***(Hanane Afeznaoui. Mordor Intelligence: Morocco's Cybersecurity Market to Reach $238 Million by 2031 // Morocco World News (https://www.moroccoworldnews.com/2026/02/280890/mordor-intelligence-moroccos-cybersecurity-market-to-reach-238-million-by-2031/). 26.02.2026).***

***

«Адміністрація з безпеки інформаційних мереж (INSA) Ефіопії випустила термінове попередження про широкомасштабну та складну кібератаку, спрямовану на користувачів WhatsApp, в якій зловмисники використовують поточні сьомі загальні вибори в країні. За даними INSA, зловмисники використовують оманливі повідомлення, замасковані під логотипи політичних партій, такі як «Висловіть свою підтримку нашій партії, натиснувши на це посилання», щоб спонукати жертв натиснути на шкідливі посилання, які надають інформацію про виборчі дільниці або попередні результати. Кампанія націлена в першу чергу на високопоставлених урядовців, впливових громадських діячів та студентів…

Агентство також наголосило на небезпеці «серійного хакерства та крадіжки особистих даних», коли зловмисники захоплюють акаунти надійних контактів, а потім вимагають гроші від їхніх контактів, часто посилаючись на вигадані надзвичайні ситуації. Студенти стають жертвами посилань, замаскованих під офіційні повідомлення університету, з метою збору особистих даних. Поширеною тактикою є спроба зловмисників зареєструвати акаунт WhatsApp жертви на іншому пристрої, а потім обманом змусити користувача поділитися шестизначним кодом підтвердження, надісланим SMS-повідомленням. INSA настійно рекомендує громадськості увімкнути двоступеневу верифікацію, ніколи не ділитися кодами підтвердження, уникати підозрілих посилань і перевіряти фінансові запити за допомогою прямих телефонних дзвінків. Це попередження з'явилося після того, як INSA раніше повідомило, що запобігло 97,8% з 13 443 спроб кібератак, зареєстрованих проти установ у першому кварталі поточного ефіопського бюджетного року». ***(Ethiopia: INSA Warns of Widespread Whatsapp Cyberattacks***

Exploiting Seventh General Election // AllAfrica (https://allafrica.com/stories/202602270614.html). 27.02.2026).

***

Кіберстрахування

«Компанія APA Insurance випустила комплексний продукт кіберстрахування для кенійських підприємств у відповідь на приголомшливий 441% стрибок кіберзагроз, зафіксований Управлінням зв'язку Кенії наприкінці 2025 року. Нова страховка призначена для великих корпорацій та малих і середніх підприємств і захищає від ризиків, що варіюються від програм-вимагачів і витоку даних до операційних збоїв та зловживань з боку інсайдерів… Генеральний директор Ашок Шах підкреслив, що поліс виходить за межі фінансової компенсації, пропонуючи комплексну систему підтримки, що включає команди реагування на інциденти, кризові комунікації, юридичні консультації та IT-фахівців для розслідування атак і відновлення даних, з метою допомогти клієнтам уникнути виплати викупу…

Цей запуск відбувається в той час, коли кенійські компанії стикаються з ескалацією атак, включаючи одинадцятикратне зростання кількості інцидентів DDoS, що обумовлено швидким впровадженням цифрових технологій, слабким внутрішнім контролем безпеки та все більш широким використанням штучного інтелекту хакерами. Хоча експерти попереджають, що страхування має супроводжуватися підвищенням рівня обізнаності з питань безпеки, страхові компанії, такі як Aon Kenya, Britam і Zamara, роблять ставку на кіберстрахування як на основний сегмент зростання, а APA навіть вивчає майбутні плани щодо захисту індивідуальних мобільних телефонів». ***(Dennis Musau. APA joins race for cyber insurance market as digital risks mount // Nation Media Group (https://www.businessdailyafrica.com/bd/corporate/technology/apa-race-for-cyber-insurance-market-as-digital-risks-mount-5370420). 24.02.2026).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«За даними нового звіту Palo Alto Networks, протягом минулого року азіатська кібершпигунська група, пов'язана з державою, провела масштабну глобальну хакерську кампанію, в результаті якої було скомпрометовано критичну інфраструктуру 37 іноземних урядів. Основними цілями були урядові відомства та міністерства, пов'язані з торгівлею, природними ресурсами, прикордонним контролем і дипломатією, а також парламенти та національні поліцейські організації. Кампанія, яка отримала назву «Shadow Campaigns», розпочалася в січні 2024 року і вважається найбільшою державною операцією з кібершпигунства з часу злом SolarWinds у 2020 році…

Головною мотивацією було шпигунство: хакери прагнули отримати доступ до конфіденційної електронної кореспонденції та внутрішніх урядових даних. Діяльність групи була вперше виявлена під час фішингових атак на європейські уряди, а подальше розслідування виявило широку, триваючу операцію. Хоча в звіті не вказано конкретну країну, такі докази, як мовні налаштування, регіональні інструменти та цільові активи, свідчать про те, що група діє з Азії, а деякі інциденти збігаються з подіями, що мають регіональний політичний інтерес, наприклад, посилення атак на Чеську Республіку після зустрічі її президента з Далай-ламою.

Серед постраждалих країн – Мексика, Бразилія, Німеччина, Італія, Індія, Індонезія, Японія, Монголія та кілька інших, загалом було скомпрометовано 70 державних організацій. Серед найвідоміших інцидентів – атаки на Міністерство гірничої промисловості та енергетики Бразилії, ймовірно пов'язані з рідкісними мінеральними ресурсами, та на міністерства Мексики у зв'язку з глобальними торговельними угодами. Кампанія також активізувала зусилля проти європейських країн, зокрема Німеччини та Чехії, і була спрямована на урядову інфраструктуру Гондурасу безпосередньо перед національними виборами.

Уряд США не постраждав, але Агентство з кібербезпеки та безпеки інфраструктури (CISA) співпрацює з партнерами для усунення вразливостей. Масштаби, методи та цілі «тіньових кампаній» підкреслюють зростаючу загрозу та потенційні довгострокові наслідки для національної безпеки та основних державних служб у всьому світі…» ***(Brendan Rascius. Asian cyber-spy group breached 37 foreign governments as US works to patch vulnerabilities across agencies: report // Independent (https://www.independent.co.uk/news/world/americas/us-politics/asian-cyber-hackers-37-nations-b2914693.html). 05.02.2026).***

***

«Російські хакери, підтримувані державою, відомі як APT28 (також називаються Fancy Bear, Sednit, Forest Blizzard і Sofacy), швидко скористалися критичною вразливістю Microsoft Office (CVE-2026-21509) менш ніж через 48 годин після випуску Microsoft екстреного патча. Група провела реверс-інжиніринг оновлення, щоб розробити просунутий експлойт, націлений на дипломатичні, морські та транспортні організації щонайменше в дев'яти країнах, переважно в Східній Європі, а також в ОАЕ та Болівії…

Кампанія, яка розпочалася 28 січня 2026 року, використовувала фішингові електронні листи, надіслані з раніше зламаних урядових облікових записів, завдяки чому приманки виглядали знайомими та надійними. Ланцюжок зараження був дуже складним і прихованим: експлойти та корисні навантаження були зашифровані, працювали повністю в пам'яті та використовували надійні канали, такі як HTTPS, для хмарних служб і законних потоків електронної пошти, щоб уникнути виявлення. Кампанія доставила два нових імплантати-бекдори, BeardShell і NotDoor.

BeardShell забезпечував повну розвідку системи, стійкість за допомогою введення процесів у Windows svchost.exe та поперечне переміщення в мережах, не залишаючи слідів на диску. NotDoor, що постачався як макрос VBA після

вимкнення захисту макросів Outlook, відстежував та викрадав дані електронної пошти, об'єднуючи повідомлення у файли .msg та надсилаючи їх на хмарні облікові записи, контрольовані зловмисниками, одночасно видаляючи докази з папок «Надіслано»…

Компанія Trellix, яка проаналізувала цю кампанію, з високою впевненістю приписала її APT28, зазначивши історію кібершпигунства та передових методів роботи цієї групи, включаючи багатоступеневе шкідливе програмне забезпечення, заплутування та зловживання хмарними сервісами. Ця кампанія підкреслює, як швидко державні суб'єкти можуть використовувати нові вразливості, скорочуючи час, необхідний захисникам для виправлення систем, та підкреслюючи необхідність швидких, проактивних заходів з кібербезпеки. Trellix опублікувала індикатори компрометації, щоб допомогти організаціям оцінити свою вразливість». ***(Dan Goodin. Microsoft releases urgent Office patch. Russian-state hackers pounce // Condé Nast (https://arstechnica.com/security/2026/02/russian-state-hackers-exploit-office-vulnerability-to-infect-computers/). 05.02.2026).***

***

«Міністр закордонних справ Італії Антоніо Таяні оголосив у Вашингтоні, що італійські спецслужби успішно запобігли серії кібератак російського походження, спрямованих проти офісів Міністерства закордонних справ, зокрема у Вашингтоні, та кількох об'єктів Зимових Олімпійських ігор, таких як готелі в Кортіні. Ці спроби атак відбуваються на тлі посилення занепокоєння, оскільки минулі Олімпійські ігри в Парижі (2024) і Пхьончхані (2018) також стикалися з кіберзагрозами, які широко приписують російським суб'єктам і які часто розглядають як помсту за заборону Росії брати участь в іграх через допінг і війну в Україні…

Зимові Олімпійські ігри 2026 року, які пройдуть у Мілані та Кортіна-д'Ампеццо з 6 по 22 лютого, як очікується, привернуть 2 мільйони відвідувачів, у тому числі 60 000 на церемонії відкриття, на якій буде присутній віце-президент США Джей Ді Венс. Заходи безпеки будуть масштабними: центр Мілана стане «червоною зоною», закритою для руху транспорту, з посиленими перевірками на кордонах і залізничних станціях, регулярними обшуками на наявність вибухівки та снайперами, розміщеними на ключових об'єктах. Близько 6000 поліцейських і 2000 військовослужбовців, оснащених технікою, дронами та літаками, забезпечуватимуть безпеку в регіоні під координацією цілодобової Олімпійської оперативної кімнати в Римі.

Ця подія також супроводжується суперечками щодо присутності агентів Імміграційної та митної служби США (ICE), які, як стверджують італійські чиновники, виконують лише консультативні функції, а також запланованими протестами з різних питань, від екологічних проблем до участі Ізраїлю. Центральне місце займає міжнародне співробітництво, в якому беруть участь Інтерпол, Європол та іноземні поліцейські сили, що займаються обміном інформацією та кризовим управлінням. Незважаючи на кіберзагрози та складну ситуацію з безпекою, італійські власті наголошують на необхідності активних, скоординованих зусиль для забезпечення безпеки та цілісності ігор…» ***(Jon***

Shelton. Italy says it has foiled Russian Olympic cyberattacks // Deutsche Welle (https://www.dw.com/en/italy-says-it-has-foiled-russian-olympic-cyberattacks/a-75809776). 04.02.2026).

***

«Нещодавно створений російський хакерський альянс «Російський легіон» розпочав скоординовану кампанію кібератак проти Данії, націлену на критичну інфраструктуру та державні служби. Альянс, до якого входять такі групи, як Cardinal, The White Pulse, Russian Partizan та Inteid, публічно оголосив про своє створення 27 січня 2026 року, що ознаменувало значне посилення діяльності хактивістів, пов'язаних з державою, проти західних країн…

Кампанія під назвою «OpDenmark» розпочалася з розподілених атак типу «відмова в обслуговуванні» (DDoS), спрямованих на дезорганізацію роботи данських організацій та тиск на уряд з метою скасування запланованого пакету військової допомоги Україні на суму 1,5 млрд данських крон. Після висунення 48-годинного ультиматуму «Російський легіон» попередив, що DDoS-атаки — це лише початок, і погрожував більш серйозними кібероперaціями, якщо їхні вимоги не будуть виконані.

Після закінчення терміну кілька данських компаній та організацій державного сектору, особливо в енергетичній галузі, повідомили про перебої в роботі послуг. Аналітики Truesec визначили Russian Legion як пов'язану з державою, але незалежно діючу загрозу, що представляє скоординовані зусилля відомих хактивістських груп, спрямовані на посилення свого впливу за допомогою спільних кампаній. Ця схема відображає попередню кібердіяльність, пов'язану з Росією, під час міжнародних конфліктів, спрямовану на створення психологічного тиску та оперативних перебоїв…

Методика атак Russian Legion поєднує технічні порушення з психологічними операціями. Група використовує послуги DDoS-for-hire, щоб перевантажити мережі-мішені, починаючи з публічних погроз у Telegram, а потім проводячи атаки з невеликим впливом, щоб продемонструвати свої можливості. Потім вони публікують скріншоти уражених веб-сайтів, щоб викликати страх і привернути увагу ЗМІ, навіть якщо фактичний збиток є обмеженим. Психологічний компонент призначений для створення невизначеності серед громадян і тиску на осіб, що приймають рішення.

Хоча ці кампанії можуть спричинити тимчасові порушення, історичні дані свідчать, що організації з надійними захисними заходами, такими як обмеження швидкості, геоблокування та спеціалізований захист від DDoS-атак, можуть пом'якшити вплив і запобігти ескалації до катастрофічних наслідків». ***(Tushar Subhra Dutta. Russian Hacker Alliance Targeting Denmark in Large-Scale Cyberattack // Cyber Security News (https://cybersecuritynews.com/russian-hacker-alliance-targeting-denmark/). 02.02.2026).***

***

«Італія відбила серію кібератак, спрямованих на деякі офіси її Міністерства закордонних справ, зокрема одне у Вашингтоні, а також на веб-

сайти та готелі Зимових Олімпійських ігор у Кортіна-д'Ампеццо, заявив у середу міністр закордонних справ Антоніо Таяні.

Спілкуючись із журналістами під час поїздки до столиці США, Таяні заявив, що спроби нападів були «російського походження», але не надав додаткових подробиць.

«Ми запобігли серії кібератак на сайти міністерств закордонних справ, починаючи з Вашингтона, а також стосувалися деяких об'єктів Зимових Олімпійських ігор, зокрема готелів у Кортіні», – сказав Таяні лише за два дні до п'ятничної церемонії відкриття на стадіоні «Сан-Сіро» в Мілані.

Зимові Олімпійські ігри розпочалися в середу першими матчами з керлінгу в Кортіні.

Міністр внутрішніх справ Італії Маттео П'янтедозі заявив у середу парламенту, що на території проведення Ігор, яка простягається від Мілана до Доломітових Альп, розміщено 6000 співробітників служби безпеки, включаючи експертів зі знешкодження бомб, снайперів та антитерористичних підрозділів». ***(Italy averted Russian-linked cyberattacks targeting Winter Olympics websites, foreign minister says // Associated Newspapers Limited (https://www.dailymail.co.uk/wires/ap/article-15528863/Italy-averted-Russian-linked-cyberattacks-targeting-Winter-Olympics-websites-foreign-minister-says.html). 04.02.2026).***

***

«Індійська стартап-сцена, особливо молоді компанії, що розробляють інструменти кібербезпеки або розвідки для правоохоронних органів, стала останньою мішенню пакистанської групи APT36 (Transparent Tribe). Ця група, що діє з 2013 року, переключилася зі своїх звичайних жертв у сфері уряду та оборони на підприємницький сектор, заманюючи співробітників за допомогою фішингових листів із вкладенням ISO-файлу під назвою MeetBisht.iso. Усередині контейнера ярлик, замаскований під аркуш Excel, запускає пакетний скрипт, який показує нешкідливий документ-приманку, одночасно тихо встановлюючи Crimson RAT. Скрипт пригнічує попередження безпеки, розміщує шкідливе програмне забезпечення в надійному шляху AppData під випадковим ім'ям, а потім запускає його… Crimson RAT — штучно «роздутий» до 34 МБ для уникнення сканерів сигнатур, наповнений випадковими іменами функцій і пов'язаний з жорстко закодованими серверами C2 на незвичайних TCP-портах (18661, 20856, 26868, 29261, 36628) — надає зловмисникам повний віддалений контроль: перегляд екрану, запис аудіо, крадіжку файлів і маніпулювання системою. Фішингові приманки є переконливими, оскільки вони запозичують реальні біографічні дані індійського засновника, а інфляція сміттєвих даних шкідливого програмного забезпечення та ланцюжок виконання на основі PowerShell допомагають йому обійти звичайні засоби захисту. Аналітики з безпеки рекомендують блокувати вкладення файлів-контейнерів від невідомих відправників, проводити навчання користувачів з питань безпеки, розгортати інструменти для кінцевих точок, які позначають підозрілі зміни в PowerShell або файловій системі, а також контролювати вихідний трафік до нестандартних портів RAT, одночасно

оновлюючи канали інформації про загрози, що містять перелік інфраструктури C2 Transparent Tribe…» ***(Tushar Subhra Dutta. Transparent Tribe Hacker Group Attacking India's Startup Ecosystem // Cyber Security News (https://cybersecuritynews.com/transparent-tribe-hacker-group/). 06.02.2026).***

***

«Польща заборонила в'їзд автомобілів китайського виробництва на військові об'єкти через побоювання, що вбудовані датчики можуть збирати конфіденційні дані. Польська армія також забороняє підключати службові телефони до інформаційно-розважальних систем у китайських автомобілях. Ці обмеження застосовуються до захищених об'єктів, але не до загальнодоступних місць, таких як лікарні, клініки, бібліотеки, прокуратури або гарнізонні клуби…

Транспортні засоби можуть бути допущені до в'їзду, якщо певні функції будуть вимкнені та будуть вжиті інші заходи безпеки, характерні для конкретного об'єкта. Армія описала ці заходи як запобіжні, що відповідають практиці союзників по NATO щодо дотримання високих стандартів захисту оборонної інфраструктури». ***(Poland bars Chinese-made cars from military sites over data security fears // Reuters (https://www.reuters.com/business/aerospace-defense/poland-bars-chinese-made-cars-military-sites-over-data-security-fears-2026-02-18/). 18.02.2026).***

***

«…Сучасні конфлікти все частіше розгортаються на цифровому полі бою, де актори, пов'язані з національними державами, націлюються на цивільну інфраструктуру — лікарні, енергетику, транспорт і комунікації — щоб без єдиного пострілу порушити військову реакцію, громадський порядок і роботу основних служб. Кібертактика еволюціонувала від шпигунства до використання вразливостей програмного забезпечення, ланцюгів постачання та соціальної інженерії, а взаємопов'язаність критичних систем перетворює окремі слабкі місця на ланцюжок каскадних збоїв…

Глобальне поширення відбувається швидко і без розбору, як це було видно під час атаки NotPetya у 2017 році, яка перетнула кордони і паралізувала транспорт, виробництво та роздрібну торгівлю, довівши, що будь-яка організація, пов'язана з глобальними ланцюгами поставок, знаходиться в зоні ураження. Звичайні громадяни також є мішенями: дезінформація підриває довіру, а фішинг, який використовується як зброя, збирає облікові дані, а агреговані особисті дані дозволяють маніпулювати впливовими особами… Цей системний ризик створює навантаження на кіберстрахування, де традиційні поліси, які часто виключають військові дії, не можуть покрити одночасні міжгалузеві збитки, що призводить до суперечливих спорів щодо страхового покриття саме тоді, коли підтримка є найбільш необхідною. У відповідь на це, аналіз загроз повинен стати пріоритетом керівництва, а не функцією бек-офісу: організації повинні виявляти нові загрози на ранній стадії, інтерпретувати їх у геополітичному контексті та перетворювати отримані відомості на дії — виправлення, посилення аутентифікації та відпрацювання реагування на інциденти…

Оскільки військові дії тепер поширюються на центри обробки даних, соціальні платформи та мережі, що лежать в основі економіки, питання полягає не в тому, чи торкнеться кіберконфлікт організацію, а в тому, коли це станеться; стійкість буде залежати від того, наскільки рішуче лідери готуються, керують і діють напередодні наступного удару». ***(Andrew Martin. Threat Intelligence in the Heat of Cyber Warfare // Cyber Defense Media Group (https://www.cyberdefensemagazine.com/threat-intelligence-in-the-heat-of-cyber-warfare/). 18.02.2026).***

***

«Нове опитування POLITICO, проведене в США, Канаді, Франції, Німеччині та Великій Британії, виявило значну розбіжність між громадською думкою та обережною позицією урядів країн NATO щодо гібридної війни. Більшість респондентів у всіх п'яти країнах вважають серйозні кібератаки, такі як відключення лікарень або електромереж, а також саботаж підводних кабелів або енергетичних трубопроводів, актами війни. Найбільш рішуче налаштовані канадці: 73% з них вважають кібератаки на лікарні актами війни…

Незважаючи на зростання кількості інцидентів, що підтримуються державою, включаючи пов'язані з Росією атаки програм-вимагачів на системи охорони здоров'я США, фатальну кібератаку на британську службу охорони здоров'я (NHS) та іранські спроби атаки на Бостонську дитячу лікарню, союзники по NATO як і раніше не бажають застосовувати статтю 5 щодо кібератак, залишаючи поріг для колективної реакції нечітким. Опитування відображає зростаюче розчарування громадськості цією стриманістю, особливо в Європі, де більшість у Німеччині, Франції та Великій Британії вважають Росію головною глобальною загрозою…

Хоча дрібніші цифрові диверсії, такі як витік розмов лідерів або втручання у вибори, рідше розглядаються як війна, респонденти з усіх країн сходяться на думці, що кібербезпека, штучний інтелект і традиційна військова сила однаково важливі для національної оборони, причому щонайменше третина респондентів у кожній країні вважає кібербезпеку одним із найвищих пріоритетів у сфері оборонних витрат. Результати дослідження підкреслюють чітку вимогу громадськості щодо більш рішучої кіберполітики, включаючи наступальні можливості, оскільки уряди від США до Німеччини сигналізують про перехід до проактивної кіберзахисту в умовах ескалації гібридних загроз». ***(Maggie Miller, Dana Nickel and Antoaneta Roussi. Top NATO allies believe cyberattacks on hospitals are an act of war. They're still struggling to fight back // POLITICO LLC (https://www.politico.com/news/2026/02/21/poll-us-nato-cyber-warfare-00789496). 21.02.2026).***

***

«Низка гренландських веб-сайтів зараз стикається з розподіленою атакою типу «відмова в обслуговуванні» (DDoS), повідомили в п'ятницю місцеві ЗМІ з посиланням на дані данської влади.

Датське агентство соціального забезпечення заявило, що йому відомо про DDoS-атаки, спрямовані на гренландські веб-сайти.

«Ми уважно стежимо за ситуацією та ведемо постійний діалог з відповідними органами влади Данії та Гренландії щодо поточних атак», – повідомило агентство телекомпанії DR, підтверджуючи кібератаку.

Спираючись на інформацію, телекомпанія повідомила, що за атаками стоїть проросійське хакерське угруповання NoName057(16), нагадавши, що це ж угруповання здійснило масовані атаки на веб-сайти данських муніципалітетів та міністерств під час муніципальних виборів у листопаді.

Служба оборонної розвідки Данії (DE) вважає групу пов'язаною з російською державою». ***(Burak Bir. Several Greenlandic websites hit by cyberattack, Danish authority confirms // Anadolu Ajansı (https://www.aa.com.tr/en/europe/several-greenlandic-websites-hit-by-cyberattack-danish-authority-confirms/3835969). 21.02.2026).***

***

«Російська державна хакерська група APT28 (також відома як Fancy Bear) розпочала нову шпигунську кампанію під назвою Operation MacroMaze, яка триватиме з вересня 2025 року до січня 2026 року і спрямована проти організацій у Західній та Центральній Європі. За даними команди LAB52 іспанської компанії з кібербезпеки S2 Grupo, кампанія базується на не надто складних, але дуже прихованих інструментах, які використовують легальні сервіси для управління та викрадення даних…

Атака починається з фішингових електронних листів, що містять шкідливі документи Word, які використовують поле INCLUDEPICTURE, що вказує на віддалене зображення, розміщене на webhook[.]site. При відкритті документ автоматично завантажує зображення, яке діє як піксель відстеження, повідомляючи зловмиснику про успішність приманки. Вбудовані макроси потім скидають багатоступеневий корисний вантаж: VBScript запускає пакетний файл, який встановлює стійкість за допомогою запланованих завдань, відтворює невеликий корисний вантаж HTML, закодований у Base64, у Microsoft Edge (у режимі без головки або з вікном, переміщеним за межі екрана), отримує команди з кінцевої точки webhook зловмисника, виконує їх і непомітно виводить результат у вигляді HTML-файлу…

З часом макроси еволюціонували, щоб поліпшити ухилення — перейшовши від виконання безголовного браузера до імітації клавіатури (SendKeys) для обходу запитів безпеки та агресивного припинення інших процесів Edge. Використовуючи повсякденні мови сценаріїв, легітимні служби веб-хуків та стандартні функції браузера, APT28 мінімізує виявні артефакти, зберігаючи надійне дистанційне керування та крадіжку даних. Кампанія демонструє, що складних результатів можна досягти за допомогою навмисно простих інструментів з низьким рівнем розпізнавання, ретельно організованих для прихованого функціонування». ***(Ravie Lakshmanan. APT28 Targeted European Entities Using Webhook-Based Macro Malware // The Hacker News (https://thehackernews.com/2026/02/apt28-targeted-european-entities-using.html). 23.02.2026).***

***

«Служба електронної безпеки Азербайджану (ESS) успішно перехопила та нейтралізувала серію кібератак, спрямованих як на урядові, так і на приватні організації. Влада підтвердила, що атаки були організовані хакерською групою «Narketing163», яка використовувала методи соціальної інженерії для психологічного маніпулювання одержувачами. Група надсилала шкідливі електронні листи, замасковані під офіційну кореспонденцію від відомих компаній, намагаючись обдурити користувачів і змусити їх відкрити шкідливі вкладення. Частина шкідливого програмного забезпечення поширювалася через веб-сайт, що використовував домен країни .az. Технічний аналіз показав, що група раніше проводила подібні операції, але ESS швидко ідентифікувала підозрілий домен і вжила заходів для блокування подальшого поширення шкідливих файлів…» ***(Aghakazim Guliyev. Azerbaijan blocks "Narketing163" cyberattack on govt, private networks // Caliber (https://caliber.az/en/post/azerbaijan-blocks-narketing163-cyberattack-on-govt-private-networks). 27.02.2026).***

***

«У суботу, 28 лютого 2026 року, в рамках операції «Roar of the Lion» було завдано військових ударів по командних центрах IRGC (Корпус вартових ісламської революції), після чого, за повідомленнями, Іран опинився в майже повній цифровій імлі через масштабну і безпрецедентну кібератаку. Атака паралізувала критичну інфраструктуру, офіційні новинні сайти та комунікації служб безпеки, що призвело до повного відключення комунікацій іранського керівництва. NetBlocks підтвердив, що інтернет-з'єднання в Ірані впало до лише 4% від нормального рівня, що свідчить про майже повне відключення по всій країні. Пропагандистські органи режиму також стали мішенню атаки: веб-сайт IRNA (Агенція новин Ісламської республіки) був відключений, а пов'язане з IRGC інформаційне агентство Tasnim зазнало серйозних збоїв і хакерських атак, в результаті яких, як повідомляється, були опубліковані підривні повідомлення проти Верховного лідера…

Західні розвідувальні джерела вказали, що основною метою атаки було пошкодження комунікаційної інфраструктури IRGC, щоб запобігти координації контратак і запуску дронів або балістичних ракет. Атака була комплексна і поєднувала електронну війну, яка порушила навігацію та комунікації, з атаками типу «відмова в обслуговуванні» (DDoS) і глибоким вторгненням у системи даних, пов'язані з енергетичною та авіаційною інфраструктурою Ірану. Навіть ізольована мережа «національного інтернету» режиму, як повідомляється, не витримала тиску комбінованої атаки. Ця масштабна операція була описана як кульмінація кампанії, що розпочалася в січні з хакерських атак на урядові супутникові трансляції, що залишило Іран цифровим чином вразливим та ізольованим у момент гострої кризи». ***(ITAY GAL. Israel plunges Iran into darkness with largest cyberattack in history during attack against Iran // Jpost Inc. (https://www.jpost.com/israel-news/defense-news/article-888271). 28.02.2026).***

***

«Згідно з доповіддю Radware «Глобальні кіберзагрози 2026», минулого року Ізраїль був країною, яка найбільше постраждала від кібератак на геополітичному ґрунті, прийнявши на себе 12,2% всіх таких атак у світі. Доповідь свідчить про різке зростання цифрових воєнних дій, зокрема про приголомшливий 168-відсотковий стрибок атак типу «розподілена відмова в обслуговуванні» (DDoS) на рівні мережі та 120-відсоткове зростання атак на рівні додатків. Ідеологічно мотивовані групи, які взяли на себе відповідальність за близько 16 000 унікальних атак на Telegram, проводили тривалі кампанії протягом 2025 року, що зробило кібератаки щоденним явищем для багатьох ізраїльських організацій, включаючи урядові веб-сайти та критичну інфраструктуру…

Radware визначила рівень додатків, на якому працюють веб-сайти та API, як «головне поле бою» через прямий вплив на бізнес-операції. Найбільше постраждали такі сектори, як технології, телекомунікації та фінанси, де багато атак тривали менше хвилини, що робило їх виявлення вручну практично неможливим. Зловмисна діяльність ботів також зросла на 92% завдяки доступності генеративних інструментів штучного інтелекту, які дозволяють зловмисникам з обмеженими ресурсами запускати великомасштабні автоматизовані кампанії. Віцепрезидент Radware з питань аналізу загроз Рон Мейран попередив, що зловмисники поєднують автоматизацію, штучний інтелект і багатовекторні стратегії, змушуючи організації впроваджувати автоматизовані засоби захисту, здатні реагувати за лічені секунди. Компанія очікує, що ці тенденції збережуться і будуть формувати глобальне операційне середовище протягом найближчих років». ***(ANNA AHRONHEIM. Israel was world's top target for geopolitical cyberattacks in 2025, report finds // Jpost Inc. (https://www.jpost.com/israel-news/article-887255). 19.02.2026).***

***

Кіберзахист критичної інфраструктури

«Глобальний ринок кібербезпеки в авіації має подвоїтися протягом наступних восьми років, зростаючи з приблизно 10,8 млрд доларів США у 2025 році до близько 22,9 млрд доларів США до 2034 року, із прогнозованим середньорічним темпом зростання 8,7%. Таке стрімке зростання зумовлене триваючою цифровою трансформацією авіаційної галузі, яка збільшила площу атаки через підключені салони, цифрові двійники, біометричні потоки пасажирів та широке впровадження хмарних і периферійних послуг.

Послуги з кібербезпеки зараз є необхідними для захисту літаків, авіакомпаній, роботи аеропортів та екосистеми пасажирів, яка містить великий обсяг даних. Зростання кількості атак на операційні технології (OT), такі як пристрої, підключені до воріт, багажу, систем заправки паливом та електропостачання, спонукало сектор перейти від традиційних засобів захисту периметра до архітектур, що передбачають порушення безпеки, нульову довіру, постійний моніторинг та стратегії відновлення стійкості…

Кодифікація нормативних актів є ще одним ключовим фактором зростання, оскільки органи влади перетворюють рекомендації з кібербезпеки на обов'язкові вимоги до проектування та експлуатації, прискорюючи затвердження бюджетів та нагляд на рівні правління в авіакомпаніях та операторах аеропортів.

У регіональному розрізі Північна Америка лідирує за витратами на кібербезпеку завдяки великим паркам повітряних суден, щільним хабам та ранньому впровадженню вимог FAA та TSA. Європа просуває гармонізацію та закупівлі через програми EASA та Eurocontrol, тоді як Азіатсько-Тихоокеанський регіон є найшвидше зростаючим регіоном, де розширюються парки повітряних суден, а нові аеропорти впроваджують моделі нульової довіри та пріоритету хмарних технологій. Близький Схід інвестує значні кошти в мегахаби, а Латинська Америка зосереджується на модернізації центрів безпеки та управлінні ризиками третіх сторін.

Глобальні ініціативи ICAO допомагають узгодити базові вимоги до кібербезпеки в різних регіонах, хоча рівень зрілості залишається нерівномірним. Загалом, зростання ринку відображає зростаючу залежність авіаційної галузі від цифрових систем та нагальну потребу в надійних, адаптивних заходах кібербезпеки…» ***(Matthew Wilson. Global aviation cybersecurity market predicted to double to USD 22.9 billion // Regional Gateway (https://www.regionalgateway.net/global-aviation-cybersecurity-market-predicted-to-double-to-usd-22-9-billion/). 05.02.2026).***

***

«…Європейське агентство з безпеки авіації (EASA) запровадило комплексну систему інформаційної безпеки, відому як Part-IS, щоб вирішити проблему зростаючої вразливості авіаційної галузі до кіберзагроз в умовах швидкої цифрової трансформації. Складаючись з Делегованого регламенту (ЄС) 2022/1645 та Імплементаційного регламенту (ЄС) 2023/203, Part-IS зобов'язує майже всі суб'єкти цивільної авіації ЄС — від операторів аеродромів та організацій з технічного обслуговування до постачальників аеронавігаційних послуг — впровадити структуровану систему управління інформаційною безпекою (ISMS), пропорційну їхньому ризику. Регламенти набирають чинності з 16 жовтня 2025 року або 22 лютого 2026 року, залежно від типу суб'єкта, з додатковим 18-місячним пільговим періодом для досягнення повної операційної відповідності…

Основні зобов'язання включають виявлення та зменшення ризиків, встановлення чіткого управління та підзвітності, забезпечення виявлення та повідомлення про інциденти, а також управління вразливими місцями в ланцюжку поставок. Дотримання вимог контролюється EASA та національними органами влади, а за недотримання передбачені штрафи у розмірі до 4% річного обороту або анулювання сертифіката. Важливо, що дотримання вимог Part-IS не звільняє організації від виконання Директиви ЄС NIS 2, якщо вони підпадають під її дію. Ця зміна в законодавстві підносить кібербезпеку з рівня IT-проблеми до рівня основної вимоги безпеки, що вимагає від зацікавлених сторін в авіації узгодити своє управління, переглянути контракти з постачальниками та прийняти модель зрілості «Наявна, Придатна, Оперативна, Ефективна» (PSOE) для захисту критичної

інфраструктури…» ***(Ozan Akyurek, Nicolas Brice, Dean E. Griffith, Olivier Haas, Holger Neumann and Mauricio F. Paez. Civil Aviation Cybersecurity: EASA Part-IS Sets New Information Security Obligations // Jones Day (https://www.jonesday.com/en/insights/2026/02/civil-aviation-cybersecurity-easa-partis-sets-new-information-security-obligations). 03.02.2026).***

***

«Північноамериканські супутникові системи стають все більш вразливими, оскільки «наземний сегмент» є стратегічним вузьким місцем і часто найпростішим способом компрометації всієї супутникової групи, особливо з огляду на те, що тисячі нових супутників LEO, запущених з 2020 року, залежать від взаємопов'язаних наземних мереж. Цей ризик переважно створюють два основні суб'єкти загрози: висококваліфіковані противники «Tier 6», що підтримуються державою, про що свідчить збій у роботі Viasat у 2022 році, який стався через незахищені вразливості Fortinet VPN у наземній інфраструктурі, а не в супутниках, та злочинні угруповання «Tier 5», які атакують комерційних операторів за допомогою програм-вимагачів. Перехід на комерційне готове обладнання ще більше знижує бар'єри, дозволяючи зловмисникам картографувати системи за допомогою відкритих досліджень та стандартних інструментів…

Наслідки порушення наземного контролю виходять за межі простоїв: перебої можуть підірвати легітимність уряду, підірвати довіру до критично важливих служб і створити інформаційний вакуум, який ворожі суб'єкти можуть використати для поширення дезінформації. З технічної точки зору, найбільший ризик становить «цілісність місії»: якщо зловмисники скомпрометують підсистему управління та обробки даних, вони можуть захопити контроль, змінити орбіти, вивести з ладу корисні навантаження або використовувати підробку телеметричних даних, щоб спонукати операторів виконати маневри, які назавжди знищать активи… Постійною проблемою є відсутність єдиних міжнародних норм регулювання космічної безпеки — на відміну від обов'язкової цифрової модернізації авіації — що робить цей сектор привабливим для шпигунства та крадіжки запатентованих технологій. Ставки посилюються залежністю від синхронізації GNSS/GPS; значне порушення може спричинити фінансові «раптові обвали», навіть незважаючи на те, що ця загроза стимулює швидке зростання ринку кібербезпеки в космосі, який, за прогнозами, до кінця 2026 року досягне близько 5,2 млрд доларів США, а також розширення співпраці через такі органи, як Space ISAC…

Прогнози передбачають, що в найближчому майбутньому програми-вимагачі будуть націлені на невеликі наземні станції (що в першу чергу призведе до витоку даних), в середньостроковій перспективі існує ризик використання державою незахищених VPN для шпигунства та крадіжки схем, а до 2027 року існує висока ймовірність серйозної системної несправності, якщо регуляторні та безпекові прогалини залишаться невирішеними, що потенційно може бути спровоковано атакою на сигнали точного часу з серйозними глобальними фінансовими наслідками». ***(Ana Moroșanu. Cybersecurity Vulnerabilities in North American Satellite Ground Segments // Bloomsbury Intelligence and Security CIC***

(https://bisi.org.uk/reports/cybersecurity-vulnerabilities-in-north-american-satellite-ground-segments). 23.02.2026).

***

«…Енергетична галузь, зокрема нафтогазовий сектор, стала головним об'єктом для кіберзлочинців: за останній рік кількість атак з використанням програм-вимагачів зросла майже на 1000%, а середня сума викупу подвоїлася у 2025 році. Ця вразливість зумовлена поєднанням застарілих систем, регуляторних викликів та широких площин атаки, які зараз експлуатуються бандами зловмисників, що використовують штучний інтелект для швидших і точніших атак. Інцидент з Colonial Pipeline у 2021 році є суворим нагадуванням про потенціал катастрофічних порушень, коли один скомпрометований обліковий запис VPN призвів до зупинки майже половини постачання палива на східному узбережжі США та виплати викупу в розмірі декількох мільйонів доларів…

Традиційні засоби кібербезпеки, які зазвичай зосереджуються на виявленні та реагуванні, виявляються недостатніми, оскільки зловмисники часто можуть обійти їх ще до того, як спрацює сигнал тривоги, що призводить до значних збитків, таких як витік даних або зупинка роботи. Morphisec пропонує принципово інший, превентивний підхід із запатентованою технологією Automated Moving Target Defense (AMTD). Замість того, щоб реагувати на загрози, Morphisec проактивно запобігає їм, постійно змінюючи пам'ять під час виконання, створюючи непередбачувану і постійно мінливу поверхню атаки, що унеможливлює виконання шкідливого програмного забезпечення…

Цей «цифровий засіб індивідуального захисту» діє як важлива система безпеки поряд з існуючими інструментами безпеки, зупиняючи просунуті варіанти програм-вимагачів, такі як LockBit і BlackCat, перш ніж вони можуть завдати шкоди, запобігаючи поширенню та не вимагаючи ручного налаштування. Оскільки програми-вимагачі розвиваються швидше, ніж традиційні засоби захисту, енергетичний сектор повинен перейти від реактивної до проактивної позиції в галузі кібербезпеки, ставлячи на перше місце профілактику, щоб захистити критичну інфраструктуру, забезпечити оперативну стійкість та зменшити ризики для бізнесу, пов'язані зі складними кіберзагрозами». ***(Mission-Critical Preemptive Cybersecurity in Oil and Gas: Key Insights for CISOs and Cybersecurity Professionals // Morphisec (https://www.morphisec.com/blog/mission-critical-preemptive-cybersecurity-in-oil-and-gas-key-insights-for-cisos-and-cybersecurity-professionals/). 26.02.2026).***

***

Кіберзахист виробничих об’єктів

«…Ще будучи аспірантами Університету Алабами в Хантсвіллі (UAH), Аарон Верт і Рішаб Дас перетворили свою дисертаційну роботу в Центрі досліджень і освіти в галузі кібербезпеки на два американські патенти, які зміцнюють промислові системи управління проти кібератак…

Патент Верта «Вбудована система запобігання вторгненням для промислових контролерів» оснащує програмований логічний контролер (PLC) вбудованим цифровим двійником, який швидко моделює вплив кожного вхідного мережевого пакета або завантаження логіки драбини. Якщо моделювання передбачає шкідливу поведінку, PLC блокує команду, перш ніж вона може пошкодити фізичний процес, яким вона керує, — будь то заводська лінія або частина електромережі. За словами Верта, завдання полягало в тому, щоб виявити шкідливий код, який виглядає цілком нормально; цифровий двійник «еврика» вирішив цю проблему після трьох років ітеративного проектування…

Патент Даса «Вбудована система виявлення вторгнень для промислових контролерів» додає захист типу «ройового розуму». Кожен контролер виконує локальний моніторинг, а потім обмінюється компактними, синхронізованими за часом зведеннями про безпеку зі своїми сусідами. Коли достатня кількість контролерів підтверджує аномалію, колектив надсилає операторам сигнал тривоги, забезпечуючи остаточну лінію захисту на пристрої. Створення точної синхронізації годинника та алгоритму виявлення в режимі реального часу, який міг би працювати на обмеженому апаратному забезпеченні, вимагало переписати тисячі рядків коду, але в кінцевому підсумку система виявила імітовану атаку на нафтовий термінал саме так, як і передбачалося…» ***(Two UAH CCRE Doctoral Researchers Secure Patents to Defend Against Sophisticated Cyber Attacks // Newswise, Inc (https://www.newswise.com/articles/two-uah-ccre-doctoral-researchers-secure-patents-to-defend-against-sophisticated-cyber-attacks). 06.02.2026).***

***

«Цифрова трансформація сприяє експоненційному зростанню вартості в гірничодобувній промисловості, де розвідка з використанням штучного інтелекту, цифрові двійники, автономні флоти та прогнозне технічне обслуговування забезпечують більш безпечну, ефективну та капіталоощадну діяльність. Однак ці досягнення також створюють значні кіберризики, оскільки інциденти можуть швидко поширюватися по взаємопов'язаній інфраструктурі, загрожуючи безпеці, виробництву та вартості підприємства…

Штучний інтелект змінює ландшафт загроз, трансформуючи як кібернапади, так і кіберзахист. Швидке впровадження агентного штучного інтелекту — автономних систем, що діють і взаємодіють — несе нові ризики, такі як можливість виконання зловмисних інструкцій зі швидкістю машини, що перетворює окремий злом на скоординовану атаку з декількома порушеннями. Кіберзлочинці можуть використовувати ці агенти, що призводить до витоку даних, перебоїв у роботі та навіть загроз безпеці, таких як неправильне маршрутизування автономних транспортних засобів або порушення блокування безпеки.

Державні суб'єкти все частіше націлюються на критично важливі мінерали та інфраструктуру, плануючи довгострокові операції, що варіюються від шпигунства до фінансування незаконної діяльності. Сучасні гірничодобувні підприємства також стикаються з вразливістю ланцюгів постачання, оскільки зловмисники використовують слабкі ланки серед виробників обладнання, постачальників програмного забезпечення та інтеграційних партнерів. Злиття та поглинання

додають додаткового ризику через спільні системи та непослідовні практики безпеки, що робить кібер-дуже важливим, як екологічні або фінансові оцінки…

Щоб вирішити ці проблеми, гірничодобувні компанії повинні узгодити технологічні амбіції з операційною реальністю та регуляторними очікуваннями. Моделі та агенти штучного інтелекту повинні розглядатися як критично важливі активи — ретельно інвентаризуватися, контролюватися за версіями, мати обмежений доступ та підлягати суворому контролю змін. Ефективне управління вимагає співпраці між операторами, виробниками оригінального обладнання, постачальниками даних, правоохоронними органами та регуляторними органами.

Транскордонні операції повинні відповідати численним законам про конфіденційність, кібербезпеку та галузевим законам, а також суворим строкам розкриття інформації. Після кіберінциденту здатність швидко і достовірно встановити, до яких даних було отримано доступ або які дані були викрадені, має вирішальне значення для реагування з точки зору нормативно-правового регулювання, законодавства та репутації. Незмінне ведення журналів, доступ на основі ролей, мінімізація даних та комплексне відображення даних є необхідними для готовності до судово-медичної експертизи та судових розглядів.

Плани реагування на інциденти повинні враховувати особливості штучного інтелекту та операційних технологій, передбачати чіткі повноваження щодо прийняття рішень, надійне управління ідентифікацією та регулярну звітність на рівні правління щодо управління штучним інтелектом та стійкості. Також важливе значення мають навчання протидії фейковим відео та соціальному інжинірингу на основі штучного інтелекту, а також інвестиції в підготовку до криміналістичних розслідувань.

Правління повинні мати відповідний нагляд за сайтом і розуміти, як працюють механізми управління ШІ та інформацією, включаючи те, як швидко можна ізолювати агентів ШІ та як їх використання фіксується в журналах. Кіберготовність зараз є вимогою на рівні правління, яка підлягає юридичній перевірці, а перевірка прийняття рішень має вирішальне значення для зменшення регуляторних та репутаційних збитків…

Співпраця є надзвичайно важливою — як внутрішньо між юридичними, кібербезпековими, операційними та комунікаційними командами, так і зовні через галузеві платформи та взаємодію з правоохоронними органами. Штучний інтелект, якщо його застосовувати обережно під наглядом людини, може прискорити реагування після інциденту та скоротити розрив між виявленням та захисними діями.

Зрештою, стійкість стає конкурентною перевагою у гірничодобувній галузі. Компанії, які можуть продемонструвати надійне управління ШІ, управління інформацією та транскордонну відповідність вимогам, зможуть впевнено модернізуватися, захистити свою діяльність та зберегти ліцензію на діяльність. Кібербезпека, якщо її правильно реалізувати, не є перешкодою для інновацій, а є основою, яка дозволяє швидко та контрольовано впроваджувати нові технології». ***(Linda Sheehan, Megan Claassens and Shaheen Solwa. AI, cybersecurity and operational resilience in mining // ENSafrica***

(https://www.ensafrica.com/news/detail/11273/ai-cybersecurity-and-operational-resilience-i). 03.02.2026).

***

Кіберзахист закладів охорони здоров'я

«…Масштабна атака програм-вимагачів у п'ятницю змусила Медичний центр Університету Міссісіпі (UMMC), одного з найбільших постачальників медичних послуг у штаті, закрити всі 35 своїх клінік і скасувати планові процедури, що стало «багатоденною подією», яка викликала загальнонаціональну стурбованість щодо кібербезпеки лікарень. Оскільки електронна система медичних записів стала недоступною, лікарі повернулися до використання ручки та паперу для лікування пацієнтів, а ФБР та Міністерство охорони здоров'я та соціальних служб мобілізують ресурси для розслідування та усунення порушення…

Хоча відділення швидкої допомоги залишаються відкритими, а персонал проходить навчання на випадок таких відключень, віце-канцлер UMMC ЛуЕнн Вудворд заявила, що тривалість відключення невідома, оскільки ІТ-системи були відключені для ретельної оцінки ризиків. Цей інцидент відображає тривожну тенденцію до збільшення кількості атак програм-вимагачів на медичні заклади США, які не тільки коштують мільярди, але й загрожують безпеці пацієнтів, порушуючи надання невідкладної допомоги, особливо в сільських районах…

Хоча зловмисники зв'язалися з UMMC, залишається незрозумілим, чи вимагали вони викуп. Ця атака також збігається з поширеними в галузі побоюваннями щодо можливих кібернападів з боку Ірану в разі ескалації військової напруженості, хоча на даний момент немає доказів, що пов'язують Іран з інцидентом у Міссісіпі». ***(Sean Lyngaas. Major cyberattack forces closure of clinics across Mississippi // A Warner Bros. Discovery Company (https://edition.cnn.com/2026/02/20/politics/cyberattack-closes-clinics-mississippi). 20.02.2026).***

***

«Health New Zealand закликала MediMap зробити все можливе, щоб впоратися з наслідками кібератаки, яка в неділю порушила роботу платформи управління ліками, змусивши її відключитися на час розслідування та перевірки цілісності даних. Інцидент, який розпочався близько 13:30, призвів до зміни записів, зокрема деяких живих пацієнтів було позначено як померлих, а інших — неправильно позначено, в системі, яка широко використовується в закладах догляду за літніми людьми, інвалідами, хоспісах та громадах для електронного виписування рецептів та координації історії прийому ліків. Даррен Дуглас з Міністерства охорони здоров'я Нової Зеландії підкреслив, що новозеландці очікують надійного захисту медичних даних, і зазначив, що MediMap, як приватна компанія, несе відповідальність за безпеку своєї платформи. Міністерство охорони здоров'я Нової Зеландії активувало свою команду з

управління кіберінцидентами та координує свої дії з іншими агентствами, включаючи Національний сектор кібербезпеки…

MediMap заявила, що виявила несанкціонований доступ до імен, дат народження, лікарів, місць надання медичної допомоги та статусу проживання, залучила зовнішніх кіберфахівців, перевела платформу в режим технічного обслуговування для захисту безпеки пацієнтів та повідомила про це Управління комісара з питань конфіденційності та поліцію. З вимкненням додатка до 60 % закладів догляду за літніми людьми та кілька хоспісів перейшли на ручні паперові процеси; деякі медсестри повідомили про збільшення потреби в персоналі, подовження циклів прийому ліків та підвищення ризику затримок…

Прем'єр-міністр Крістофер Люксон і заступник міністра охорони здоров'я Девід Сеймур назвали цей збій тривожним і нагадали про необхідність посилення кібербезпеки, зазначивши, що він стався після серйозного інциденту в системі Manage My Health наприкінці 2025 року, коли група хакерів заявила, що викрала 108 ГБ даних пацієнтів і вимагала викуп. MediMap принесла вибачення, пообіцяла постійні оновлення і працює над безпечним відновленням, а медичні заклади надають пріоритет безперебійному наданню медичної допомоги». ***(Patient data changed as major NZ health app MediMap hacked // Radio New Zealand (https://www.rnz.co.nz/news/national/587773/patient-data-changed-as-major-nz-health-app-medimap-hacked). 24.02.2025).***

***

Захист персональних даних та соціальні мережі

«…29 січня 2026 року Федеральна комісія з питань зв'язку (FCC) опублікувала публічне повідомлення, в якому попередила малих і середніх постачальників послуг зв'язку про зростаючу загрозу програм-вимагачів, які порушують роботу і ставлять під загрозу конфіденційні дані. Це попередження є частиною більш широкої федеральної ініціативи з підвищення пріоритетності кібербезпеки, оскільки такі агентства, як HHS OCR і DOJ, значно посилили заходи щодо забезпечення дотримання вимог до організацій охорони здоров'я та підрядників у сфері оборони за невиконання стандартів безпеки. На тлі тиску з боку Конгресу через гучні порушення, такі як Salt Typhoon, FCC підкреслила, що атаки програм-вимагачів часто є наслідком соціальної інженерії, вразливостей програмного забезпечення та викрадених облікових даних, що призводить до шифрування файлів та витоку даних…

Щоб зменшити ці ризики, FCC рекомендує найкращі практики, які відповідають рекомендаціям CISA, FTC та NIST, такі як впровадження багатофакторної автентифікації, регулярне оновлення програмного забезпечення, надійне резервне копіювання даних та навчання співробітників. Організаціям настійно рекомендується впроваджувати архітектури «нульової довіри», використовувати сучасні засоби виявлення, такі як EDR та MDR, а також ретельно перевіряти сторонніх постачальників. Окрім дотримання нормативних вимог,

інвестиції в проактивні заходи кібербезпеки та адекватне страхування є необхідними для захисту мереж від дедалі більш витончених кіберзагроз…» ***(Stephen Sharbaugh, Jill Canfield and Tyler R. Bridegan. Surge in Ransomware Incidents Prompts Federal Cybersecurity Guidance and Enforcement Across Sectors // Womble Bond Dickinson (US) LLP (https://www.womblebonddickinson.com/us/insights/alerts/surge-ransomware-incidents-prompts-federal-cybersecurity-guidance-and-enforcement). 11.02.2026).***

***

«Рада з кібербезпеки ОАЕ (CSC) закликала жителів уникати поширення конфіденційної особистої інформації в соціальних мережах, попередивши, що надмірне поширення інформації може призвести до шахрайства та крадіжки особистих даних. За повідомленнями, близько 40% користувачів стикалися з порушеннями конфіденційності, пов'язаними з публікацією таких даних, як домашні адреси, номери телефонів, плани подорожей та сімейні фотографії… Рада підкреслила, що навіть незначна інформація може бути використана в цілеспрямованих шахрайських схемах. Для зменшення ризику вона радить оновлювати програмне забезпечення, обмежувати дозволи додатків, використовувати надійні паролі та багатофакторну автентифікацію, перевіряти безпеку платформ перед обміном інформацією та ретельно контролювати облікові записи. CSC також наголосила на важливості індивідуальної відповідальності за захист персональних даних і пропагує безпечніші звички в Інтернеті через свою постійну інформаційну кампанію «Cyber Pulse», яка має на меті зміцнити довіру та цифрову стійкість в ОАЕ». ***(UAE cybersecurity authority warns residents against sharing personal data on social media // Galadari Printing and Publishing LLC. (https://www.khaleejtimes.com/uae/cybersecurity-council-warn-share-personal-data-social-media-scam-fraud). 22.02.2026).***

***

Правове забезпечення захисту персональних даних

«З 1 січня 2026 року нові правила штату Каліфорнія вимагають від підприємств, які обробляють особисті дані щонайменше 250 000 споживачів (або 50 000 у випадку конфіденційних даних) або отримують значні доходи від продажу даних, проводити щорічний ретельний аудит кібербезпеки. На відміну від оцінок ризиків, орієнтованих на конкретні види діяльності, цей аудит оцінює загальну ефективність програми кібербезпеки в захисті персональних даних від несанкціонованого доступу або втрати. Хоча великі підприємства з валовим доходом понад 100 мільйонів доларів повинні подати свій перший комплексний звіт до квітня 2028 року за попередній рік, всі підприємства, що відповідають вимогам, зрештою зіткнуться з цим щорічним зобов'язанням…

Аудит повинен проводитися кваліфікованим незалежним фахівцем — зовнішнім або внутрішнім аудитором, який не входить до ланцюжка підпорядкування в сфері кібербезпеки — який покладається на докази, а не на

твердження керівництва. З огляду на конкретні та детальні вимоги законодавства Каліфорнії, існуючі аудити можуть потребувати доповнення або узгодження для забезпечення відповідності. Аудит охоплює широкий спектр заходів контролю, включаючи нагляд за третіми сторонами, інвентаризацію та класифікацію даних, а також тестування вразливості. Важливо, що відповідальний керівник повинен засвідчити та подати результати аудиту до державного регуляторного органу під страхом покарання за неправдиві свідчення, що створює значний ризик особистої відповідальності за неточності. Для підготовки підприємствам рекомендується провести «пробні» аудити в 2026 році, щоб завчасно виявити прогалини та скористатися юридичною допомогою для визначення застосовності, перевірки структури аудиту та управління поданням документів до регуляторних органів…» ***(Michael Young. Understanding California Cyber Audit Requirements // Taft Stettinius & Hollister LLP (https://www.privacyanddatasecurityinsight.com/2026/02/understanding-california-cyber-audit-requirements/#page=1). 10.02.2026).***

***

Масштабні витоки персональних даних

«У лютому 2026 року група здирників ShinyHunters оприлюднила набори даних, які, як стверджується, містять понад 1 мільйон записів з Гарвардського університету та 1,2 мільйона з Пенсильванського університету, розкривши конфіденційну особисту інформацію та інформацію про донорів. Порушення безпеки в Гарварді, виявлене в листопаді 2025 року, стало результатом фішингової атаки за допомогою телефону (вішингу), яка скомпрометувала системи університету з питань випускників та розвитку (AAD). Серед викрадених даних — адреси електронної пошти, номери телефонів, домашні та робочі адреси, інформація про відвідування заходів, деталі пожертв та біографічні дані, пов'язані зі збором коштів та взаємодією з випускниками. Також було розкрито внутрішні стратегії, такі як «паузи в прийомі», що узгоджують збір коштів із процесами прийому, а також інформація про статки та контактні дані відомих донорів…

Компанія Hudson Rock, що спеціалізується на кібербезпеці, описала цей інцидент як крах інституційного суверенітету даних, підкресливши, що були розкриті приватні відомості, фінансові деталі та складні соціальні мережі донорів університету. Цей випадок показує, що найціннішими даними зараз є метадані впливу — централізована інформація про вступ до навчальних закладів, статки та сімейні ієрархії, що зберігається на хмарних платформах, вразливих до атак.

Університет Пенсильванії підтвердив факт порушення, але заперечив його масштаби, заявивши, що, попри твердження ShinyHunters, насправді постраждало менше 10 осіб. Обидва університети попередили постраждалих осіб про необхідність бути пильними щодо підозрілих повідомлень та спроб фішингу, пов'язаних із цим інцидентом…

Атака ShinyHunters підкреслює зростаючу загрозу з боку досвідчених кіберзлочинців, які націлені на академічні установи не тільки заради фінансових

даних, але й заради цінної реляційної та стратегічної інформації, яку можна використовувати для вимагання або подальших атак. Установам настійно рекомендується посилити заходи кібербезпеки та проінформувати свої спільноти про ризики соціальної інженерії та фішингу». ***(Ernestas Naprys. Massive data leak hits Harvard and UPenn: ShinyHunters dump stolen records // Cybernews (https://cybernews.com/security/hackers-dump-data-stolen-from-harvard-upenn/). 05.02.2026).***

***

«…30 січня хактивістське угруповання Chronus Group заявило, що викрало 2,3 ТБ даних щонайменше з 25 мексиканських урядових установ, що потенційно може розкрити інформацію про 28 % населення, включаючи дані з універсальної системи охорони здоров'я IMSS Bienestar. Однак мексиканське агентство з цифрових технологій (ATDT) применшило значення цієї події, заявивши, що витік складається з перероблених даних з попередніх порушень застарілих систем, що управляються сторонніми постачальниками, а не з нового вторгнення в конфіденційні урядові системи. Аналітики з Recorded Future та ESET припускають, що Chronus є неформальним об'єднанням, яке використовує бренд «кібертероризм» для поширення страху та привернення уваги ЗМІ, часто перебільшуючи важливість своїх знахідок для побудови свого бренду…

Незважаючи на заперечення уряду, цей інцидент підкреслює погіршення ситуації з безпекою в Латинській Америці, де зараз в середньому відбувається понад 3000 кібератак на тиждень. Хоча ATDT анулювала скомпрометовані облікові дані та вжила заходів для усунення наслідків, експерти попереджають, що залежність регіону від децентралізованих сторонніх послуг створює постійні вразливості. Оскільки латиноамериканські фахівці з безпеки вже повідомляють про найнижчий рівень довіри до національних систем кіберзахисту в світі, будь-який подальший сплеск шахрайства, пов'язаного з цими даними, може ще більше підірвати довіру громадськості до цифрової стійкості Мексики…» ***(Robert Lemos. Big Breach or Smooth Sailing? Mexican Gov't Faces Leak Allegations // TechTarget, Inc. (https://www.darkreading.com/cyberattacks-data-breaches/big-breach-or-nada-de-nada-mexican-govt-faces-leak-allegations). 04.02.2026).***

***

«Південнокорейські чиновники пов'язали великий витік даних у гіганті електронної комерції Coupang з помилками в управлінні, а не з витонченою кібератакою, закликавши до термінового вдосконалення систем безпеки компанії. Попереднє розслідування Міністерства науки виявило, що колишній інженер Coupang скористався вразливістю системи автентифікації, щоб отримати доступ до облікових записів клієнтів з квітня по листопад 2025 року, після попередньої невдалої спроби в січні. В результаті порушення були викрадені особисті дані приблизно 33,7 мільйона клієнтів, включаючи імена та номери телефонів…

Міністерство розкритикувало Coupang за те, що компанія не скасувала безпечний ключ колишнього співробітника вчасно та перешкоджала

розслідуванню, видаливши дані, незважаючи на урядовий наказ про їх збереження. Coupang загрожує штраф у розмірі до 30 мільйонів вон (20 596 доларів) за те, що не повідомила про порушення протягом необхідних 24 годин, оскільки повідомлення надійшло через 53 години.

Coupang наполягає, що порушення було вчинено одним недобросовісним співробітником, який створив 140 мільйонів запитів, використовуючи викрадений ключ, і що немає доказів зовнішнього доступу або подальшої шкоди. Компанія повідомила про інцидент внутрішньо і співпрацює з органами влади, одночасно посилюючи свої заходи безпеки…

У розслідуванні, яке триває, беруть участь поліція та орган з нагляду за захистом даних, а на колишнього китайського співробітника видано ордер на арешт. Coupang також стикається з податковою перевіркою та парламентським розслідуванням через відсутність керівників на слуханнях. Цей інцидент посилив негативну реакцію громадськості та політиків, висвітливши вразливість кібербезпеки на тлі торговельних напружень між США та Японією щодо регуляторних заходів». ***(Heekyong Yang, Hyunjoo Jin. South Korea blames Coupang data breach on management failure, not sophisticated attack // Reuters (https://www.reuters.com/sustainability/boards-policy-regulation/south-korea-says-coupang-must-address-security-loopholes-probe-data-breach-2026-02-10/). 10.02.2026).***

***

«PayPal повідомив про витік даних, що торкнувся частини його клієнтів, через помилку в коді програми для подання заявок на кредит PayPal Working Capital (PPWC), в результаті якої конфіденційна особиста інформація була доступна з 1 липня 2025 року по 13 грудня 2025 року. Компанія виявила проблему 12 грудня 2025 року і згодом виправила помилковий код. На відміну від традиційного зовнішнього вторгнення, цей інцидент був внутрішньою вразливістю, яка дозволила несанкціонований доступ до даних, включаючи імена, адреси, номери телефонів і, що найважливіше, номери соціального страхування та дати народження… PayPal, глобальний платіжний гігант з понад 400 мільйонами рахунків, вжив заходів для припинення несанкціонованого доступу, скинув паролі для уражених рахунків і відшкодував збитки невеликій кількості клієнтів, які зазнали несанкціонованих транзакцій. Щоб зменшити ризики, такі як крадіжка особистих даних, компанія пропонує два роки безкоштовного моніторингу кредитів та відновлення особистих даних через Equifax, радить постраждалим особам залишатися пильними щодо потенційних атак соціального інжинірингу та перевіряти свої кредитні звіти». ***(Alex Lekander. PayPal notifies PPWC customers of five-month-long data breach // CyberInsider.com (https://cyberinsider.com/paypal-notifies-ppwc-customers-of-five-month-long-data-breach/). 20.02.2026).***

***

«23 лютого 2026 року «Олімпік» (Марсель) став жертвою кібератаки, під час якої хакер заявив, що володіє базою даних 400 000 уболівальників і має намір її продати. 24 лютого клуб негайно випустив заяву, в якій підтвердив спробу

вторгнення, але заперечив масштаби порушення, запевнивши вболівальників, що банківські дані та паролі не були скомпрометовані. Інцидент, який спричинив тимчасовий збій у роботі вебсайту, було швидко локалізовано, і клуб подав офіційну скаргу до французького органу з захисту даних CNIL… Хоча конкретні технічні деталі, ознаки компрометації або шкідливе програмне забезпечення не були розкриті, схема атаки відповідає типовим методам експлуатації веб-додатків, таким як SQL-ін'єкція або credential stuffing. Ця подія підкреслює зростання кіберзагроз, з якими стикаються спортивні організації, та важливість надійних заходів безпеки, прозорої комунікації та дотримання нормативних вимог. Рекомендації щодо мінімізації ризиків для подібних організацій включають регулярне тестування вразливостей загальнодоступних додатків, впровадження багатофакторної аутентифікації та проведення навчання з питань безпеки». ***(Olympique Marseille Cyberattack 2026: Club Confirms Attempted Website Breach Amid Supporter Data Leak Claims // Rescana (https://www.rescana.com/post/olympique-marseille-cyberattack-2026-club-confirms-attempted-website-breach-amid-supporter-data-lea). 02.2026).***

***

«У Франції виявлено масштабне порушення безпеки даних, в результаті якого було розкрито конфіденційну інформацію приблизно 15 мільйонів громадян після кібератаки, спрямованої на 1500 лікарів, які використовували медичне програмне забезпечення від Cegedim Sante наприкінці 2025 року. За даними телеканалу France 2, було отримано доступ до відкритої бази даних, яка містила не тільки адміністративні дані пацієнтів, такі як імена, адреси та номери телефонів, але й надзвичайно конфіденційні записи лікарів, включаючи такі деталі, як «ВІЛ-позитивний», «мусульманська мати, що носить хіджаб» та «син у в'язниці»…

Міністерство охорони здоров'я Франції визнало факт порушення, зазначивши, що хоча записи лікаря про приватне життя пацієнтів не порушують GDPR, у викраденій базі даних містяться дані про відомих політичних діячів та посадовців, відповідальних за національну безпеку. Cegedim Sante підтвердила факт атаки та подала скаргу до прокуратури. Хоча компанія стверджує, що порушення стосувалося лише адміністративних записів, а структуровані медичні записи залишилися недоторканими, Міністерство охорони здоров'я підкреслило, що близько 169 000 пацієнтів були зачеплені записами, що містили конфіденційні особисті коментарі, хоча повний обсяг 15 мільйонів викрадених записів все ще розслідується. Прокуратура Парижа розпочала розслідування цього інциденту». ***(Ilayda Cakirtekin. 15M French citizens affected by massive data breach following cyberattack on medical software // Anadolu Ajansı (https://www.aa.com.tr/en/europe/15m-french-citizens-affected-by-massive-data-breach-following-cyberattack-on-medical-software/3842345). 27.02.2026).***

***

«Французька компанія ManoMano, що займається електронною комерцією в сфері ремонту та облаштування житла, повідомила про витік

даних, який стався в січні, але про який клієнтам стало відомо лише нещодавно. Інцидент стався внаслідок кібератаки, яка зачепила стороннього субпідрядника з обслуговування клієнтів, який, судячи з усього, був інстанцією Zendesk компанії. Згідно з повідомленням ManoMano, серед викрадених даних є імена клієнтів, адреси електронної пошти, номери телефонів та листування зі службою обслуговування клієнтів. Однак зловмисник під псевдонімом «Indra» взяв на себе відповідальність за цю атаку на хакерському порталі BreachForums, стверджуючи, що витік даних був набагато більшим…

Хакер стверджує, що викрав 43 ГБ даних, включаючи інформацію, пов'язану з 37,8 мільйонами облікових записів користувачів, понад 900 000 квитків на обслуговування та понад 13 000 вкладень. За повідомленнями, викрадені дані стосуються користувачів з усіх п'яти європейських країн, де працює ManoMano — Франції, Німеччини, Італії, Іспанії та Великої Британії. Зловмисник стверджує, що отримав доступ, зламавши систему служби підтримки клієнтів, розташовану в Тунісі. ManoMano — популярний веб-сайт про DIY та садівництво, який щомісяця відвідують понад 50 мільйонів користувачів». ***(Ionut Arghire. 38 Million Allegedly Impacted by ManoMano Data Breach // Wired Business Media (https://www.securityweek.com/38-million-allegedly-impacted-by-manomano-data-breach/). 27.02.2026).***

***

«Нідерландська телекомунікаційна компанія Odido стала жертвою серйозного порушення безпеки даних, скоєного відомою хакерською групою «ShinyHunters». В результаті однієї з наймасштабніших кібератак в Нідерландах компанія Odido підтвердила крадіжку персональних даних 6 мільйонів клієнтів, включаючи конфіденційну інформацію, таку як імена, номери телефонів та фінансові дані. Викрадені дані публікуються в даркнеті.

Незважаючи на наслідки витоку, Odido вирішила не вести переговори з кіберзлочинцями і не піддаватися на шантаж. Рішення було прийнято після консультацій з експертами з кібербезпеки та правоохоронними органами. За повідомленнями, хакерська група погрожує щодня публікувати значний обсяг даних клієнтів, щоб отримати викуп.

Влада, включаючи національну поліцію Нідерландів, не рекомендує платити викуп, наголошуючи, що будь-яка виплата може фінансувати майбутні кібератаки, не гарантуючи безпечного видалення викрадених даних. Поліція продовжує розслідування порушення, намагаючись мінімізувати наслідки для постраждалих клієнтів». ***(Massive Data Breach: Dutch Telecom Odido Hacked // Devdiscourse (https://www.devdiscourse.com/article/law-order/3818958-massive-data-breach-dutch-telecom-odido-hacked). 26.02.2026).***

***

«OpenAI оголосила про значний прорив у галузі кодування на основі штучного інтелекту завдяки своїй новій моделі GPT-5.3-Codex, яка перевершує попередні версії та системи-конкуренти за показниками кодування. Цей прогрес виводить OpenAI на передові позиції у розробці програмного забезпечення на основі штучного інтелекту, що може змінити підхід до написання, тестування та налагодження коду. Однак компанія впроваджує GPT-5.3-Codex із суворим контролем і відкладає повний доступ для розробників та API через посилення занепокоєння з приводу кібербезпеки…

Хоча платні користувачі ChatGPT можуть використовувати модель для щоденних завдань з кодування, OpenAI обмежує доступ для додатків з високим рівнем ризику в галузі кібербезпеки та автоматизує використання в великих масштабах. Доступ до чутливих функцій можливий лише через нову програму довіреного доступу для перевірених фахівців з безпеки. У блозі OpenAI наголошується на обережному підході, що передбачає застосування найповніших на сьогодні заходів безпеки в галузі кібербезпеки, включаючи навчання з питань безпеки, автоматизований моніторинг та застосування засобів захисту від загроз…

Генеральний директор Сем Альтман зазначив, що GPT-5.3-Codex є першою моделлю, яка досягла «високого» рівня ризику кібербезпеки у внутрішній системі готовності OpenAI, визнавши, що її вдосконалені можливості кодування та міркування можуть потенційно призвести до реальних кібератак у разі неправильного використання. Як результат, OpenAI надає пріоритет безпеці та відповідальному впровадженню, шукаючи баланс між інноваціями та безпекою...» ***(Sharon Goldman. OpenAI's new model leaps ahead in coding capabilities—but raises unprecedented cybersecurity risks // Fortune Media IP Limited (https://fortune.com/2026/02/05/openai-gpt-5-3-codex-warns-unprecedented-cybersecurity-risks/). 05.02.2026).***

***

«Агентство з кібербезпеки та безпеки інфраструктури (CISA) видало обов'язкову оперативну директиву, яка вимагає від федеральних агентств припинити використання периферійних пристроїв, таких як брандмауери, маршрутизатори, пристрої мережевої безпеки та пристрої Інтернету речей, які більше не отримують оновлень безпеки від постачальників. CISA попереджає, що периферійні пристрої, підтримка яких припинена (EOS), становлять суттєву і постійну загрозу, оскільки вони часто стають мішенню для досвідчених зловмисників через їх глибоку інтеграцію з організаційними мережами та системами управління ідентифікацією…

Згідно з новою директивою, агентства повинні негайно оновити всі застарілі периферійні пристрої до підтримуваної версії, за умови, що це не порушить виконання критично важливих функцій. Протягом трьох місяців агентства повинні повідомити CISA, які пристрої з нового списку периферійних пристроїв EOS використовуються. Потім вони мають 12 місяців, щоб вивести з експлуатації всі

перелічені пристрої EOS, і повинні скласти інвентарний список усіх периферійних пристроїв, які втратять підтримку протягом наступного року, а також повідомити цей інвентарний список CISA.

Протягом 18 місяців усі пристрої, термін експлуатації яких закінчується, повинні бути вилучені, а протягом 24 місяців агентства повинні встановити процеси для відстеження та поступового виведення з експлуатації пристроїв, термін експлуатації яких закінчується. Хоча ця директива є обов'язковою лише для федеральних агентств, CISA закликає місцеві органи влади, підприємства та міжнародних партнерів наслідувати її приклад, наголошуючи, що пристрої, які більше не підтримуються, ніколи не повинні залишатися в корпоративних мережах…

Ця директива є наслідком багаторічних кібератак з боку національних держав, які використовували вразливі периферійні пристрої, що призводило до серйозних порушень безпеки. CISA у співпраці з ФБР та Національним центром кібербезпеки Великої Британії також оприлюднює інформаційний бюлетень з рекомендаціями щодо захисту периферійних пристроїв. Хоча повноваження CISA щодо забезпечення дотримання законодавства є обмеженими, вона буде співпрацювати з Білим домом з метою контролю за дотриманням вимог та надання підтримки агентствам у виконанні цих нових вимог у сфері кібербезпеки». ***(Eric Geller. CISA orders feds to disconnect unsupported network edge devices // TechTarget, Inc. (https://www.cybersecuritydive.com/news/cisa-edge-devices-binding-operational-directive/811539/). 05.02.2026).***

***

«Проблеми безпеки, пов'язані з агентом штучного інтелекту OpenClaw та його соціальною мережею Moltbook, швидко стають реальністю, оскільки дослідники виявили низку серйозних вразливостей. OpenClaw, популярний персональний агент штучного інтелекту, працює локально, але за замовчуванням має повний доступ до системи, що дозволяє йому читати файли, виконувати команди, керувати обліковими даними та взаємодіяти із зовнішніми сервісами, такими як Discord, Slack і Telegram. Цей широкий доступ у поєднанні зі слабкою або відсутньою автентифікацією в його Model Context Protocol (MCP) створює величезну площину для атак.

Дослідники склали каталог вразливостей, серед яких помилки віддаленого виконання коду, відкрита база даних соціальних графіків та екосистема плагінів, заражена шкідливим програмним забезпеченням. Наприклад, шлюз Clawdbot, який часто прив'язаний до 0.0.0.0 на порту 18789, відкриває повний адміністративний API, роблячи його доступним для зловмисників. Відсутність безпеки MCP дозволяє зловмисникам збирати облікові дані у вигляді звичайного тексту, історії чатів і навіть видавати команди, ніби вони є власниками агента…

Особливо серйозна вразливість, CVE-2026-25253, дозволяла зловмисникам створювати шкідливі посилання, які при відкритті в браузері, аутентифікованому в інтерфейсі OpenClaw Control, могли викрасти токени та надати доступ на рівні оператора, що дозволяло віддалено виконувати код. Ця вразливість працює навіть

якщо шлюз налаштований на прослуховування тільки інтерфейсу loopback, що підриває припущення про безпеку localhost.

Moltbook, соціальна мережа OpenClaw, схожа на Reddit, зазнала критичної помилки в налаштуваннях бекенду, що призвело до витоку її основної бази даних, в результаті чого було викрадено десятки тисяч адрес електронної пошти, 1,5 мільйона API-ключів та приватних повідомлень. Зловмисники могли видавати себе за будь-якого бота, публікувати або видаляти контент, а також потенційно отруювати моделі штучного інтелекту або запускати кампанії з дезінформації. Оскільки більшість облікових записів Moltbook є агентами OpenClaw, платформа успадковує всі вразливості безпеки OpenClaw…

Функція постійної пам'яті OpenClaw означає, що приховані інструкції в контенті можуть викликати затримку, атаки зі станом, що робить експлойти більш небезпечними з часом. Екосистема плагінів також піддається зловживанням, оскільки доступні сотні заражених шкідливим програмним забезпеченням «навичок», які часто маскуються під легальні інструменти.

Незважаючи на ці проблеми, багато вразливостей виникають через неправильні налаштування і могли бути виявлені за допомогою належних перевірок безпеки. Однак швидке зростання екосистеми та відсутність надійної безпеки роблять її привабливою мішенню для зловмисників і ризикованим середовищем для користувачів та розробників. Експерти з безпеки попереджають, що організації повинні інвестувати в засоби захисту на основі штучного інтелекту вже зараз, оскільки загрози швидко еволюціонують, а ризики ігнорування цих вразливостей є значними. Наразі рекомендується бути обережними при використанні OpenClaw та Moltbook, враховуючи відсутність значущих засобів контролю безпеки». ***(Steven J. Vaughan-Nichols. It took a researcher fewer than 2 hours to hijack OpenClaw // The New Stack (https://thenewstack.io/openclaw-moltbot-security-concerns/). 05.02.2026).***

***

«…Незважаючи на недавню паніку, спричинену штучним інтелектом, яка знищила 300 мільярдів доларів ринкової вартості програмного забезпечення, аналітик Morgan Stanley Мета Маршалл стверджує, що штучний інтелект є потужним стимулом для кібербезпеки, перетворюючи розпродаж на можливість для покупок. Маршалл стверджує, що штучний інтелект розширює площу атаки через вразливості в згенерованому коді та великих мовних моделях (LLM), змушуючи організації збільшувати витрати на безпеку для захисту від складних загроз, таких як швидке введення та отруєння даних… Вона прогнозує, що ринок безпеки штучного інтелекту може зрости з 16 мільярдів доларів до понад 45 мільярдів доларів у найближчі роки. Хоча Маршалл зберігає позитивні оцінки лідерів галузі CrowdStrike і Palo Alto Networks, посилаючись на успішні придбання останньої та чистий список злиттів і поглинань першої, вона вбачає ще більший потенціал зростання в таких пошкоджених акціях, як Zscaler, SailPoint, SentinelOne і Netskope, прогнозуючи, що ці компанії перевищать очікування щодо зростання і запропонують потенційний прибуток від 30% до понад 120%...» ***(Vuk Zdinjak. Morgan Stanley flags $45B hidden cybersecurity***

opportunity // The Arena Media Brands, LLC (https://www.thestreet.com/investing/stocks/morgan-stanley-flags-45b-hidden-cybersecurity-opportunity). 15.02.2026).

***

«Штучний інтелект і квантові обчислення перейшли від теорії до безпосередньої кіберреальності, трансформувавши як напад, так і захист. ШІ тепер автоматизує виявлення, виправлення та прогнозування реакції для захисників, але водночас дозволяє зловмисникам запускати фейкові відео, самомодифікуюче шкідливе програмне забезпечення та гіперреалістичний фішинг у великих масштабах. Фішинг, створений за допомогою ШІ, вже досягає 54% клікабельності проти 12% для традиційних кампаній, інциденти з депфейками зросли на 680%, а глобальні атаки на основі ШІ, за прогнозами, перевищать 28 мільйонів у 2025 році. Оскільки організації впроваджують автономні системи ШІ швидше, ніж розвиваються рамки управління, ризик збільшується у всьому рівнянні «загроза-вразливість-вплив»…

Водночас квантові обчислення стають структурним руйнівником. З появою масштабованих систем широко використовувані стандарти шифрування, такі як RSA, можуть бути швидко зламані за допомогою алгоритмів, таких як алгоритм Шора, що призведе до розкриття десятиліть зібраних зашифрованих даних. Уряди закликають до переходу на постквантову криптографію (PQC), проте лише деякі організації мають плани готовності, що залишає фінансові системи, інтелектуальну власність та національну безпеку незахищеними…

Традиційні моделі кібербезпеки, орієнтовані на периметр, вже не є достатніми в світі, сформованому штучним інтелектом, квантовими технологіями, Інтернетом речей, 5G та конвергенцією хмарних технологій. Щоб залишатися стійкими, організації повинні впроваджувати гібридну та PQC-криптографію, реалізовувати засоби управління штучним інтелектом, підвищувати кваліфікацію своїх співробітників, впроваджувати архітектури Zero Trust, посилювати кібергігієну та покращувати координацію між державним і приватним секторами. Ера штучного інтелекту та квантових загроз не наближається — вона вже настала. Стратегічна переорієнтація більше не є опцією, а є необхідною умовою виживання в умовах прискореного технологічного розвитку». ***(Chuck Brooks. Why Cybersecurity Strategies and Frameworks Must Be Recalibrated in the Age of AI and Quantum Threats // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/why-cybersecurity-strategies-and-frameworks-must-be-recalibrated-in-the-age-of-ai-and-quantum-threats/). 18.02.2026).***

***

«Ред-тімінг (Red teaming), який давно використовується для виявлення слабких місць у традиційних IT-системах, все частіше застосовується до генеративної ШІ для підвищення довіри та безпеки, проте недетермінована поведінка ШІ та відсутність фіксованих правил вимагають нових тактик оцінки. Основними ризиками, що зумовлюють використання червоної команди в ШІ, є витік даних — коли конфіденційна інформація витягується за допомогою

суперечливих підказок — та помилкові результати, оскільки великі мовні моделі (LLM) можуть бути маніпульовані з метою ігнорування захисних бар'єрів за допомогою хитромудрих формулювань, довгих або заплутаних інструкцій та введення підказок, що може мати серйозні наслідки для громадської безпеки (наприклад, введення в оману служб екстреної допомоги шляхом спотворення даних про місцезнаходження)…

Щоб відповісти на ці виклики, фахівці застосовують три стратегії. По-перше, команда «червоних» систематично створює та повторює запити на «втечу з в'язниці», приховує шкідливі команди в довгих текстах і перевіряє запити на приватні дані, одночасно навчаючи внутрішні детектори виявляти ознаки зловживання. По-друге, мультимодальна команда червоних атакує штучний інтелект, який обробляє зображення, аудіо або відео, подаючи оманливі вхідні дані, такі як непомітні візуальні зміни дорожніх знаків, які можуть заплутати автономні транспортні засоби, або отруюючи дані моделі, викриваючи розширену поверхню атаки зору, мови та сенсорних конвеєрів. По-третє, цифрове двійникове «Ред-тімінг» створює високоточні віртуальні копії систем штучного інтелекту та їхніх середовищ для безпечного моделювання гіпотетичних сценаріїв, таких як втручання в робочий процес служби екстреної допомоги міста, та спостереження за режимами відмови без створення загрози для реальних операцій…

Хоча ці методи, специфічні для ШІ, розвиваються, вони доповнюють (а не замінюють) такі основні засоби, як тестування на проникнення та моніторинг поверхні атаки, створюючи багаторівневий підхід до забезпечення безпеки, який краще захищає та стабілізує системи ШІ, оскільки вони відіграють важливу роль у суспільстві». ***(Darren Pulsipher. How Red Teams are Reinventing Cybersecurity for the Age of AI // Cyber Defense Media Group (https://www.cyberdefensemagazine.com/how-red-teams-are-reinventing-cybersecurity-for-the-age-of-ai/). 19.02.2026).***

***

«Нове дослідження, проведене постачальником послуг з управління безпекою LevelBlue, виявляє значну неготовність CIO (директор з інформаційних технологій або IT-директор) до кіберзагроз, пов'язаних з штучним інтелектом. Хоча 51% опитаних CIO очікують атак на основі штучного інтелекту протягом найближчих 12 місяців, лише третина вважає, що їхня організація готова до реагування. Рівень впевненості ще більше знижується при оцінці оборонних можливостей: лише 20% вважають себе високоефективними у протидії супротивникам, що використовують штучний інтелект, і така ж частка вважає себе високоефективними у використанні штучного інтелекту для підвищення власної кібербезпеки, незважаючи на те, що 72% вважають, що інструменти на основі штучного інтелекту стануть необхідними для виявлення та реагування…

CIO в цілому вважають, що штучний інтелект відіграє подвійну роль — сприяє інноваціям і стимулює нові форми кіберзлочинності — проте нинішні засоби контролю не встигають за цими змінами. Майже половина (49%) планує надати пріоритет інтеграції кібербезпеки в усі бізнес-функції, а 39% мають намір

збільшити участь керівництва в обговоренні питань стійкості. Однак внутрішні бар'єри залишаються: 47% вказують на недостатню пріоритетність кіберстійкості для керівництва, менше половини вважають, що їхні KPI ефективно пов'язують безпеку з бізнес-результатами, а 49% повідомляють про невідповідність між схильністю до бізнес-ризиків та управлінням ризиками кібербезпеки…

Інвестиції надходять як у фундаментальні, так і в специфічні для ШІ ініціативи з безпеки: 76% використовують машинне навчання для виявлення загроз, а 70% використовують генеративний ШІ для протидії складним методам соціальної інженерії. Ризики ланцюга поставок викликають дедалі більшу стурбованість: 56% керівників ІТ-відділів очікують на неминучі атаки на ланцюг поставок програмного забезпечення, тоді як лише 22% мають чітке уявлення про цей ланцюг. Організації також все частіше звертаються до зовнішньої підтримки, і протягом наступних двох років планується подвоїти залучення фахівців з реагування на інциденти. У звіті рекомендується поліпшити узгодженість дій керівництва щодо кіберризиків, пов'язаних зі штучним інтелектом, інтегрувати безпеку в усі бізнес-функції, посилити належну перевірку ланцюга поставок та залучити зовнішніх експертів для підготовки до інцидентів». ***(Joseph Gabriel Lagonsin. CIOs brace for AI-led cyber attacks but feel unready // TechDay (https://securitybrief.com.au/story/cios-brace-for-ai-led-cyber-attacks-but-feel-unready). 26.02.2026).***

***

«Останній глобальний звіт Fastly з досліджень у сфері безпеки показує, що організації в Південно-Східній Азії все частіше пов'язують впровадження штучного інтелекту з інцидентами в сфері кібербезпеки: 69% респондентів вважають, що їхні останні порушення безпеки пов'язані з інструментами або моделями штучного інтелекту. У звіті це називається «швидкісним податком на штучний інтелект»: «AI-first»-бізнеси — ті, що з самого початку інтегрують штучний інтелект у свої основні процеси — в середньому витрачають майже сім місяців на відновлення після інцидентів, що на 80 днів довше, ніж організації, що не використовують штучний інтелект, і несуть витрати, що перевищують 135%. У глобальному масштабі 44% «AI-first»-організацій повідомили, що штучний інтелект був безпосередньо використаний у їхньому останньому інциденті, порівняно з лише 6% інших…

Швидке поширення штучного інтелекту змінює поверхні атаки через агентні робочі процеси, децентралізовані потоки даних та масове автоматичне збирання даних для навчання, що збільшує навантаження на інфраструктуру та ускладнює виявлення загроз. У Південно-Східній Азії 67% респондентів зараз вважають збирання даних штучним інтелектом істотним центром витрат, середній річний вплив якого перевищує 372 000 доларів. Окрім прямих порушень, трафік, пов'язаний зі штучним інтелектом, сприяє оперативним збоям (53%), підвищенню витрат на інфраструктуру (51%) та інцидентам безпеки або витоку даних (50%)…

Щоб протидіяти цим ризикам, організації збільшують інвестиції в брандмауери веб-додатків (72%), рішення для безпеки API (66%) та інструменти виявлення агентів (64%), тоді як 83% висловлюють занепокоєння щодо DDoS-атак,

спрямованих на агентів ШІ. Однак дефіцит кваліфікованих кадрів залишається гострим: 61% потребують більше знань у галузі безпеки ШІ, а 59% повідомляють про збільшення навантаження на існуючі команди. Fastly попереджає, що оскільки ШІ стає невід'ємною частиною бізнес-операцій, безпека повинна розвиватися такими ж темпами — модернізуючи засоби контролю, видимість та реагування на інциденти, щоб відповідати швидкості інновацій, а не сповільнювати її». ***(Catherine Knowles. AI-first firms in Southeast Asia face rising cyber risk // TechDay (https://securitybrief.asia/story/ai-first-firms-in-southeast-asia-face-rising-cyber-risk). 27.02.2026).***

***

«У міру того як організації все частіше використовують штучний інтелект, нове глобальне опитування 2000 IT-керівників показує відповідне зростання ризиків кібербезпеки, витрат і часу відновлення. Дослідження, проведене Sapio від імені Fastly, виявило, що організації, які в першу чергу використовують ШІ, несуть на 135% вищі витрати від інцидентів безпеки і витрачають в середньому 6,8 місяця на відновлення — на цілих 80 днів довше, ніж їхні колеги, які не використовують ШІ. Це ускладнюється тим, що понад третина організацій, які використовують штучний інтелект, повідомляють, що пряме використання їхніх інструментів штучного інтелекту сприяло останньому інциденту, а 53% визнають, що їхнім командам бракує необхідних знань у галузі штучного інтелекту для боротьби з цими новими загрозами…

Опитування також висвітлює більш широкі проблеми безпеки: 90% всіх організацій стикалися з принаймні одним інцидентом протягом минулого року, а 66% зазнали повторного інциденту протягом трьох місяців. У відповідь на це організації збільшують інвестиції в інструменти для виявлення агентів штучного інтелекту (56%), захист API та розгортання брандмауерів веб-додатків. Однак розвиток штучного інтелекту привів до появи ще однієї значної проблеми: боти штучного інтелекту, що збирають веб-контент, стали істотним центром витрат для 64% підприємств, а пов'язані з цим витрати на інфраструктуру зросли до понад 348 000 доларів на рік. У міру подальшого впровадження штучного інтелекту стає очевидним, що команди з кібербезпеки повинні готуватися до більш складних і дорогих загроз, одночасно працюючи над усуненням зростаючого дефіциту кваліфікованих кадрів у своїх організаціях». ***(Michael Vizard. Survey Surfaces Increased Cybersecurity Risks Following AI Adoption // Techstrong Group Inc. (https://securityboulevard.com/2026/02/survey-surfaces-increased-cybersecurity-risks-following-ai-adoption/). 25.02.2026).***

***

«…Швидке і широке впровадження штучного інтелекту (ШІ) у всіх секторах бізнесу кардинально змінило ситуацію в галузі кібербезпеки, створивши нове і складне середовище загроз на 2026 рік, де акцент повинен бути перенесений з обговорення використання ШІ на активне управління високими ризиками і постійними прогалинами в безпеці, які він створює. Основна нова загроза походить від некерованих інструментів ШІ, зокрема великих

мовних моделей (LLM), які створюють вразливості, такі як швидке введення та випадковий витік даних. Що ще важливіше, ШІ еволюціонує від реактивного інструменту до автономного або «агентного» актора, який використовується як зброя для зниження бар'єру входу для зловмисників і забезпечення повністю автоматизованих послідовностей атак…

Ця еволюція привела до появи «Ransomware 3.0» — загрози нового покоління, яка виходить за межі простого шифрування даних і зосереджується на тонкій маніпуляції цілісністю даних, змінюючи або пошкоджуючи критично важливі записи з часом. Такий підхід становить катастрофічний ризик, оскільки підриває довіру до фінансових записів та інтелектуальної власності, потенційно завдаючи непоправної шкоди бренду, яку традиційні рішення безпеки на основі сигнатур не в змозі виявити.

У відповідь на ці загрози, що прискорюються штучним інтелектом, кібербезпека більше не може розглядатися як суто IT-проблема, а повинна стати обов'язковою складовою організаційної культури. Нова стратегія захисту повинна базуватися на моделі кіберстійкості Zero Trust, заснованій на принципі «ніколи не довіряй, завжди перевіряй». Це вимагає розглядати кожного агента штучного інтелекту як ідентифікацію з високим рівнем ризику, застосовувати надійну, захищену від фішингу аутентифікацію машин та суворий доступ з мінімальними привілеями…

У 2026 році управління ідентифікаційними даними — як людськими, так і машинними — стане найважливішим полем битви. Оскільки зловмисники зараз вміло обходять стандартну багатофакторну автентифікацію (MFA), організаціям необхідно обов'язково впровадити технології MFA, стійкі до фішингу, такі як FIDO2 і Passkeys, як єдиний метод входу в систему. Керівники служб інформаційної безпеки повинні вжити негайних заходів, проводячи аудити для класифікації всіх інструментів штучного інтелекту, включаючи тіньові IT, та встановити спеціальні політики безпеки для штучного інтелекту в рамках існуючої системи управління ідентифікацією та доступом (IAM). Зрештою, організації повинні підвищити управління штучним інтелектом до стратегічного пріоритету, перебудувати свої системи захисту на основі принципів Zero Trust та сприяти культурі безпеки у всіх відділах, щоб перетворити ці нові ризики на стійку конкурентну перевагу». ***(Andy Syrewicze. How AI adoption is reshaping the cybersecurity threat landscape and defence strategies // Kadium Ltd (https://networkingplus.co.uk/opinion-details?itemid=9422&post=how-ai-adoption-is-reshaping-the-cybersecurity-threat-landscape-and-defence-strategies--195359). 27.02.2026).***

***

Штучний інтелект, як інструмент боротьби із кіберзлочинністю

«…Існує значна розбіжність між керівництвом у сфері кібербезпеки та аналітиками на передовій щодо продуктивності інструментів штучного інтелекту: 71% керівників повідомляють про поліпшення, тоді як серед

аналітиків таких лише 22%. Ця розбіжність вказує на структурну проблему, коли агенти штучного інтелекту розгортаються в центрах безпеки (SOC) з архітектурою даних, оптимізованою для людського тлумачення, наприклад, журналами та таблицями, а не для машинного мислення… Оскільки в поточних даних відсутній операційний контекст або «причина» подій, пов'язаних з безпекою, інструменти штучного інтелекту часто не можуть самостійно міркувати, що вимагає надмірного нагляду і призводить до недовіри аналітиків. Щоб вирішити цю проблему, експерти стверджують, що галузь повинна перенести акцент з якості моделей на архітектуру даних, зокрема шляхом створення «графіків контексту безпеки», які фіксують інституційні знання та логіку, що лежить в основі минулих рішень… Реструктуризуючи дані для забезпечення контексту, необхідного для надійного функціонування штучного інтелекту, організації можуть поліпшити управління, зменшити необхідність «догляду» за автономними агентами та зберегти важливі колективні знання, незважаючи на високу плинність кадрів». ***(Kolawole Samuel Adebayo. Better Data Could Unlock AI's Full Potential In Cybersecurity // Forbes Media LLC. (https://www.forbes.com/sites/kolawolesamueladebayo/2026/02/17/better-data-could-unlock-ais-full-potential-in-cybersecurity/). 17.02.2026).***

***

«Акції компаній, що займаються кібербезпекою, різко впали після того, як 20 лютого компанія Anthropic оголосила про випуск «Claude Code Security» — автоматизованого інструменту штучного інтелекту для сканування вразливостей коду. Лідером падіння стала компанія CrowdStrike, акції якої подешевшали майже на 17%, а інші компанії, такі як Okta, Zscaler, Palo Alto Networks і SentinelOne, також зазнали значних втрат… Цей розпродаж, який призвів до падіння індексу First Trust Nasdaq Cybersecurity ETF (CIBR) до найнижчого рівня з квітня 2025 року, відображає побоювання ринку, що автоматизація за допомогою штучного інтелекту може призвести до скорочення прибутку традиційних компаній, що займаються кібербезпекою… Однак аналітик Bank of America Меділін Брукс стверджує, що реакція ринку є надмірною, зазначаючи, що інструмент Anthropic зосереджений виключно на скануванні коду перед виробництвом, а не на моніторингу часу виконання, власній телеметрії та контролі в режимі реального часу, які забезпечують відомі платформи. Брукс стверджує, що, хоча ШІ пропонує додатковий рівень, йому бракує контексту та структурних переваг основних постачальників послуг з кібербезпеки, що робить заміну платформи малоймовірною». ***(Piero Cingari. Cybersecurity Stocks Are Cratering On AI Threat: Is This A Buy Opportunity? // Benzinga (https://www.benzinga.com/markets/tech/26/02/50834000/cybersecurity-stocks-fall-anthropic-claude-code-security-buy-opportunity). 24.02.2026).***

***

«…Індійські акції компаній, що займаються кібербезпекою, у вівторок зазнали значного падіння, втративши до 15% на тлі побоювань, викликаних випуском нового інструменту штучного інтелекту від Anthropic, Claude Code Security. Інвестори побоюються, що цей інструмент штучного інтелекту, який

може самостійно виявляти та усувати складні вразливості програмного забезпечення, міркуючи як людський дослідник, може замінити традиційні платформи кібербезпеки… Найбільше постраждала компанія Tac Infosec, що котирується на біржі SME: її акції впали на 15% і втратили більше половини своєї вартості порівняно з 52-тижневим максимумом, а інші великі гравці, такі як L&T Technology Services, Affle і Cigniti Technologies, також зазнали різкого падіння. Однак експерти, такі як Сантош Міна з Swastika Investmart, відзначають, що прямий вплив на індійські акції був відносно обмеженим порівняно з більш різким падінням, яке спостерігалося у американських аналогів, таких як CrowdStrike, оскільки сектор кібербезпеки в Індії є меншим… Незважаючи на миттєву реакцію ринку, аналітики залишаються оптимістичними щодо довгострокових структурних можливостей для таких компаній, як Quick Heal та eMudhra, прогнозуючи перехід до інтегрованих в штучний інтелект корпоративних пропозицій, як тільки перша паніка вщухне». ***(Pawan Kumar Nahar. Anthropic AI tool buzz: Are cybersecurity stocks next after IT rout? Analysts' views amid global cues // India Today Group (https://www.businesstoday.in/markets/stocks/story/anthropic-ai-tool-buzz-are-cybersecurity-stocks-next-after-it-rout-analysts-views-amid-global-cues-517775-2026-02-24). 24.02.2026).***

***

«Роль новітніх генеративних та агентних систем штучного інтелекту в забезпеченні кібербезпеки в школах залишається невизначеною, навіть попри те, що 51% освітян передбачають, що штучний інтелект посилить кіберзагрози в наступному році. Хоча традиційне машинне навчання вже давно використовується в інструментах безпеки, нові генеративні моделі тестуються в таких районах, як Оук-Парк в Іллінойсі, для виконання таких завдань, як аналіз журналів служби підтримки та виявлення прогалин у планах реагування на інциденти… Однак перші результати є неоднозначними, оскільки моделі іноді генерують «відволікаючі маневри» або мають проблеми з великими наборами даних. Керівники округів, такі як Вільям Бракетт, зазначають, що інтегровані постачальниками інструменти штучного інтелекту, навчені на конкретних форматах даних, наразі є більш надійними, ніж загальні моделі…

Незважаючи на ажіотаж, впровадженню заважають скептицизм щодо заяв постачальників, обмеженість ресурсів та той факт, що існуючі інструменти, які не використовують штучний інтелект, часто виконують завдання більш ефективно. Експерти, такі як Емі Маклафлін та Дуг Левін, стверджують, що більшість IT-команд округів не мають достатніх ресурсів для створення власних засобів захисту на основі штучного інтелекту, а перспективи цієї технології є в основному футуристичними. Крім того, дефіцит бюджету та скорочення федерального фінансування кібербезпеки роблять дорогі рішення на основі штучного інтелекту менш доступними… Для широкого впровадження школам потрібні індивідуальні, перевірені продукти, чіткі найкращі практики та покращення рівня обізнаності про штучний інтелект, хоча на даний момент найефективнішою стратегією залишаються фундаментальні засоби захисту — навчання, оцінка ризиків та планування дій у разі інцидентів». ***(Lauraine Langreo. AI Empowers Cyber***

Criminals. Could It Also Help Schools Fight Them? // e.Republic LLC (https://www.govtech.com/education/k-12/ai-empowers-cyber-criminals-could-it-also-help-schools-fight-them). 20.02.2026).

***

«У звіті Apono «Стан кіберризиків, пов'язаних з агентною ШІ, у 2026 році» зроблено висновок, що підприємства зацікавлені в агентної ШІ, але навмисно обмежують її впровадження, оскільки засоби контролю безпеки, особливо ідентифікація, доступ і дозволи, ще не достатньо досконалі, щоб забезпечити широку автономію. У глобальному дослідженні 98% респондентів заявили, що проблеми безпеки та даних вже уповільнили впровадження, додали етапи перевірки або звузили обсяг проектів; 77% повідомили про помірне уповільнення, а 21% — про значні затримки або скорочення…

Всі респонденти погодилися, що атаки на робочі процеси агентного ШІ будуть більш згубними, ніж традиційні кібератаки, проте лише 21% відчували себе готовими до таких інцидентів, а 98% повідомили про постійне протистояння між тиском на впровадження ШІ та пріоритетами кібербезпеки. Керівництво Apono стверджує, що ця реальність суперечить ринковим наративам про швидку заміну агентів ШІ: експерименти широко поширені, але керівники служб інформаційної безпеки «натискають на гальма», коли проекти переходять у стадію виробництва, доки не буде посилено фундаментальне управління доступом». ***(New Apono Report Reveals 98% of Cybersecurity Leaders Are Slowing Agentic AI Adoption Due to Insufficient Security Controls // Cision US Inc (https://www.prnewswire.com/il/news-releases/new-apono-report-reveals-98-of-cybersecurity-leaders-are-slowing-agentic-ai-adoption-due-to-insufficient-security-controls-302696914.html). 25.02.2026).***

***

«Новий багатонаціональний звіт Exabeam «Від впровадження до відповідальності: нова економіка штучного інтелекту в кібербезпеці» виявляє критичний парадокс у галузі: хоча 95% організацій збільшують свої бюджети на кібербезпеку в 2026 році, головним чином завдяки трансформації штучного інтелекту, керівники служб безпеки намагаються оцінити та обґрунтувати ці інвестиції перед зацікавленими сторонами бізнесу. Дослідження, в якому взяли участь 750 IT-керівників, показало, що штучний інтелект є одночасно головним чинником збільшення бюджетів (44%), першою інвестицією, яку скорочують (44%), і найскладнішою для обґрунтування (32%)…

Цей «розрив у демонстрації цінності» підкреслює значну розбіжність між показниками безпеки та бізнес-результатами. Хоча 87% керівників служб безпеки впевнені, що їхні інвестиції приносять цінність, 30% повідомляють, що їхні ради директорів не розуміють зв'язку між витратами на кібербезпеку та стійкістю бізнесу. Проблема полягає в тому, що вони покладаються на традиційні, доштучні показники, такі як середній час вирішення проблеми (MTTR), які в середовищі, що підтримується штучним інтелектом, вже не демонструють належного зниження ризиків. Як зазначив Керівник служби інформаційної безпеки Exabeam Кевін

Кірквуд, «ради директорів фінансують не швидше закриття квитків, а вимірюване зниження ризиків і стійкість бізнесу»…

Регіональні відмінності у впровадженні ШІ також вражають: Саудівська Аравія (75% повідомляють про поліпшення) є набагато більш агресивною, ніж Японія (27%) і Нідерланди (30%), що відображає різні національні та організаційні пріоритети. У звіті робиться висновок, що для збереження поточного обсягу бюджету керівники служб безпеки повинні вийти за межі простого впровадження ШІ та розробити нові рамки, які безпосередньо пов'язують ефективність безпеки з стійкістю бізнесу, перекладаючи технічні вдосконалення на мову бізнес-впливу. Якщо цього не зробити, існує ризик скорочення цих важливих бюджетів, коли економічні умови неминуче зміняться». ***(Exabeam Research: AI Accountability Becomes the New Mandate as Cybersecurity Economics Shift // Business Wire, Inc. (https://www.businesswire.com/news/home/20260224474207/en/Exabeam-Research-AI-Accountability-Becomes-the-New-Mandate-as-Cybersecurity-Economics-Shift). 24.02.2026).***

***

Штучний інтелект, як зброя кіберзлочинців

«Група Google Threat Intelligence повідомляє, що державні зловмисники, зокрема північнокорейська група UNC2970, все частіше використовують генеративну модель штучного інтелекту Gemini для прискорення кібератак. Група UNC2970, пов'язана з Lazarus Group, використовувала Gemini для розвідки, синтезуючи відкриті джерела інформації для профілювання цілей у сфері оборони та кібербезпеки, зокрема для картографування технічних ролей і зарплат, щоб підтримувати фішингові кампанії, замасковані під пропозиції про роботу… Ця тенденція поширюється на китайські та іранські групи; такі суб'єкти, як Mustang Panda та APT41, використовували цей інструмент для складання досьє на окремих осіб, усунення несправностей в експлойт-коді та розробки веб-оболонок, а іранська APT42 створювала персонажів для соціальної інженерії та кодувала скрипти… Окрім ручного зловживання, Google виявив такі шкідливі програми, як «HONESTCUE», яка зловживає API Gemini для генерації безфайлових корисних навантажень, та «COINBAIT», набір для фішингу, створений за допомогою штучного інтелекту. У звіті також детально описано атаки з вилученням моделей, спрямовані на клонування пропрієтарного штучного інтелекту шляхом систематичного запитування, що спонукало Google посилити свої заходи безпеки проти технік обходу на основі персони та закликати захисників застосовувати подібні можливості на основі штучного інтелекту, щоб відповідати швидкості розвитку загроз». ***(Ravie Lakshmanan. Google Reports State-Backed Hackers Using Gemini AI for Recon and Attack Support // The Hacker News (https://thehackernews.com/2026/02/google-reports-state-backed-hackers.html). 12.02.2026).***

***

«Deepfakes — синтетичний аудіо, відео та зображення, створені за допомогою передових технологій штучного інтелекту, особливо генеративних суперечливих мереж (GAN) — швидко еволюціонували від онлайн-цікавинок до потужних інструментів для шахрайства, маніпуляцій та дестабілізації, підриваючи основну передумову, що бачити — значить вірити. Доступні інструменти з відкритим кодом, комерційні платформи та пропозиції «deepfake-as-a-service» тепер дозволяють навіть акторам із середніми навичками створювати переконливі медіа з мізерних зразків, що дає можливість для зловживань у реальному світі — від шахрайства з підробкою голосу керівника (наприклад, переказ 220 000 євро у 2019 році) до спіфішингу та компрометації ділової електронної пошти, політичної дезінформації та вимагання за допомогою сфабрикованого компрометуючого контенту…

Результатом цього є ризики для окремих осіб (порушення конфіденційності, шкода репутації, фінансові втрати), організацій (соціальна інженерія, шахрайство, шкода бренду) та демократій (дезінформація виборців, зниження довіри до інститутів). Виявлення поєднує моделі штучного інтелекту/машинного навчання, які виявляють синтетичні артефакти (динаміку обличчя, освітлення, аудіовізуальні невідповідності), біометричні ознаки та водяні знаки, ручну та колективну перевірку, а також системи походження, що використовують метадані з захистом від підробки або блокчейн; проте кожен метод має свої обмеження в умовах гонки озброєнь у якості генерації, особливо з підробками низької роздільної здатності, в прямому ефірі або з урахуванням детекторів…

Тому для пом'якшення наслідків застосовуються технічні та організаційні заходи: інтеграція API-інтерфейсів для виявлення та інструментів визначення походження, моніторинг контенту в режимі реального часу та посилення аутентифікації, щоб чутливі дії ніколи не залежали виключно від голосу або відео (на користь MFA, токенів, поведінкового аналізу). Навчання та посібники з реагування на інциденти повинні готувати персонал до скептичного ставлення до термінових запитів, пов'язаних із засобами масової інформації, а міжгалузева співпраця, стандарти та еволюціонуючі правові рамки (розкриття інформації, підзвітність, санкції) допомагають обмежити зловживання, не придушуючи свободу вираження думок та інновації. У міру зростання реалістичності та доступності генеративної штучної інтелекту, лише мультидисциплінарний підхід — технічний прогрес, реформа політики та широка цифрова грамотність — може зберегти цифрову довіру та стійкість у все більш синтетичному медіа-просторі». ***(Joe Guerra. Deepfakes, Synthetic Media, and Digital Trust: The Cybersecurity Implications of Deepfake Technology and Methods for Detection and Mitigation // Cyber Defense Media Group (https://www.cyberdefensemagazine.com/deepfakes-synthetic-media-and-digital-trust-the-cybersecurity-implications-of-deepfake-technology-and-methods-for-detection-and-mitigation/). 19.02.2026).***

***

«Кібертероризм стає серйозною глобальною загрозою, оскільки сучасні суспільства все більше покладаються на цифрові системи в банківській сфері, охороні здоров'я, транспорті та державній діяльності. Терористи зараз використовують технології для здійснення атак з будь-якої точки світу, націлюючись на критичну інфраструктуру, викрадаючи конфіденційну інформацію, поширюючи страх і порушуючи роботу важливих служб. Ці атаки особливо небезпечні, оскільки злочинці можуть приховувати свою особу і швидко завдавати великомасштабної шкоди…

Кібертероризм передбачає використання комп'ютерів та Інтернету для залякування або примусу урядів чи населення з політичною або соціальною метою. На відміну від кіберзлочинності чи кібервійни, які можуть бути мотивовані прибутком або державним конфліктом, кібертероризм має на меті заподіяти шкоду, викликати страх і спричинити хаос. Атаки можуть включати злом енергомереж, викрадення військових секретів, поширення фейкових новин або напад на фінансові системи. Атака шкідливого програмного забезпечення на індійську атомну електростанцію Куданкулам у 2019 році, яку приписують трояну Dtrack, та атака Stuxnet на іранські ядерні об'єкти є реальними прикладами того, як кібертероризм може заподіяти фізичну та психологічну шкоду.

Еволюція кібертероризму була підсилена глобальною взаємопов'язаністю, геополітичною напруженістю та поширенням цифрових інструментів. Ранні кібератаки обмежувалися псуванням веб-сайтів або погрозливими електронними листами, але сьогоднішні атаки є більш витонченими і спрямовані на енергомережі, лікарні та урядові мережі. Екстремістські угруповання використовують соціальні мережі та зашифровані повідомлення для вербування членів, поширення пропаганди та координації атак…

Міжнародні та національні заходи включають зусилля Організації Об'єднаних Націй, Міжнародного союзу електрозв'язку та національних агентств, таких як індійська CERT-IN та Міністерство внутрішньої безпеки США. Ці організації працюють над поліпшенням кібербезпеки, координацією заходів реагування та розробкою правил відповідальної поведінки в кіберпросторі. Однак боротьба з кібертероризмом залишається складним завданням через здатність зловмисників діяти глобально та анонімно, швидкі технологічні зміни, відсутність універсальних правових рамок та обмеженість ресурсів у багатьох країнах…

У перспективі очікується, що загроза кібертероризму стане ще більш складною з розвитком штучного інтелекту, Інтернету речей та гібридних тактик ведення війни, що поєднують цифрові та фізичні атаки. Щоб протидіяти цим ризикам, країни повинні оновити законодавчу базу, посилити міжнародне співробітництво, інвестувати в навчання з питань кібербезпеки, сприяти розвитку партнерських відносин між державним і приватним секторами та підвищувати обізнаність громадян у питаннях кібербезпеки.

Підсумовуючи, кібертероризм становить серйозну і зростаючу загрозу для глобальної безпеки. У міру поглиблення цифрової залежності уряди та організації повинні співпрацювати з метою зміцнення захисту, вдосконалення політики та

налагодження міжнародної співпраці для захисту людей, систем та економік від цієї зростаючої загрози». ***(Cyber Terrorism: A New Threat To World Security – OpEd // Eurasia Review (https://www.eurasiareview.com/05022026-cyber-terrorism-a-new-threat-to-world-security-oped/). 05.02.2026).***

***

«Протягом шести місяців інфраструктура оновлень для Notepad++ — широко використовуваного текстового редактора для Windows — була скомпрометована хакерами, які, як підозрюється, працювали на китайську державу, що дозволило їм поширювати версії програми з вбудованими «задніми дверцятами» серед обраних цілей. Атака розпочалася в червні 2025 року, коли зловмисники отримали контроль над трафіком оновлень для notepad-plus-plus.org, перенаправляючи певних користувачів на шкідливі сервери, які встановлювали складний «задній вхід» під назвою Chrysalis. Notepad++ повністю відновив контроль над своєю інфраструктурою лише в грудні…

Зловмисники скористалися слабкими місцями в процесі оновлення Notepad++, зокрема недостатніми засобами перевірки в старих версіях та використанням самопідписаних сертифікатів. Навіть після внесення деяких виправлень зловмисники зберігали доступ до внутрішніх служб аж до грудня, що давало їм змогу продовжувати перенаправляти трафік оновлень. Бакдор Chrysalis, який характеризується як багатофункціональний і стійкий, давав змогу безпосередньо контролювати уражені пристрої. Про кілька інцидентів було повідомлено в організаціях, що мають інтереси в Східній Азії.

Дослідники в галузі безпеки відзначили, що атака була цілеспрямованою, а скомпрометовані сервери використовувалися для доставки шкідливого програмного забезпечення лише конкретним користувачам. Цей інцидент також висвітлив більш широкі ризики, оскільки пошукові системи переповнені рекламою троянських версій Notepad++ та шкідливих розширень, що збільшує загрозу для користувачів.

Розробники Notepad++ закликали всіх користувачів оновити програму до версії 8.9.1 або вище, а організаціям рекомендується заблокувати процес оновлення або обмежити доступ до Інтернету для Notepad++, якщо це можливо. Цей інцидент підкреслює виклики, з якими стикаються проекти з відкритим кодом у підтримці надійної безпеки, особливо з огляду на їх широке використання та обмежене фінансування…» ***(Dan Goodin. Notepad++ users take note: It's time to check if you're hacked // Condé Nast (https://arstechnica.com/security/2026/02/notepad-updater-was-compromised-for-6-months-in-supply-chain-attack/). 02.02.2026).***

***

«29 грудня 2025 року Польща зазнала скоординованої кібератаки, спрямованої проти понад 30 вітрових і сонячних електростанцій, великої теплоелектростанції та виробничого підприємства. Атаки, що відбулися під час суворої зимової погоди, мали суто деструктивний характер і були спрямовані на пошкодження критичної інфраструктури, а не на викрадення інформації. Це стало першою задокументованою деструктивною операцією, здійсненою

високотехнологічною групою зловмисників проти європейської енергетичної інфраструктури, що свідчить про значне посилення кіберзагроз для цього сектору…

Зловмисники зосередилися на підстанціях, які підключають відновлювані джерела енергії до розподільної мережі, націлившись на пристрої промислової автоматизації, такі як віддалені термінальні пристрої, інтерфейси «людина-машина», реле захисту та комунікаційне обладнання. Проникнувши у внутрішні мережі, зловмисники провели детальну розвідку, а потім застосували спеціально розроблене шкідливе програмне забезпечення для знищення даних, яке безповоротно знищує дані та пошкоджує прошивку…

Комунікація між електростанціями, що використовують відновлювані джерела енергії, та оператором розподільчої системи була порушена, хоча виробництво електроенергії продовжувалося. Аналітики з cert.pl пов'язали інфраструктуру атаки з відомими групами зловмисників, серед яких «Static Tundra», «Berserk Bear», «Ghost Blizzard» та «Dragonfly», які раніше вже здійснювали атаки на енергетичний сектор.

Зловмисники використовували ідентичне шкідливе програмне забезпечення для знищення даних на декількох цілях, виконуючи частково автоматизовані послідовності атак після декількох тижнів таємного проникнення в мережу. Хоча технологія виявлення та реагування на кінцевих точках заблокувала шкідливе програмне забезпечення на теплоелектростанції, виробничий об'єкт також зіткнувся з подібною атакою. Операція продемонструвала ретельне планування та тактичний перехід до руйнівних кампаній, підкресливши зростаючий ризик для критичної інфраструктури з боку кіберзлочинців, пов'язаних з державою». ***(Tushar Subhra Dutta. 30 Wind and Solar Farms in Poland Faced Coordinated Cyberattacks // Cyber Security News (https://cybersecuritynews.com/solar-farms-in-poland-faced-coordinated-cyberattacks/). 02.02.2026).***

***

«Згідно з останнім звітом Cofense, у 2025 році кожні 19 секунд відбувалася зловмисна атака електронною поштою — це більш ніж удвічі перевищує показник 2024 року — що було зумовлено центральною роллю штучного інтелекту в сучасних фішингових кампаніях. Штучний інтелект кардинально змінив фішинг, дозволивши зловмисникам створювати високо персоналізовані електронні листи, динамічно адаптувати фішингові сторінки до пристроїв жертв, генерувати тисячі унікальних варіантів атак та керувати зараженими системами у великих масштабах. Традиційні засоби захисту периметра стають все менш ефективними, оскільки загрози тепер трансформуються після доставки, що вимагає від організацій впровадження засобів видимості після доставки, людської розвідки та контекстного виявлення…

Поліморфні атаки стали нормою: 76% URL-адрес, що містять початкове зараження, і 82% шкідливих файлів у фішингових атаках є унікальними, що дозволяє їм обходити традиційні засоби захисту на основі зіставлення зразків. Зловмисники використовують загальнодоступні дані, такі як домашні адреси та

активність у соціальних мережах, щоб персоналізувати кожне фішингове повідомлення, роблячи їх надійними та унікальними.

Зловмисники також використовують динамічні фішингові сайти, які доставляють різні корисні навантаження залежно від браузера, операційної системи або пристрою жертви. Ці сайти можуть надавати виконувані файли Windows для користувачів ПК, пакети macOS для користувачів Mac та оптимізовані сторінки для збору облікових даних для мобільних відвідувачів. Сучасні фішингові набори виявляють засоби безпеки та перенаправляють аналітиків на легітимні сайти, ще більше ухиляючись від виявлення…

Кількість випадків компрометації ділової електронної пошти (BEC) різко зросла, а атаки з використанням штучного інтелекту зараз становлять 18% від усіх шкідливих електронних листів. Ці текстові повідомлення, що не містять граматичних помилок, дуже схожі на легітимні внутрішні повідомлення, обходять більшість засобів контролю безпеки та використовують довіру організації.

Крім того, зловмисники використовують законні інструменти віддаленого доступу в безпрецедентних масштабах, що призвело до 900% зростання зловживань такими платформами, як ConnectWise ScreenConnect і GoTo Remote Desktop. Шкідливі файли розміщуються на надійних платформах, підписуються дійсними сертифікатами і передаються через встановлені домени, що ускладнює їх виявлення системами виявлення кінцевих точок.

Загалом, у звіті підкреслюється нагальна необхідність для організацій вийти за межі традиційних засобів захисту та впровадити передові, контекстно-орієнтовані стратегії безпеки для боротьби з швидкозмінним ландшафтом загроз, сформованим фішингом та кібератаками на основі штучного інтелекту». ***(Ian Barker. AI-powered phishing attacks doubled in 2025 // BetaNews, Inc. (https://betanews.com/article/ai-powered-phishing-attacks-doubled-in-2025/). 04.02.2025).***

***

«Jaguar Land Rover (JLR) повідомила про подальші значні збитки, оскільки продовжує відновлюватися після масштабної кібератаки, яка змусила компанію зупинити виробництво на всіх своїх заводах у Великобританії на п'ять тижнів, починаючи з 1 вересня 2025 року. Компанія зафіксувала додаткові витрати у розмірі 64 мільйони фунтів стерлінгів, пов'язані з хакерською атакою, що збільшило загальні витрати, пов'язані з кібератакою, до щонайменше 260 мільйонів фунтів стерлінгів за рік. Ці перебої призвели до базового збитку JLR у розмірі 310 мільйонів фунтів стерлінгів до оподаткування за третій квартал, що є різким відхиленням від прибутку в розмірі 523 мільйонів фунтів стерлінгів роком раніше. Доходи за квартал впали на 39% у порівнянні з аналогічним періодом минулого року до 4,5 мільярда фунтів стерлінгів, оскільки обсяги продажів постраждали від зупинки виробництва, а нормальна робота була відновлена лише в середині листопада…

Збитки JLR ще більше поглибилися через діючі мита США, заплановане припинення виробництва старих моделей Jaguar перед випуском нових та погіршення ринкових умов у Китаї. Збитки компанії з початку року становлять 444

млн фунтів стерлінгів, порівняно з прибутком у 1,6 млрд фунтів стерлінгів у попередньому році.

Новий генеральний директор П.Б. Баладжі назвав цей квартал «складним», вказавши на кіберінцидент, перехід на нові моделі та мита як ключові фактори. Однак він висловив оптимізм щодо значного поліпшення показників у четвертому кварталі, підкресливши, що компанія зосереджена на відновленні та управлінні глобальними викликами. Витрати на кібератаку включають найм консультантів для управління інцидентом, але не враховують втрачені продажі або збільшення витрат на інженерні роботи, що свідчить про те, що реальний фінансовий вплив може бути ще більшим». ***(Jaguar Land Rover reports £310m loss after lengthy cyber attack // ITV Consumer Limited (https://www.itv.com/news/central/2026-02-05/jlr-reports-310m-loss-after-lengthy-cyber-attack). 05.02.2026).***

***

«Conpet, національний оператор нафтопроводів Румунії, повідомив про кібератаку, яка порушила роботу його бізнес-систем і вивела з ладу його веб-сайт, хоча основні операції та послуги з транспортування нафти не постраждали. Conpet управляє майже 4000 кілометрів трубопроводів, постачаючи сиру нафту та нафтопродукти на нафтопереробні заводи по всій країні. Компанія підтвердила, що, хоча її корпоративна IT-інфраструктура зазнала впливу, її операційні технології, включаючи SCADA та телекомунікаційні системи, не були порушені, що забезпечило безперебійне транспортування нафти.

Атака, яка сталася у вівторок, розслідується за допомогою національних органів з кібербезпеки. Conpet також повідомила про це Управління з розслідування організованої злочинності та тероризму (DIICOT) і подала кримінальну скаргу. Відповідальність за атаку взяла на себе група хакерів Qilin, яка розмістила Conpet на своєму сайті в даркнеті і заявила про викрадення майже 1 ТБ внутрішніх документів, включаючи фінансові записи та скани паспортів…

Цей інцидент став продовженням серії недавніх атак програм-вимагачів на критичну інфраструктуру Румунії, зокрема на сектори водопостачання, енергетики та охорони здоров'я. Протягом минулого року такі організації, як Romanian Waters, Oltenia Energy Complex, Electrica Group та понад 100 лікарень, зазнали подібних зломів, що підкреслює зростаючу загрозу програм-вимагачів для основних служб Румунії». ***(Sergiu Gatlan. Romanian oil pipeline operator Conpet discloses cyberattack // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/romanian-oil-pipeline-operator-conpet-discloses-cyberattack-qilin-ransomware/). 05.02.2026).***

***

«Цифровий сквотинг перетворився з простої проблеми, пов'язаної з торговими марками, на серйозну загрозу кібербезпеці, про що свідчить рекордний обсяг спорів щодо доменів, розглянутих Всесвітньою організацією інтелектуальної власності (ВОІВ) у 2025 році — 6200, що на 68% більше, ніж у 2020 році. Злочинні мережі зараз використовують підроблені домени не тільки для їх перепродажу з метою отримання прибутку, але й для крадіжки даних клієнтів,

розповсюдження шкідливого програмного забезпечення та підриву репутації брендів за допомогою різних обманних тактик. До них належать: типосквотинг, що передбачає реєстрацію поширених помилок у написанні популярних веб-сайтів; комбосквотинг, що додає ключові слова до законних назв брендів; TLD-сквотинг, що використовує альтернативні розширення доменів, такі як .net або .org, для імітації відомих .com-бізнесів; та гомографічні атаки, що використовують візуально схожі символи з різних алфавітів для створення майже невиявних підробок. Дослідження SecPod виявило 19-кратне збільшення кількості зловмисних кампаній сквоттингу між кінцем 2024 року та серединою 2025 року, причому 99% доменів, що піддалися сквоттингу, використовувалися для фішингу облікових даних або поширення шкідливого програмного забезпечення…

Серйозність цієї проблеми ілюструє досвід компанії Decodo (раніше Smartproxy), провідного постачальника веб-даних, який зіткнувся з агресивним підробленням з боку зловмисників у Китаї, які зареєстрували домени smartproxy.org і smartproxy.cn, щоб імітувати його законні послуги. Клієнти, які несвідомо взаємодіяли з цими клонами, втратили гроші на послуги, які вони ніколи не отримували, а коли підробки провалилися, це призвело до негативної реакції, яка пошкодила рейтинг довіри до справжньої компанії. Як зазначив генеральний директор Decodo Витаутас Савіцкас, шахраї не просто крадуть гроші — кожен підроблений сайт ускладнює чесним компаніям завоювання довіри. Гучні суперечки щодо доменів ще більше підкреслюють цю проблему: Tesla роками працювала під доменом teslamotors.com, перш ніж, за повідомленнями, придбала tesla.com за кілька мільйонів доларів; ByteDance виграла суперечку в WIPO щодо tiktoks.com після відмови від пропозиції в розмірі 145 000 доларів від двох осіб, які зареєстрували домен за 2000 доларів; Microsoft уклала мирову угоду з підлітком на ім'я Майк Роу, який зареєстрував mikerowesoft.com; а шахраї використовували підроблені домени Amul для здійснення шахрайських схем з працевлаштуванням та франчайзингом з 2018 по 2020 рік.

Фінансові ризики є надзвичайно великими: у 2025 році фішинг-атаки, що здійснюються з шахрайських доменів, коштуватимуть організаціям у середньому 4,8 мільйона доларів за кожну злом, оскільки жертви несвідомо надають свої облікові дані або завантажують програми-вимагачі. Експерти закликають підприємства перейти від реактивних до проактивних стратегій. Вайдотас Юкнис, головний комерційний директор Decodo, радить компаніям негайно провести аудит своїх доменних портфелів і вжити заходів захисту, включаючи захисну реєстрацію поширених помилок в написанні та альтернативних розширень, перш ніж їх заберуть шахраї, послуги постійного моніторингу, що сканують нові реєстрації доменів, схожих на їхній бренд, та заходи з інформування клієнтів, що чітко перелічують офіційні домени та попереджають користувачів про відомих шахраїв. В епоху, коли домен компанії є її візитною карткою, залишення його без охорони спонукає злочинців використовувати вразливі місця, що може коштувати бізнесу надто дорого…» ***(Dhivya. Cybercriminals Use Malicious Cybersquatting Attacks to Distribute Malware and Hijack Data // Cyber Security News (https://cybersecuritynews.com/cybercriminals-use-malicious-cybersquatting-attacks/). 07.02.2023).***

***

«Офіційна оцінка Кенії щодо збитків від кіберзлочинів у розмірі 30 мільярдів шилінгів на 2025 рік є, майже напевно, занадто низькою, згідно з новим ринковим дослідженням ESET, яке вказує на поширене недооцінювання кількості атак, особливо атак з використанням програм-вимагачів. Хоча ESET прогнозує 40-відсоткове зростання кількості публічно розкритих випадків використання програм-вимагачів у всьому світі у 2025 році, інциденти в Кенії в основному замовчуються, щоб уникнути шкоди репутації, перебоїв у роботі або пильного контролю з боку регуляторних органів, що не дозволяє країні побачити справжній масштаб загрози. Ця культура мовчання маскує зростаючу вразливість критично важливих секторів, в той час як глобальні групи, що надають послуги з використання програм-вимагачів, такі як Akira, Qilin і більш прихований новачок Warlock, вдосконалюють свої тактики, а штампи на базі штучного інтелекту, такі як PromptLock, демонструють нову хвилю автоматизованого створення скриптів у режимі реального часу…

Навіть при обмеженій видимості програм-вимагачів, інші кіберризики в Кенії є надзвичайно очевидними. Шахрайські схеми з використанням штучного інтелекту — відео з глибокою підробкою, фішингові сторінки, створені за допомогою штучного інтелекту, та швидкоплинні онлайн-реклами — набули широкого поширення, що призвело до 62-відсоткового зростання кількості шахрайських кампаній на основі HTML, таких як інвестиційна афера Nomani. В одному з недавніх випадків було використано відео з глибокою підробкою відомого кенійського політика для продажу фальшивих інвестицій, що ілюструє, наскільки переконливо штучний інтелект може посилити охоплення та вплив. Мобільні загрози також зростають: ESET зафіксував 87% глобальне зростання шкідливого програмного забезпечення, пов'язаного з NFC, включаючи нову сім'ю RatOn, яка поєднує атаки ретрансляції NFC з можливостями троянських програм віддаленого доступу.

ESET попереджає, що без відвертого розкриття інформації про інциденти та проактивних заходів захисту — від інструментів безпеки з підтримкою штучного інтелекту до надійних планів резервного копіювання та відновлення — кенійські організації можуть серйозно недооцінювати як частоту, так і складність атак, спрямованих проти них…» ***(JACKTONE LAWI. Under-reporting masks scale of ransomware crisis, ESET warn // The Star (https://www.the-star.co.ke/business/2026-02-07-under-reporting-masks-scale-of-ransomware-crisis-eset-warn). 07.02.2026).***

***

«Рада з кібербезпеки ОАЕ визначила фінансові дані як основну ціль для онлайн-шахраїв, виявивши, що приблизно 60 відсотків фінансових кібератак походять від викрадених облікових даних. Відповідно, рада закликає як приватних осіб, так і організації посилити захист від нових цифрових загроз, зазначаючи, що скомпрометовані паролі часто слугують шлюзами для крадіжки особистих даних та несанкціонованого доступу до банківських рахунків. Для зменшення цих ризиків рада наголошує на важливості основних запобіжних заходів, таких як оновлення операційних систем, видалення ненадійних додатків та

уникнення зберігання конфіденційних даних на незахищених пристроях, при цьому особливо виділяючи двофакторну автентифікацію як один з найефективніших бар'єрів проти вторгнення…

Окрім технічних заходів безпеки, рада попередила, що кіберзлочинці часто використовують непрямі шляхи, такі як зламані електронні поштові або соціальні мережі, або застосовують обманні тактики, наприклад, імітують легітимний брендинг банку у фальшивих рекламних оголошеннях, щоб обдурити користувачів. Щоб протидіяти таким спробам соціального інжинірингу, користувачам рекомендується ретельно перевіряти повідомлення, уникати підозрілих посилань і утримуватися від здійснення банківських операцій через публічні мережі Wi-Fi. Зрештою, рада рекомендує прийняти більш безпечні цифрові звички, включаючи використання надійних, унікальних паролів, безпечних методів оплати та миттєвих банківських сповіщень, щоб забезпечити швидке виявлення та повідомлення про будь-яку незвичайну активність…» ***(Six in ten financial cyberattacks start with stolen login details // Al Nisr Publishing LLC (https://gulfnews.com/uae/people/six-in-ten-financial-cyberattacks-start-with-stolen-login-details-1.500435954). 08.02.2026).***

***

«У жовтні 2025 року уряди з усього світу зібралися в Ханої, В'єтнам, щоб підписати Конвенцію Організації Об'єднаних Націй про боротьбу з кіберзлочинністю, яка зараз відома як «Ханойська конвенція». Як перший глобальний договір, присвячений запобіганню, розслідуванню та судовому переслідуванню кіберзлочинів, Ханойська конвенція є важливим кроком вперед у міжнародній співпраці, хоча геополітична напруженість може ускладнити її впровадження.

Прийнята Генеральною Асамблеєю ООН у грудні 2024 року та відкрита для підписання в жовтні 2025 року, Конвенція була підписана 74 країнами і залишатиметься відкритою для підписання до кінця 2026 року. Спочатку договір був ініційований Росією як альтернатива Будапештській конвенції Ради Європи, що викликало дискусії щодо побоювань, що широкі визначення кіберзлочинів можуть бути використані для придушення інакомислення або прав людини…

Ханойська конвенція встановлює комплексну систему збору, збереження, обміну та використання електронних доказів за межами країни — сфера, яка раніше гальмувалася через невідповідність національних законів та повільну взаємну правову допомогу. Країни, що підписали конвенцію, погоджуються криміналізувати конкретні кіберзлочини, такі як незаконний доступ до комп'ютерних систем, втручання в дані, онлайн-шахрайство та злочини, пов'язані з експлуатацією дітей. Конвенція також встановлює глобальні стандарти поводження з електронними доказами, включаючи збереження даних, законний обшук і вилучення, а також збір даних про трафік у режимі реального часу під час серйозних розслідувань. Також встановлюються механізми взаємної правової допомоги, екстрадиції та цілодобова мережа національних контактних пунктів для забезпечення швидкої міжнародної співпраці…

Після підписання країни повинні завершити внутрішні процеси з метою імплементації Конвенції та подати документи про ратифікацію до ООН. Договір

набере чинності через 90 днів після 40-ї ратифікації. Потім буде скликано Конференцію держав-учасниць (COSP) для нагляду за імплементацією та сприяння співпраці, з можливістю укладення в майбутньому протоколів для протидії новим загрозам.

Для транснаціональних компаній Ханойська конвенція означає перехід до більш гармонізованого глобального кіберзаконодавства, більш суворого звітування про порушення та більш тісної співпраці з правоохоронними органами. Компаніям доведеться узгодити програми кібербезпеки на глобальному рівні, вдосконалити протоколи цифрової криміналістики та зберігання даних, переглянути плани реагування на інциденти та підготуватися до посиленого контролю щодо доступу до даних та захисту прав людини. Важливе значення матимуть державно-приватні партнерства, оскільки Конвенція наголошує на необхідності співпраці у сфері аналізу загроз та обміну інформацією між урядами та приватним сектором…

Ханойська конвенція є історичною віхою у глобальному кіберуправлінні, але її успіх залежатиме від ефективної співпраці між державним і приватним секторами та здатності долати геополітичні виклики в процесі впровадження та забезпечення дотримання її положень країнами». ***(Justine Phillips, Manh Hung Tran and Alex Do. The Hanoi Convention: How the World is Combatting Cybercrime and What the Global Treaty Means for Businesses // Baker McKenzie (https://connectontech.bakermckenzie.com/the-hanoi-convention-how-the-world-is-combatting-cybercrime-and-what-the-global-treaty-means-for-businesses/#page=1). 03.02.2026).***

***

«Bitdefender виявив складну схему шахрайства, спрямовану на європейських та американських покупців напередодні Зимових Олімпійських ігор 2026 року в Мілані-Кортіні. Шахрайські веб-сайти, що імітують офіційний магазин олімпійської атрибутики, рекламуються за допомогою підроблених рекламних оголошень Meta, які пропонують знижки до 80% на «офіційну» атрибутику. Ці майже ідентичні копії використовують ті самі фотографії товарів, колірну гаму, брендинг та колекції, щоб ввести користувачів в оману…

Натискання на рекламу веде до сайтів, призначених для збору платіжних даних, адрес, номерів телефонів, електронних адрес та облікових даних для входу. Жертви можуть отримати підроблені товари або взагалі нічого, а їхні особисті дані наражаються на ризик. Шахрайство базується на доменах, зареєстрованих з інтервалом у кілька днів, та новостворених сторінках у Facebook, що свідчить про скоординовану операцію, яка швидко змінюється, щоб уникнути виявлення.

Офіційний магазин Олімпійських ігор пропонує скромні знижки, такі як «Зареєструйтеся та заощаджуйте 15%», тоді як підроблені сайти рекламують надзвичайні знижки до 80%. Багато шахрайських сайтів зникають незабаром після обробки платежів, унеможливлюючи повернення коштів. Bitdefender радить перевіряти деталі реєстрації домену, бути обережними щодо нереалістичних знижок та перевіряти історію сторінки у Facebook…

Прес-служба Milano Cortina 2026 підтвердила, що їй відомо про несанкціоновані сайти, які незаконно використовують бренд Ігор, і повідомляє про

них владі для їхнього видалення. Meta поки що не прокоментувала цю ситуацію. З наближенням Ігор масштаб і витонченість шахрайства ставлять під загрозу тисячі потенційних покупців». ***(Emilio Parodi. Fake Milano Cortina sites target thousands with discount scams, cybersecurity firm says // Reuters (https://www.reuters.com/sports/fake-milano-cortina-sites-target-thousands-with-discount-scams-cybersecurity-2026-02-17/). 17.02.2026).***

***

«Системи бронювання та інформації німецького залізничного оператора знову доступні для всіх клієнтів після того, як у вівторок вони були виведені з ладу внаслідок розподіленої атаки типу «відмова в обслуговуванні» (DDoS), повідомила залізниця в середу.

«Наші контрзаходи були ефективними і дозволили мінімізувати вплив на наших клієнтів», — написала Deutsche Bahn у своєму блозі, не уточнюючи, хто міг бути відповідальним за цю атаку.

Deutsche Bahn раніше ставала об'єктом дій, які німецькі власті підозрюють у саботажі, зокрема, зловмисники перерізали оптоволоконні кабелі та змусили зупинити залізничний рух». ***(German railway booking systems hit by DDoS attack // Reuters (https://www.reuters.com/technology/german-railway-booking-systems-hit-by-ddos-attack-2026-02-18/). 18.02.2026).***

***

«Об'єднані Арабські Емірати запобігли організованим кібератакам, спрямованим на цифрову інфраструктуру та життєво важливі сектори країни, повідомило в суботу державне інформаційне агентство.

Атаки «включали спроби проникнення в мережі, розгортання програм-вимагачів та проведення систематичних фішингових кампаній, спрямованих на національні платформи», а також використання технологій штучного інтелекту для розробки засобів нападу, додало агентство. У повідомленні не вказано, хто несе відповідальність за ці атаки». ***(UAE foils cyber attacks, state news agency says // Reuters (https://www.reuters.com/world/middle-east/uae-foils-cyber-attacks-state-news-agency-says-2026-02-21/). 21.02.2026).***

***

«…Звіт Unit 42® 2026 Global Incident Response Report, в якому проаналізовано понад 750 серйозних кіберінцидентів у 50 країнах, виявляє критичні зміни в ландшафті загроз: атаки стають швидшими, масштабнішими та все більше покладаються на використання надійних з'єднань. Зловмисники використовують штучний інтелект для скорочення термінів, і витік даних відбувається всього за 72 хвилини — у чотири рази швидше, ніж у попередньому році. Ідентичність стала основним засобом атаки, який використовується майже в 90% випадків, оскільки зловмисники все частіше «входять» у систему за допомогою викрадених облікових даних, щоб обійти захист. Ризики ланцюга поставок і діяльність на основі браузера також є значними векторами, оскільки зловмисники зловживають сторонніми SaaS-додатками та

рутинними робочими процесами, щоб розширити свій вплив… Крім того, тактика вимагання виходить за межі шифрування: кількість атак на основі шифрування зменшилася на 15% на користь прямого викрадення даних. Незважаючи на таку витонченість, більшість порушень все ще пов'язані з можливими витоками, а не з новими способами зловживання; понад 90% інцидентів сталися через неправильну конфігурацію, розростання інструментів та прогалини у видимості. Для боротьби з цим керівникам служб безпеки рекомендується зменшити вразливість шляхом захисту всієї екосистеми, мінімізувати вплив за допомогою більш суворого управління ідентифікацією та збільшити швидкість реагування, використовуючи видимість на основі штучного інтелекту для стримування загроз, перш ніж вони переростуть у повномасштабні порушення». ***(Sam Rubin. 2026 Unit 42 Global Incident Response Report — Attacks Now 4x Faster // Palo Alto Networks (https://www.paloaltonetworks.com/blog/2026/02/unit-42-global-ir-report/). 17.02.2026).***

***

«Оператор готелів і казино Wynn Resorts у Лас-Вегасі підтвердив інцидент з кібербезпекою, в результаті якого третя сторона отримала доступ до даних, що належать нинішнім і колишнім співробітникам, хоча, за повідомленнями, це не вплинуло на роботу з клієнтами та їхній досвід. Відповідальність за це взяла на себе хакерська група ShinyHunters, яка заявила про викрадення понад 800 000 записів, включаючи номери соціального страхування та інформацію про зарплати, і зажадала викуп у розмірі 1,5 мільйона доларів під загрозою витоку даних до 23 лютого…

Хоча статус платежу залишається незрозумілим, представник компанії заявив, що зловмисники стверджують, що видалили дані, і жодних доказів їх оприлюднення не виявлено. У відповідь Wynn пропонує співробітникам моніторинг кредитів і співпрацює з зовнішніми консультантами для посилення безпеки. Тим часом у федеральному суді позивач, який представляє інтереси клієнтів, звинувачує Wynn у нездатності усунути відомі ризики кібербезпеки, посилаючись на попередні порушення в галузі та власні документи компанії, подані до Комісії з цінних паперів і бірж (SEC), в яких визнаються вразливості». ***(David Charns. Wynn Resorts target of cybersecurity breach // Nexstar Media Inc. (https://www.8newsnow.com/news/local-news/wynn-resorts-target-of-cybersecurity-breach-lawsuit-says/). 24.02.2026).***

***

«…8 лютого 2026 року авіакомпанія Air Côte d'Ivoire, національний авіаперевізник Кот-д'Івуару, зазнала кібератаки, в результаті якої було викрадено невідому кількість даних, хоча польоти продовжувалися без перебоїв завдяки протоколам безперебійної роботи авіакомпанії. Після виявлення інциденту компанія повідомила про нього національні органи з кібербезпеки, зокрема Національне агентство з кібербезпеки Кот-д'Івуару (ANSSI-CI) та Орган регулювання телекомунікацій Кот-д'Івуару (ARTCI), і залучила експертів для розслідування порушення та зміцнення своїх IT-систем. Хоча

авіакомпанія офіційно не назвала винуватців, джерела інформації про загрози вказують, що відповідальність за це взяла на себе група хакерів INC Ransom, яка заявила про викрадення 194 ГБ даних. INC Ransom, активна з 2023 року, відома тим, що атакує відомі організації, такі як Xerox і NHS Scotland, погрожуючи опублікувати викрадені дані, якщо викуп не буде сплачений…» ***(Anton Mous. Air Côte d'Ivoire reveals cyberattack: "some data was stolen" // Cybernews (https://cybernews.com/cybercrime/air-cote-divoire-cyberattack-data-stolen/). 25.02.2026).***

***

«У звіті CrowdStrike «Глобальні загрози 2026 року» міститься попередження про те, що кібервтручання прискорюються до швидкості роботи машин, причому найшвидший спостережуваний «час прориву» (інтервал від початкового доступу до побічного переміщення) становить лише 27 секунд, а середній показник для суб'єктів, що мають фінансову мотивацію, у 2025 році скоротиться до 29 хвилин, що звужує вікно для захисників, щоб виявити та стримати атаки до ескалації привілеїв, виявлення даних або розгортання програм-вимагачів. Цей стрибок зумовлений широким використанням зловмисниками штучного інтелекту для автоматизації розвідки, створення шкідливих скриптів та вдосконалення кампаній з фішингу та крадіжки облікових даних — операції з використанням штучного інтелекту зросли на 89% у порівнянні з минулим роком, — тоді як самі системи штучного інтелекту стають мішенями через швидке введення та експлуатацію платформ розробки для підтримання стійкості…

Супротивники все частіше «живуть за рахунок землі», зловживаючи законними хмарними сервісами, платформами SaaS та скомпрометованими ідентичностями, що дозволяє їм змішувати зловмисну діяльність із звичайним трафіком і здійснювати швидке викрадення даних, іноді вже за кілька хвилин після отримання першого доступу. Традиційні, ручні, точкові методи безпеки не можуть йти в ногу з автоматизацією, штучним інтелектом та хмарними шляхами атак; у звіті стверджується, що ефективний захист зараз вимагає постійного моніторингу, автоматичного виявлення та майже миттєвої реакції, оскільки якщо середовища не спроектовані для майже миттєвої реакції, зловмисники можуть вже поширитися по мережі, перш ніж хтось зрозуміє, що відбувається злом». ***(David Unyime Nkanta. Cyberattack Breakout in Just 27 Seconds? 2026 Threat Report Reveals Shocking Speed // IBTimes LLC (https://www.ibtimes.co.uk/cybersecurity-report-ai-driven-threats-1781320). 24.02.2026).***

***

«В останньому звіті Amazon про загрози, присвяченому «кібератаці на Amazon AI», виявлено, що з 11 січня по 18 лютого зловмисники захопили понад 600 пристроїв у 55 країнах, скориставшись незахищеними портами управління та слабкою однофакторною автентифікацією, а не складними вразливостями. Керівник служби інформаційної безпеки Amazon CJ Moses заявив, що вразливості FortiGate не використовувалися; натомість фундаментальні

прогалини в безпеці дозволили зловмисникам з низьким та середнім рівнем кваліфікації швидко розширити свої можливості, використовуючи комерційно доступні технології штучного інтелекту для створення скриптів атак, автоматизації розвідки, планування латеральних переміщень та переходу від добре захищених цілей до більш легких…

Після проникнення через брандмауери зловмисники викрали повні конфігурації пристроїв, включаючи облікові дані SSL-VPN, паролі адміністраторів та карти мережі, що дозволило їм отримати більш глибокий доступ до Active Directory та систем резервного копіювання. Amazon оцінив це як підготовку до майбутнього вимагання викупу, а не як негайне порушення роботи. Те, що кампанія базувалася на неправильних налаштуваннях, а не на CVE, підкреслює постійні прогалини в гігієні безпеки та ілюструє, як штучний інтелект прискорює операції зловмисників… Amazon поділився індикаторами компрометації та закликав організації посилити захист периферійних пристроїв, запровадити багатофакторну автентифікацію та стежити за поведінкою після експлуатації, попередивши, що захист повинен розвиватися в темпі впровадження штучного інтелекту до 2026 року». ***(Anudeep Mahavadi. Amazon AI Cyberattack Hits 600 FortiGate Devices // Analytics Insight (https://www.analyticsinsight.net/news/amazon-ai-cyberattack-hits-600-fortigate-devices). 21.02.2026).***

***

«Аналіз даних про страхові виплати за кіберзлочини за 2025 рік, проведений компанією Resilience, показує стратегічну зміну в економіці кіберзлочинності: зараз зловмисники віддають перевагу крадіжці даних і тривалим, багатоетапним вторгненням, а не простому шифруванню. Вимоги про викуп, спрямовані виключно на приховування викрадених даних, зросли з 49% заяв у першій половині року до 65% у другій половині, що становить 57% від усіх інцидентів загалом, оскільки зловмисники обходять дедалі надійніші стратегії резервного копіювання. Шкідливе програмне забезпечення для викрадення інформації стало критичним попередником цих атак: понад 2 мільярди облікових даних було зібрано і часто виявлено в середовищах жертв перед розгортанням програм-вимагачів, що підкреслює його важливість як сигналу раннього попередження…

У звіті також підкреслюється зростаюча витонченість таких груп зловмисників, як Interlock, які, як було виявлено, шукають у викрадених даних поліси кіберстрахування, щоб адаптувати вимоги щодо викупу та максимізувати виплати. Ризик, пов'язаний з постачальниками, став основною вразливістю, що становить 18% від загальних збитків у портфелі Resilience, оскільки зловмисники використовують механізми скидання паролів і проникають у репозиторії відкритого коду, щоб викликати ланцюгові порушення… Ці тенденції свідчать про нову реальність, в якій кібератаки є більш обдуманими, а їхні наслідки виходять далеко за межі початкового інциденту, накопичуючись протягом місяців або навіть років. Щоб протидіяти цій моделі кіберризику «все, скрізь, одночасно», Resilience рекомендує організаціям надавати пріоритет інвестиціям у запобігання втраті даних, архітектуру нульової довіри, проактивний моніторинг облікових даних,

настільні вправи та плани дій постачальників на випадок надзвичайних ситуацій, одночасно забезпечуючи, щоб їх страхове покриття відображало підвищені рівні серйозності 2025 року, а не історичні середні значення». ***(Resilience 2025 Cyber Risk Report reveals evolving economics of extortion, material cyber losses // Industrial Cyber (https://industrialcyber.co/news/resilience-2025-cyber-risk-report-reveals-evolving-economics-of-extortion-material-cyber-losses/). 27.02.2026).***

***

«Згідно з білою книгою південнокорейської компанії CYTUR за 2026 рік, програми-вимагачі та атаки на ланцюги поставок все частіше проникають в операційні технології (OT) суден, а нові правила IACS мають на меті перевести морську галузь від паперової відповідності до доведеної кіберстійкості. У звіті, що базується на даних платформи CYTUR з аналізу загроз, зазначається, що кількість кіберінцидентів у морській галузі зросла на 103% між 2024 і 2025 роками, що пов'язано з підвищенням рівня підключення на борту суден. Зловмисники тепер безпосередньо націлюються на OT-системи, такі як контроль баластної води та моніторинг двигунів, що в деяких випадках призводить до повного зупинення роботи суден. Вразливість ланцюгів постачання також стала критичною точкою входу, оскільки зловмисники використовують залежність програмного забезпечення, щоб заразити кілька суден одним порушенням, і використовують скомпрометовані супутникові канали для передачі сфальсифікованої інформації про судна…

Оскільки судна, побудовані відповідно до єдиних вимог IACS E26 та E27, почнуть поставлятися в 2026 році, галузь стоїть перед вирішальним моментом, коли кібербезпека буде перевірена на практиці під час морських випробувань, що зробить її центральним елементом «права на експлуатацію» судна. Ця зміна підкреслює зростаючу важливість не тільки захисних заходів контролю, але й здатності швидко відновлюватися після інциденту, оскільки кібербезпека переходить від технічного аспекту до основної операційної необхідності». ***(Arnel Murga. CYTUR flags cyber risk to vessel operations // Antares Digital Group (https://thedigitalship.com/news/maritime-satellite-communications/cytur-flags-cyber-risk-to-vessel-operations/). 23.02.2026).***

***

«Австралійська птахівнича група Hazeldenes підтвердила, що її виробництво було порушено внаслідок кібератаки, виявленої 19 лютого, що змусило компанію вжити негайних заходів для локалізації порушення, залучити зовнішніх експертів з безпеки та повідомити про це органи влади. Компанія, більшу частину акцій якої володіє приватна інвестиційна фірма BGH Capital і яка переробляє близько 900 000 птахів на тиждень, розпочала «поетапне відновлення виробництва» для безпечного повернення до роботи. Хоча Hazeldenes не надала детальної інформації про вплив на клієнтів, ABC повідомила, що паби та м'ясні магазини у Вікторії зазнали дефіциту курятини, пов'язаного з інцидентом… Компанія принесла вибачення за перебої в роботі та заявила, що повідомить усіх осіб, чиї дані могли бути порушені. Ця атака є останньою в серії кіберінцидентів,

спрямованих проти глобальних харчових підприємств, включаючи японського гіганта з виробництва напоїв Asahi, американського оптового продавця United Natural Foods, багатонаціональну молочну компанію Arla Foods та південноафриканську компанію з виробництва птиці Astral Foods, яка минулої весни опублікувала попередження про зниження прибутку через подібне порушення». ***(Simon Harvey. Australia chicken processor Hazeldenes hit by cyberattack // yahoo finance (https://finance.yahoo.com/news/australia-chicken-processor-hazeldenes-hit-125215759.html). 25.02.2026).***

***

«Фінансовий сектор залишається галуззю, яка найбільше страждає від кібератак: у 2024 році 65% організацій постраждали від програм-вимагачів (це найвищий показник серед усіх галузей), а середні витрати на відновлення (без урахування викупу) досягли 2,73 млн доларів. Фішинг становить 90% початкових векторів атак, а третина атак обходить традиційні засоби захисту, незважаючи на збільшення бюджетів на безпеку. У 2024 році на чорному ринку було виставлено 14,5 мільйона викрадених кредитних карток, що на 20% більше, ніж у попередньому році, що збільшує ризики для цілісності транзакцій та довіри клієнтів…

Традиційні інструменти центрів безпеки (SOC), такі як SIEM, EDR та шлюзи електронної пошти, генерують величезний обсяг сповіщень і затримують видимість, змушуючи аналітиків боротися з ручною перевіркою IOC і подовжуючи середній час реагування (MTTR). Ці прогалини дозволяють швидкоплинним загрозам, таким як кампанії Lumma Stealer, спрямовані на європейські та американські банки, спричиняти операційні простої, штрафи за порушення нормативних вимог та шкоду репутації…

Щоб протидіяти цим викликам, рішення Threat Intelligence від ANY.RUN надають проактивні, засновані на пісочниці канали та пошукові системи, якими користуються понад 15 000 організацій по всьому світу. Канали Threat Intelligence, збагачені спільнотою з 600 000 аналітиків, надають контекстні IOC (IP-адреси, домени, URL-адреси) для безперебійної інтеграції SIEM/SOAR, підвищуючи рівень виявлення на 36% і зменшуючи кількість помилкових спрацьовувань. Пошук загроз Threat Intelligence Lookup пропонує миттєві висновки щодо понад 40 типів IOC, скорочуючи MTTR на 21 хвилину та забезпечуючи швидке виявлення загроз, адаптоване до фінансового сектору.

Переходячи від реактивного оповіщення до проактивного пошуку, фінансові установи досягають більш суворого дотримання вимог PCI DSS і DORA, знижують ймовірність порушень, зменшують витрати на криміналістичну експертизу та зберігають доходи, перетворюючи інформацію про загрози на очевидну перевагу в стійкості бізнесу в умовах безперервних кібернападів». ***(Balaji N. 65% of Financial Organizations Targeted by Ransomware as Cybercriminals Escalate Attacks // Cyber Security News (https://cybersecuritynews.com/financial-organizations-ransomware-attack-2024/). 24.02.2026).***

***

«Кіберзлочинці запустили нову пропозицію «зловмисне програмне забезпечення як послуга» (MaaS) під назвою TrustConnect — підроблений інструмент віддаленого моніторингу та управління (RMM) з професійним веб-сайтом, моделлю передплати (300 доларів на місяць у криптовалюті) та інфраструктурою підтримки клієнтів. Виявлений дослідниками Proofpoint, TrustConnect функціонує як повнофункціональний троян дистанційного доступу (RAT), що дозволяє зловмисникам виконувати команди, передавати файли та дистанційно керувати зараженими машинами з веб-панелі управління…

Шкідливе програмне забезпечення поширюється за допомогою соціальної інженерії: жертв обманом змушують завантажити підписані виконувані файли, замасковані під легальні інсталятори програм (Zoom, Microsoft Teams, Adobe Reader, Google Meet), через фішингові електронні листи на тему податків, обміну документами, запрошень на зустрічі або повідомлень від уряду. Після інсталяції система жертви автоматично реєструється на порталі TrustConnect зловмисника. Фальшивий веб-сайт має подвійне призначення: він переконує сертифікаційні органи та жертв у легітимності, одночасно виступаючи в ролі бекенду для платних передплатників…

Proofpoint порушив роботу частини інфраструктури, але оператори швидко перейшли на новий варіант — DocConnect. Дослідники підозрюють, що для створення довершеного маркетингового контенту та документації були використані великі мовні моделі (LLM). Поява TrustConnect підкреслює зростаючу тенденцію, коли кіберзлочинці створюють і просувають власні «легітимні на вигляд» інструменти, щоб уникнути виявлення та зберегти постійний доступ, ефективно використовуючи модель RMM проти захисників». ***(Shweta Sharma. Don't trust TrustConnect: This fake remote support tool only helps hackers // FoundryCo, Inc. (https://www.csoonline.com/article/4135307/dont-trust-trustconnect-this-fake-remote-support-tool-only-helps-hackers.html). 20.02.2026).***

***

«…Кіберзлочинці все частіше використовують підроблені CAPTCHA як зброю. Згідно з доповіддю CrowdStrike «Глобальні загрози 2026 року», за останні два роки їх використання зросло на 563%, витіснивши традиційні приманки для оновлення браузера. Ці шкідливі CAPTCHA використовують довіру користувачів і відсутність єдиного дизайну, щоб обдурити жертв і змусити їх скомпрометувати власні пристрої за допомогою соціальної інженерії. Замість простої головоломки, ці підроблені вікна перевірки часто пропонують користувачам скопіювати та вставити команду в діалогове вікно «Виконати» Windows або термінал, після чого виконується скрипт PowerShell для завантаження шкідливого програмного забезпечення, такого як трояни, шпигунські програми або програми для викрадення інформації. Оскільки користувач ініціює завантаження на системному рівні, стандартні засоби захисту від фішингу часто обходять…

Щоб убезпечити себе, користувачі повинні пам'ятати, що легітимні CAPTCHA ніколи не вимагають виконання команд на рівні системи. Якщо CAPTCHA просить вас скопіювати та вставити інструкції, це майже напевно шахрайство, і вам слід негайно закрити вкладку. Інші ознаки, що повинні

насторожити, включають термінові або тривожні формулювання, незвичайні URL-адреси, орфографічні помилки та прохання перейти на іншу веб-сторінку для доступу до вмісту. Залишаючись пильними, оновлюючи браузери та уникаючи панічних дій, користувачі можуть значно зменшити ризик стати жертвою цієї швидко зростаючої загрози». ***(Charlie Osborne. Fake CAPTCHA attacks exploded by 563% last year: How to spot them and stay safe online // ZDNET (https://www.zdnet.com/article/fake-captcha-how-detect-stay-safe-online/). 24.02.2026).***

***

«Дослідники з безпеки компанії Varonis виявили складну службу рекламного шахрайства під назвою 1Campaign, якою керує хакер, відомий як «DuppyMeister», і яка вже щонайменше три роки дозволяє кіберзлочинцям проводити зловмисні рекламні кампанії в Google Ads. Платформа функціонує як вдосконалений клоакер, показуючи законно виглядаючі порожні сторінки рецензентам Google, сканерам безпеки та дослідникам, одночасно надаючи фішинговий або шахрайський контент реальним жертвам, що дозволяє шахрайським оголошенням пройти початкові перевірки та залишатися активними довше…

Окрім базового маскування, 1Campaign надає аналітику в режимі реального часу, детальне профілювання відвідувачів та систему оцінки шахрайства (0–100), яка автоматично блокує трафік від відомих постачальників послуг безпеки, хмарних провайдерів (Microsoft, Google, Tencent, OVH), центрів обробки даних та VPN. Він також включає запускач Google Ads, який дозволяє зловмисникам видавати себе за будь-який бренд та обходити обмеження політики, змішуючи шкідливі та нешкідливі кампанії…

1Campaign, що діє в багатьох країнах, включаючи США, Канаду, Європу, Китай і Японію, дозволила здійснювати масштабне рекламне шахрайство, підробляючи довірені бренди та уникаючи виявлення. Varonis попереджає, що такі інструменти значно збільшують охоплення та тривалість фішингових і шахрайських кампаній, підкреслюючи зростаючу проблему для рекламних платформ у боротьбі з цілеспрямованою, що обходить політику, зловмисною рекламою». ***(Sead Fadilpašić. This new cybercrime platform lets hackers run malicious Google Ads and hide from Google's screening process // Future US, Inc. (https://www.techradar.com/pro/security/this-new-cybercrime-platform-lets-hackers-run-malicious-google-ads-and-hide-from-googles-screening-process). 25.02.2026).***

***

«Група Google з аналізу загроз (GTIG) та компанія Mandiant успішно припинили складну, тривалу шпигунську кампанію, яку, як підозрюють, фінансувала китайська держава і яка відстежувалася під кодом UNC2814. Кампанія, яка тривала щонайменше з 2023 року, зашкодила 53 організаціям у 42 країнах, а також, як підозрюють, заразила мережі щонайменше у 20 інших країнах, націлюючись переважно на телекомунікаційні та урядові мережі…

Зловмисники застосували новий бекдор на основі мови C під назвою GRIDTIDE, який зловживає API Google Sheets для прихованого управління та

контролю (C2). Використовуючи жорстко закодований приватний ключ, GRIDTIDE аутентифікується в обліковому записі Google Service Account, очищає електронну таблицю, збирає дані розвідки хоста і постійно опитує комірку A1 на наявність команд, одночасно виводячи вихідні дані або викрадені файли через комірки A2-An у фрагментах, закодованих у безпечному для URL форматі Base64. Ця техніка поєднує шкідливий трафік із законними викликами API Google, уникаючи виявлення…

Підтримувані команди включають виконання команд оболонки, завантаження файлів на комп'ютер жертви та завантаження файлів з комп'ютера жертви частинами розміром приблизно 45 КБ. Хоча прямого витоку даних не спостерігалося, принаймні одна зламана система містила конфіденційну інформацію, що дозволяє ідентифікувати особу (PII).

Google та його партнери перервали кампанію, припинивши всі пов'язані з нею проекти Google Cloud, скасувавши доступ до API, заблокувавши домени та повідомивши про це організації, які зазнали впливу. Незважаючи на комплексні заходи з ліквідації, дослідники попереджають, що UNC2814, ймовірно, незабаром відновить свою діяльність за допомогою нової інфраструктури. Для сприяння заходам захисту було опубліковано правила виявлення та індикатори компрометації. Цей інцидент підкреслює зростаючу витонченість дій державних суб'єктів, які використовують надійні хмарні сервіси для таємного шпигунства у великих масштабах…» ***(Bill Toulas. Chinese cyberspies breached dozens of telecom firms, govt agencies // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/chinese-cyberspies-breached-dozens-of-telecom-firms-govt-agencies/). 25.02.2026).***

***

«Нові загальнонаціональні опитування, проведені Комісаром з питань комунікацій та Органом з цифрової безпеки Кіпру, показують різке зростання кількості кібератак на острові. За останні 12 місяців 53% підприємств (у порівнянні з 47% у 2024 році) та 33% фізичних осіб повідомили, що стали жертвами атак, причому зараз компанії зазнають атак приблизно кожні вісім днів, що є збільшенням у порівнянні з кожними десятьма днями у попередньому році. Фішинг залишається домінуючою загрозою, на яку припадає 44% інцидентів у бізнесі та 22% інцидентів серед приватних осіб…

Фінансові наслідки є значними: 51% постраждалих підприємств зазнали середніх збитків у розмірі 12 000 євро, а фізичні особи понесли середні витрати у розмірі 141 євро. Тривожним є той факт, що майже кожна четверта компанія не оновлювала свою політику кібербезпеки протягом більше року, а 43% підприємств і 74% фізичних осіб досі не знають про наявність навчальних програм з кібербезпеки. Участь у таких програмах є низькою, але ефективною — ті, хто їх відвідував, посилили заходи безпеки, такі як використання надійних паролів та уникнення підозрілих веб-сайтів…

Незважаючи на деяке зниження рівня фішингу, опитування виявляють постійні прогалини в обізнаності та підготовленості. У відповідь на це Управління цифрової безпеки планує розширити освітні семінари та кампанії з підвищення

обізнаності громадськості, щоб посилити знання та стійкість у сфері кібербезпеки як серед підприємств, так і серед громадян». ***(Kyriacos Nicolaou. One in three Cyprus citizens, half of businesses hit by cyberattacks // Cyprus-mail.com (https://cyprus-mail.com/2026/02/25/one-in-three-cyprus-citizens-half-of-businesses-hit-by-cyberattacks). 25.02.2026).***

***

«Кібератаки виявляються швидше, ніж раніше — дані Mandiant показують, що середній «час перебування» зловмисника скоротився з 416 днів близько 15 років тому до всього 11 днів у 2024 році — завдяки кращому моніторингу та поширенню швидких, гучних злочинів, таких як викрадення даних з метою вимагання викупу, хоча перевантажені роботою команди, слабка реакція на інциденти та приховані тактики APT «життя за рахунок місцевих ресурсів» все ще дозволяють деяким зловмисникам залишатися непоміченими. Водночас супротивники прискорюються: ReliaQuest повідомляє, що штучний інтелект скорочує операційні терміни, причому в 2025 році поперечне переміщення в середньому займатиме 34 хвилини (на 29% менше), а витік даних — близько шести хвилин, чому сприяють інструменти на базі штучного інтелекту, що поєднують соціальну інженерію з традиційним шкідливим програмним забезпеченням; IBM і Resilience підтверджують, що штучний інтелект скорочує цикли прийняття рішень, тоді як Sophos зазначає, що повністю автономні атаки на базі штучного інтелекту все ще є більше майбутнім, ніж сьогоденням…

Широка екосистема реагує на це — у першому щорічному звіті PCI SSC з 2006 року наголошується на глобальній співпраці, навчанні та спрощенні дотримання вимог, щоб не відставати від дедалі більш витончених і швидкоплинних загроз у сфері платежів, навіть попри те, що фрагментація та зловживання штучним інтелектом залишаються актуальними. Захисники також борються з швидким перетворенням вразливостей на зброю: VulnCheck виявив, що хоча в 2025 році було використано менше 1% вразливостей, обсяг експлойтів різко зріс (понад 14 400 експлойтів, пов'язаних з 10 500 CVE, що на 16,5% більше), а концептуальні докази, створені штучним інтелектом, додають шуму і ускладнюють визначення пріоритетів; більше половини CVE, пов'язаних з програмним забезпеченням-вимагачем, стосувалися нульових днів, що підкреслює необхідність швидшого усунення загроз…

У звіті CrowdStrike «Глобальні загрози 2026 року» ще раз підкреслюється зміна швидкості, згадуючи середній час прориву близько 29 хвилин (а в деяких випадках і 27 секунд), значну залежність від викрадених законних облікових даних та переважно вільні від шкідливого програмного забезпечення вторгнення (82 %), які поєднуються з нормальною діяльністю — часто через некеровані кінцеві точки, такі як VPN та особисті пристрої, — тоді як штучний інтелект все частіше слугує як інструмент зловмисника, так і новою поверхнею для атак». ***(News brief: Attackers gain speed in cybersecurity race // Informa TechTarget (https://www.techtarget.com/searchsecurity/news/366639638/News-brief-Attackers-gain-speed-in-cybersecurity-race). 27.02.2026).***

***

«Нові дані від Immunefi свідчать, що справжня вартість великих хакерських атак полягає не стільки у викупі, скільки у паралічі та втраті довіри в перші години реагування — 80% організацій, що зазнали атак, ніколи повністю не відновлюються. Ця реальність простежується в інциденті з Conduent, який описують як найбільший на сьогоднішній день злом в США, в результаті якого були викрадені адреси, номери соціального страхування та медична інформація щонайменше 26 мільйонів американців (в тому числі до 15,4 мільйона в Техасі та 10,5 мільйона в Орегоні), що ілюструє, як злом одного постачальника може поширитися на державні програми та страхові компанії. Незважаючи на збільшення витрат на аудит, тестування, моніторинг та виявлення за допомогою штучного інтелекту, розрив у готовності зберігається, оскільки зміна конфігурації, поспішні оновлення та інтеграція сторонніх систем знову відкривають лазівки; типовими причинами невдач є повільне виправлення, повторне використання відомих слабких місць та каскадний ризик у гібридних хмарних/локальних/постачальницьких середовищах…

Найбільш надійним показником виживання є зрілість реагування на інциденти — чіткі повноваження щодо миттєвої зупинки систем, перевірені сценарії дій, швидке повідомлення зацікавлених сторін, прозора публічна комунікація та повноважні керівники кризових ситуацій — тоді як вагання збільшує шкоду та підриває довіру швидше, ніж сама порушення. Особам, які потенційно можуть бути постраждалими, настійно рекомендується перевірити реєстри порушень (наприклад, Have I Been Pwned), змінити паролі, увімкнути 2FA, контролювати фінансові та медичні виписки та розглянути можливість захисту особистих даних. Правління все ще недооцінюють асиметричний ризик постачальників, прискорену штучним інтелектом швидкість атак та той факт, що довіра тепер є операційним ризиком; у 2026 році стійкість визначається чіткістю керівництва в першу годину, а не аудиторськими чек-листами». ***(Ron Kness. America's Largest Breach May Be a Warning: Incident Response Is the New Survival Metric // ClearanceJobs (https://news.clearancejobs.com/2026/02/27/americas-largest-breach-may-be-a-warning-incident-response-is-the-new-survival-metric/). 27.02.2026).***

***

«…Ігри, які зараз перевершують за популярністю спорт, музику та кіно, мають майже 4 мільярди гравців (80% інтернет-користувачів, 2 мільярди на мобільних пристроях) і до 2028 року мають досягти обсягу 300 мільярдів доларів серед різноманітних демографічних груп, стикаються з ескалацією ризиків кібербезпеки через свій вибуховий ріст. Фішинг за допомогою підроблених логінів/безкоштовних подарунків/валютних шахрайств, захоплення облікових записів шляхом заповнення облікових даних зі старих зломів, програм-вимагачів, рекламного ПЗ, RAT, імітації ігор та атак на ланцюги постачання третіх сторін є головними загрозами, що змушує понад 200 студій Лос-Анджелеса — глобального центру — покладатися на керовані IT-послуги для цілодобової підтримки, масштабованості хмари, відповідності вимогам та аналітики…

Засоби захисту включають MFA для обмеження ATO, запобігання DDoS-атакам (очищення/CDN/обмеження швидкості), моніторинг аномалій/бот-трафіку та гібридних хмарних конфігурацій у режимі реального часу, а також навчання користувачів/персоналу щодо фішингу та ризикованих модифікацій, що приховують шкідливе програмне забезпечення. Внутрішні ризики також є значними: випадкові порушення через помилкові відправлення, втрачені пристрої або неправильні налаштування, а також навмисний саботаж з боку незадоволених співробітників/підрядників, які зловживають привілеями для крадіжки/витоку/знищення даних. Протидіяти цьому можна за допомогою доступу з мінімальними привілеями, миттєвого звільнення, моніторингу підозрілих дій та інструментів DLP. Індивідуальні стратегії, що поєднують проактивні технології, навчання та пильність, є життєво важливими для забезпечення довгострокової безпеки цієї швидкозростаючої екосистеми». ***(The Cybersecurity Threats Endangering The Gaming Industry // CGMagazine Publishing Inc. (https://www.cgmagonline.com/articles/the-cybersecurity-gaming-industry/). 27.02.2026).***

***

Діяльність хакерів та хакерські угруповування

«Північнокорейські хакери з групи APT37 (також відомі як ScarCruft), що підтримуються державою, використовують нещодавно виявлений набір інструментів у кампанії під назвою «Ruby Jumper» для подолання повітряного проміжку між підключеними до Інтернету та фізично ізольованими комп'ютерними системами. За даними дослідників Zscaler, атака починається, коли жертва відкриває шкідливий файл ярлика Windows (LNK), який запускає скрипт PowerShell і документ-приманку — в даному випадку арабський переклад північнокорейської статті про палестинсько-ізраїльський конфлікт. Потім скрипт ініціює багатоетапний процес зараження, в результаті якого встановлюється складний набір шкідливих програм, що включає п'ять основних інструментів: RESTLEAF, SNAKEDROPPER, THUMBSBD, VIRUSTASK і FOOTWINE…

Шкідливе програмне забезпечення встановлює зв'язок із сервером управління та контролю зловмисників і встановлює середовище виконання Ruby для виконання своїх корисних навантажень. Ключовий компонент, THUMBSBD, перетворює знімні USB-накопичувачі на «двосторонній прихований ретранслятор C2», що дозволяє йому викрадати дані з систем, відірваних від мережі, та передавати їм команди. Інший інструмент, VIRUSTASK, відповідає за поширення інфекції на нові ізольовані машини шляхом перетворення знімних дисків на зброю, приховування легальних файлів і заміни їх шкідливими ярликами. Останній корисний вантаж, FOOTWINE, є шпигунським бекдором для Windows, який дозволяє здійснювати кейлоггінг, захоплення знімків екрана, аудіо/відеозапис та віддалені команди оболонки. Zscaler з високою впевненістю приписує цю кампанію APT37 на основі перекриття шкідливого програмного забезпечення (включаючи раніше пов'язаний бекдор BLUELIGHT), технік та інфраструктури C2». ***(Bill***

Toulas. APT37 hackers use new malware to breach air-gapped networks // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/apt37-hackers-use-new-malware-to-breach-air-gapped-networks/). 27.02.2026).

***

Вірусне та інше шкідливе програмне забезпечення

«Загроза GlassWorm спричинила подальші порушення ланцюга поставок в екосистемі розробки програмного забезпечення, заразивши широко використовувані програмні компоненти, що вплинуло на тисячі кінцевих користувачів. Дослідники безпеки компанії Socket нещодавно виявили атаку на ланцюг поставок, в якій були задіяні троянські версії чотирьох легальних компонентів — FTP/SFTP/SSH Sync Tool, I18n Tools, vscode mindmap та scss to css — розповсюджені через реєстр Open VSX. Загалом ці компоненти були завантажені понад 22 000 разів, перш ніж шкідливі версії були видалені…

Атака, ймовірно, була здійснена за допомогою витоку токена або несанкціонованого доступу до облікового запису видавця, що дозволило зловмиснику завантажити скомпрометовані компоненти. Мета, як і в багатьох інших атаках на ланцюжок постачання додатків, полягала в зараженні користувачів шкідливим програмним забезпеченням, що викрадає інформацію. GlassWorm, вперше виявлений наприкінці 2025 року, є саморозповсюджувальним шкідливим програмним забезпеченням, яке поширюється шляхом викрадення облікових даних розробників і публікації подальших заражених компонентів. Він використовує приховані техніки, такі як зашифровані завантажувачі та невидимі символи Unicode, а також використовує блокчейн Solana і Google Calendar для управління та контролю…

Після встановлення GlassWorm збирає широкий спектр конфіденційних даних, включаючи облікові дані розробників, гаманці криптовалюти, дані браузера та ключі доступу до хмарних сервісів. Остання атака відрізнялася від попередніх хвиль тим, що вона компрометувала акаунти відомих видавців з історією надійних розширень, а не покладалася на типосквотинг або брендджекінг.

Організації, які постраждали від атаки, повинні розглядати її як випадок витоку облікових даних, змінити всі відповідні облікові дані, перевірити останні дії в GitHub і CI, а також видалити всі скомпрометовані розширення та їхні артефакти. Цей інцидент підкреслює зростаючий ризик атак на ланцюжок поставок у розробці програмного забезпечення та необхідність пильного моніторингу і швидкого реагування на загрози, спрямовані на компоненти з відкритим кодом…» ***(Alexander Culafi. GlassWorm Malware Returns to Shatter Developer Ecosystems // TechTarget, Inc. (https://www.darkreading.com/application-security/glassworm-malware-developer-ecosystems). 03.02.2026).***

***

«З'явилося нове шкідливе програмне забезпечення для знищення даних під назвою DynoWiper, яке націлене на енергетичні компанії в Польщі і

здійснює руйнівні атаки з метою остаточного знищення критично важливих даних. Вперше виявлене в грудні 2025 року, DynoWiper відрізняється від типового програмного забезпечення для вимагання викупу тим, що перезаписує і знищує файли в уражених мережах, роблячи системи непрацездатними і викликаючи серйозні перебої в роботі…

Шкідливе програмне забезпечення було розповсюджено через кілька варіантів, включаючи файли з іменами schtask.exe, schtask2.exe та виконуваний файл оновлення. Зловмисники зробили кілька спроб запустити шкідливе програмне забезпечення, модифікуючи код для обходу засобів захисту, але інструменти виявлення та реагування на кінцевих точках успішно заблокували виконання, обмеживши збитки.

Аналітики з питань безпеки виявили значну схожість між DynoWiper і ZOV wiper, який раніше використовувався проти українських цілей, і приписали цю атаку Sandworm, проросійській групі хакерів, відомій своїми атаками на критичну інфраструктуру Східної Європи. DynoWiper діє у три етапи: він рекурсивно шукає файли на всіх дисках, перезаписує вміст файлів випадковими даними та прискорює знищення, частково перезаписуючи більші файли…

Зловмисники використали групову політику Active Directory для розповсюдження шкідливого програмного забезпечення, що вимагало прав адміністратора домену та продемонструвало їхню здатність отримати доступ високого рівня. Шкідливе програмне забезпечення було розміщено у спільній мережевій директорії для одночасного виконання на декількох машинах. Перед розгортанням DynoWiper зловмисники використовували інструменти для викрадення облікових даних та встановили зворотні з'єднання із зовнішніми серверами, що свідчить про ретельне планування та розвідку.

Ця атака знаменує собою значне посилення кіберзагроз для критичної інфраструктури. Організаціям енергетичного сектору рекомендується впровадити суворий контроль доступу, сегментацію мережі та постійний моніторинг для виявлення та запобігання таким складним вторгненням до того, як будуть застосовані руйнівні програми-витирачі…» ***(Tushar Subhra Dutta. DynoWiper Data-Wiping Malware Attacking Energy Companies to Destroy Data // Cyber Security News (https://cybersecuritynews.com/dynowiper-data-wiping-malware/). 02.02.2026).***

***

«Ботнет Aisuru, також відомий як Kimwolf, встановив новий рекорд з розподілених атак типу «відмова в обслуговуванні» (DDoS), досягнувши пікової потужності 31,4 Тбіт/с і 200 мільйонів запитів на секунду. З приблизно одним-чотирма мільйонами заражених пристроїв по всьому світу, включаючи домашні маршрутизатори та онлайн-системи відеоспостереження, Aisuru є одним з найбільших ботнетів, що існують на сьогодні. Його оператори сканують Інтернет у пошуках вразливих пристроїв, заражають їх і додають до пулу, який можна орендувати для DDoS-атак або інших незаконних дій, таких як крадіжка облікових даних, веб-скрейпінг на основі штучного інтелекту, спам та фішинг…

Aisuru — це ботнет, який надає свої величезні можливості будь-кому, хто готовий за це заплатити. Він використовувався для атак на телекомунікаційні

компанії, ігрові компанії, інтернет-провайдерів, хостинг-провайдерів та фінансові служби. Ботнет також може здавати в оренду зламані пристрої провайдерам проксі-серверів для домашнього використання, які потім використовуються для збору даних і навіть навчання моделей штучного інтелекту.

Остання рекордна атака, яку Cloudflare відбила в грудні 2025 року, була описана як «безпрецедентна бомбардування» і найбільша атака, про яку коли-небудь повідомлялося публічно. Тільки в 2025 році було зафіксовано понад 47 мільйонів DDoS-атак, що на 121% більше, ніж у попередньому році, що підкреслює зростаючу загрозу, яку становлять такі ботнети. Більша частина потужності Aisuru походить від скомпрометованих споживчих пристроїв, включаючи недавню тенденцію до використання пристроїв Android TV як зброї, що підкреслює необхідність для користувачів постійно оновлювати прошивку та додатки, а для виробників — покращувати безпеку пристроїв…

Остання рекордна атака, яку Cloudflare відбила в грудні 2025 року, була описана як «безпрецедентна бомбардування» і найбільша атака, про яку коли-небудь повідомлялося публічно. Тільки в 2025 році було зафіксовано понад 47 мільйонів DDoS-атак, що на 121% більше, ніж у попередньому році, що підкреслює зростаючу загрозу, яку становлять такі ботнети. Більша частина потужності Aisuru походить від скомпрометованих споживчих пристроїв, включаючи недавню тенденцію до використання пристроїв Android TV як зброї, що підкреслює необхідність для користувачів постійно оновлювати прошивку та додатки, а для виробників — покращувати безпеку пристроїв». ***(Charlie Osborne. Massive 31.4 Tbps DDoS attack breaks records: How the 'apex' of botnets could be weaponizing your home devices // Ziff Davis company (https://www.zdnet.com/article/what-is-aisuru-botnet-ddos-assault/). 02.02.2026).***

***

«Новий штам шкідливого програмного забезпечення для Windows, названий «RenEngine loader», поширюється через піратські комп'ютерні ігри і, за даними дослідників з компанії Cyderes, що займається кібербезпекою, міг заразити понад 400 000 пристроїв по всьому світу. Шкідливе програмне забезпечення ховалося всередині зламаних ігор та модифікованих інсталяторів ігор для популярних франшиз, включаючи Far Cry, Need for Speed, FIFA та Assassin's Creed, а шкідливий код був вбудований у легальний запускач Ren'Py — движок, який зазвичай використовується для запуску візуальних романів. Хоча піратські ігри здаються функціональними, під час інсталяції вони непомітно доставляють вбудоване шкідливе програмне забезпечення разом із ігровим контентом, оскільки запускач Ren'Py розпаковує ігрові файли, таємно ініціюючи процес інсталяції шкідливого програмного забезпечення…

Ця шкідлива програма, яка діє щонайменше з квітня минулого року, була оновлена в жовтні з метою включення даних телеметричного відстеження, що дозволило виявити масштаби зараження. Вбудований URL-адресу телеметрії реєструє приблизно від 4000 до 10 000 відвідувачів на день, причому найбільша концентрація жертв спостерігається в Індії, США та Бразилії. Cyderes ідентифікувала один сайт, «dodi-repacks[.]site», як хост для завантажень ігор, що

містять шкідливе програмне забезпечення, домен, який раніше був позначений в інших кампаніях з поширення шкідливого програмного забезпечення.

Було виявлено, що завантажувач RenEngine доставляє шпигунську програму ARC для Windows, призначену для збору конфіденційних даних з комп'ютерів жертв, включаючи збережені паролі браузера, файли cookie, гаманці криптовалюти, інформацію для автозаповнення, деталі системи та вміст буфера обміну. В інших випадках завантажувач доставляв різні корисні навантаження, такі як шпигунська програма Rhadamanthys, Async RAT і XWorm, які також можуть викрадати паролі або дозволяти хакерам дистанційно захоплювати заражений комп'ютер. Загрозу посилює той факт, що більшість антивірусних движків наразі не розпізнають початковий етап роботи шкідливого програмного забезпечення, і лише Avast, AVG та Cynet виявляють його як загрозу, згідно з даними служби перевірки шкідливого програмного забезпечення VirusTotal від Google. Користувачам, які підозрюють, що їхній ПК може бути інфікований, рекомендується розглянути можливість використання функції відновлення системи Windows або, в крайньому випадку, повної переінсталяції операційної системи…» ***(Michael Kan. Malware Hidden in Pirated Games Infects 400,000 Devices // Ziff Davis, LLC. (https://uk.pcmag.com/security/163012/malware-hidden-in-pirated-games-infects-400000-devices). 06.02.2026).***

***

«Спляче шкідливе програмне забезпечення» — тип неактивного імплантату, вбудованого в системи організації, — становить все більшу загрозу кібербезпеці, оскільки залишається невиявленим протягом тривалого часу (іноді понад два роки), поки зовнішній тригер або дата активації не «пробудять» його, спричиняючи кіберінцидент. Це шкідливе програмне забезпечення, таке як Warp Panda та Brickstorm, часто впроваджується за допомогою тонких технік, таких як фішинг або компрометація ланцюга поставок, і може самостійно модифікуватися, щоб вижити після перезавантаження системи та планового технічного обслуговування. Хоча шкідливе програмне забезпечення перебуває в неактивному стані, воно не є неактивним; воно часто збирає особисті дані та конфіденційну ділову інформацію, скануючи вразливі місця, а потім запускає атаку в моменти пікового відволікання уваги, такі як державні свята або заплановане простоювання. Наслідки є серйозними — від перебоїв у наданні послуг і знищення даних до значної шкоди репутації…

Цей тривалий період бездіяльності створює складні юридичні проблеми, зокрема визначення моменту, коли виникає обов'язок повідомлення про порушення, чи будуть діяти поліси кіберстрахування з обмеженнями щодо дати зворотної дії, а також ступінь регуляторного ризику за період, протягом якого шкідливе програмне забезпечення було активним, але не виявленим. Хоча багато організацій використовують технічні засоби захисту, такі як брандмауери та багатофакторна автентифікація, складність «сплячого» шкідливого програмного забезпечення часто вимагає найсучасніших заходів для його виявлення… Щоб зменшити ці ризики, організаціям рекомендується регулярно переглядати та оновлювати свої протоколи безпеки, проводити ретельну перевірку сторонніх

постачальників послуг та розробляти надійний план реагування на кіберінциденти, що включає навчання персоналу та чіткі стратегії комунікації. Крім того, придбання кіберстрахування з особливою увагою до положень про ретроактивну дату та забезпечення дотримання законів про захист даних є важливими кроками в управлінні наслідками цих прихованих і все більш поширених атак». ***(Nicola McCrudden. 'Sleeping Malware'- Protecting Your Organisation From Cyber Threats // National Law Forum, LLC (https://natlawreview.com/article/sleeping-malware-protecting-your-organisation-cyber-threats). 25.02.2026).***

***

«Новий складний черв'як для ланцюгів постачання, названий SANDWORMMODE, активно атакує екосистему npm. Дослідники виявили щонайменше 19 шкідливих пакетів із помилками в назвах, призначених для викрадення секретів розробників та CI/CD. Кампанія імітує популярні утиліти Node.js та інструменти кодування ШІ, і після простої інсталяції через npm інсталятор виконує багатоетапний, сильно заплутаний пакет, який негайно збирає конфіденційні дані, включаючи токени npm і GitHub, змінні середовища, криптографічні ключі та секрети з менеджерів паролів. У середовищах CI черв'як обходить вбудовані затримки, що дозволяє миттєво викрадати та поширювати дані…

Черв'як поширюється, зловживаючи викраденими обліковими даними для повторної публікації заражених пакетів та введення шкідливих «носійних» залежностей у репозиторії та файли package.json. Він також використовує зброю GitHub Action для викрадення секретів CI та модифікує git hooks, щоб забезпечити стійкість у нових репозиторіях. Новою особливістю цієї кампанії є націленість на інструменти кодування ШІ, такі як Claude і Cursor; за допомогою прихованого введення команд, він змушує помічників ШІ читати і викрадати ключі SSH та облікові дані хмарних сервісів. Хоча руйнівна функція «dead switch», здатна стерти домашній каталог користувача, поки що залишається вимкненою, її наявність вказує на те, що шкідливе програмне забезпечення все ще розвивається, створюючи значну і постійну загрозу як для машин розробників, так і для CI/CD-пайплайнів». ***(Abinaya. New Shai-Hulud–like npm Worm Attack 19+ Packages to Steal dev/CI Secrets // Cyber Security News (https://cybersecuritynews.com/shai-hulud-like-npm-worm-attack/). 21.02.2026).***

***

«Агентство з кібербезпеки та безпеки інфраструктури (CISA) випустило попередження про те, що варіант шкідливого програмного забезпечення, відомий як «Resurge», який раніше використовувався в атаках на середовища Ivanti Connect Secure, може залишатися невиявленим в системах протягом тривалого часу після порушення. Попередження було випущено після аналізу CISA трьох зразків шкідливого програмного забезпечення з пристрою постачальника критичної інфраструктури, який був скомпрометований через використання CVE-2025-0282, уразливості переповнення буфера. Аналіз показав, що Resurge може залишатися в латентному стані на пристрої доти, доки віддалений

хакер не ініціює контакт, що спонукало CISA закликати команди безпеки перевірити наявність потенційного компрометації…

Атака, вперше виявлена дослідниками Mandiant у січні 2025 року і пов'язана з китайським хакером, відомим під псевдонімом UNC5337, передбачає використання набору шкідливих файлів. Основний файл, Resurge, працює аналогічно до шкідливого програмного забезпечення Spawnchimera, створюючи SSH-тунель для управління та контролю, а також дозволяючи змінювати файли, маніпулювати перевіркою цілісності та створювати веб-оболонки. Інший файл, варіант Spawnsloth, втручається в журнали пристроїв, а третій бінарний файл використовує інструмент з відкритим кодом під назвою BusyBox для завантаження та виконання корисних навантажень. Аналітик Forrester Джефф Поллард підкреслив, що поєднання стійкості та прихованості є особливо тривожним, оскільки може ввести захисників в оману, змусивши їх повірити, що вони усунули проблему, тоді як імплант залишається активним, а дані журналів є недостовірними». ***(David Jones. 'Resurge' malware can remain undetected on devices // TechTarget, Inc. (https://www.cybersecuritydive.com/news/cisa-resurge-malware-undetected-Ivanti/813373/). 27.02.2026).***

***

Програми-вимагачі

«Групи хакерів, що використовують програми-вимагачі, все частіше орендують дешеві віртуальні машини (ВМ) у провайдерів захищеного хостингу (BPH), таких як MasterRDP, замість того, щоб будувати власні сервери, що дозволяє тисячам кіберзлочинців спільно використовувати одну інфраструктуру. Дослідники Sophos виявили, що ці злочинці використовують легальну інфраструктуру ISPsystem, використовуючи автоматично згенеровані імена хостів Windows, які з'являються в різних інцидентах і країнах. Було виявлено понад 7000 серверів із спільними іменами хостів, що походять з таких регіонів, як Росія, Європа, США, Іран та Ізраїль…

Такий підхід дозволяє хакерам масштабувати операції, залишатися анонімними та зберігати стійкість — якщо один сервер виводиться з ладу, багато інших залишаються активними. Інфраструктура підтримує цілий ряд зловмисних дій, включаючи управління та контроль програм-вимагачів, розповсюдження шкідливого програмного забезпечення, фішинг, управління ботнетами та викрадення даних. Така практика існує вже принаймні п'ять років і використовується групами програм-вимагачів, такими як LockBit, Qilin, BlackCat (ALPHV) та іншими.

Хоча цей метод робить атаки дешевшими і простішими, він також дозволяє дослідникам у сфері безпеки ефективніше відстежувати діяльність кіберзлочинців, оскільки тисячі віртуальних машин використовують однакові статичні імена хостів. Більшість уражених віртуальних машин розміщені у невеликої кількості провайдерів, деякі з яких пов'язані з державними або злочинними операціями, такими як Stark Industries Solutions Ltd і First Server Limited, які були піддані

санкціям за сприяння державним операціям Росії та дезінформаційним кампаніям…

Хоча VMmanager від ISPsystem є легальною платформою, яка широко використовується в галузі хостингу, її низька вартість і простота розгортання роблять її привабливою для кіберзлочинців, які отримують вигоду від оперативного прикриття серед тисяч легальних користувачів. Ця тенденція підкреслює постійну проблему балансування переваг технології віртуалізації з ризиками, які створюють хостингові середовища, толерантні до зловживань». ***(Emma Woollacott. Ransomware gangs are sharing virtual machines to wage cyber attacks on the cheap – but it could be their undoing // Future US, Inc. (https://www.itpro.com/security/ransomware/ransomware-gangs-are-sharing-virtual-machines-to-wage-cyber-attacks-on-the-cheap-but-it-could-be-their-undoing). 06.02.2026).***

***

«Міжнародний аеропорт Талси нещодавно зазнав атаки програм-вимагачів, що підтвердила речниця аеропорту Кім Кюлер. Інцидент не спричинив перебоїв у роботі аеропорту та щоденних перевезень, а команда з кібербезпеки аеропорту швидко зв'язалася з правоохоронними органами та розпочала розслідування, вживши заходів для локалізації та зменшення ризику…

Про цю атаку, яку приписують пов'язаній з Росією групі Qilin, повідомило видання Cybernews.com, а також сайт Ransomware.live, який відстежує випадки використання програм-вимагачів. За повідомленнями, серед викрадених даних є особиста контактна інформація керівника аеропорту, таблиці з бюджетом і доходами, банківська кореспонденція та бази даних орендарів. Групи, що використовують програми-вимагачі, такі як Qilin, зазвичай публікують викрадені дані, щоб змусити жертв заплатити викуп.

Тайлер Мур, голова кафедри кібердосліджень Університету Талси, зазначив, що такі публічні розкриття інформації є стандартною практикою для груп, що займаються викраденням даних, щоб завоювати довіру і збільшити ймовірність отримання виплати. Qilin діє з 2022 року і вважається значним гравцем у кіберзлочинному середовищі.

Міжнародний аеропорт Талси працює незалежно від міста Талса, яке в 2019 році зазнало серйозної атаки програм-вимагачів, що пошкодило значну частину його IT-інфраструктури і коштувало понад 2 мільйони доларів для повного відновлення. Недавній інцидент підкреслює постійну загрозу, яку програми-вимагачі становлять для критичної інфраструктури, та важливість надійних заходів кібербезпеки…» ***(Kevin Canfield. Tulsa, Okla., Airport Tech Teams Contain Ransomware Attack // e.Republic LLC (https://www.govtech.com/security/tulsa-okla-airport-tech-teams-contain-ransomware-attack). 02.02.2026).***

***

«…Велика німецька страхова компанія HanseMerkur з річним доходом 3 мільярди євро, як стверджується, стала жертвою атаки програм-вимагачів з боку пов'язаної з Росією банди Dragonforce. Зловмисники стверджують, що

викрали майже 97 ГБ внутрішніх даних компанії, включаючи фінансові документи, ваучери, податкові накладні та рахунки-фактури, і опублікували ці заяви на своєму дарквеб-сайті — це звичайна тактика, щоб змусити жертв заплатити викуп, який зазвичай становить від 0,7% до 5% річного доходу.

Злом також міг торкнутися партнера HanseMerkur, компанії Emirates Insurance, яка підтримує портфелі в ОАЕ. HanseMerkur, штаб-квартира якої розташована в Гамбурзі, а офіси — у Швейцарії та Дубаї, ще не підтвердила факт атаки…

Dragonforce, відома своєю прихильністю до інтересів Кремля, раніше атакувала такі великі організації, як британська Co-op, Marks & Spencer, американський універмаг Belk та Mobilelink US. Ця банда, вперше помічена в 2023 році, дотримується правил, що забороняють атакувати лікарні та критичну інфраструктуру в Росії та союзних країнах, а нещодавно уклала альянс з Qilin та Lockbit щодо надання послуг з використанням програм-вимагачів.

За даними дослідників Cybernews і Halcyon, тільки в 2025 році Dragonforce атакувала 185 організацій, причому 130 атак відбулися за останні шість місяців, що підкреслює зростаючу активність групи та постійну загрозу програм-вимагачів для глобального бізнесу». ***(Paulina Okunytė. M&S attackers hit German insurance giant – HanseMerkur // Cybernews (https://cybernews.com/security/erman-insurer-hansemekur-ransomware-breach/). 03.02.2026).***

***

«Університет La Sapienza (Ла Сапієнца) в Римі, один з найбільших університетів Європи, в якому навчається близько 120 000 студентів, зазнав серйозних збоїв після того, як, ймовірно, атака програм-вимагачів вивела з ладу його комп'ютерні системи на три дні. Університет оголосив в Instagram, що в якості запобіжного заходу проактивно вимкнув свої системи, розслідує інцидент і працює над відновленням цифрових послуг за допомогою резервних копій, які не були пошкоджені. Електронна пошта та робочі станції залишаються частково обмеженими, а веб-сайт університету все ще не працює…

Італійське інформаційне агентство Il Corriere della Sera повідомило, що під час атаки було висунуто вимогу про викуп з 72-годинним відліком, нібито надіслану раніше невідомою хакерською групою під назвою «Femwar02», яка використовувала шкідливе програмне забезпечення BabLock (Rorschach). Однак ані університет, ані італійські власті офіційно не підтвердили деталі щодо викупу. Національне агентство Італії з кібербезпеки проводить розслідування, але поки що не надало коментарів.

Незважаючи на кібератаку, іспити в університеті La Sapienza проходять за розкладом, хоча студенти повинні реєструватися безпосередньо у викладачів. Університет створив інформаційні пункти на території кампусу, щоб допомогти студентам під час перебоїв у роботі…

Університети стали частими мішенями для кіберзлочинців. Минулого року Гарвардський університет і Пенсильванський університет також стали мішенями хакерів, які намагалися вимагати викуп від навчальних закладів, хоча ці атаки не були пов'язані з використанням програм-вимагачів. Інцидент у Ла Сапієнца

підкреслює постійну вразливість навчальних закладів до кіберзагроз та важливість надійних заходів кібербезпеки та систем резервного копіювання». ***(Lorenzo Franceschi-Bicchierai. One of Europe's largest universities knocked offline for days after cyberattack // TechCrunch Media LLC. (https://techcrunch.com/2026/02/05/one-of-europes-largest-universities-knocked-offline-for-days-after-cyberattack/). 05.02.2026).***

***

«Помилка в коді варіанту програми-вимагача, розробленої групою Nitrogen, створила незвичайну ситуацію, в якій зашифровані дані стають повністю невідновними — не тільки для жертви, але й для самих зловмисників. Ця програма-вимагач спеціально націлена на гіпервізори VMware ESXi, які слугують хост-серверами віртуальних машин, використовуючи той факт, що, хоча системні адміністратори зазвичай застосовують потужний захист кінцевих точок на хост-операційних системах, вони іноді нехтують безпекою самих гіпервізорів. Критична помилка виникає під час процесу шифрування, коли вісім байтів (64 біти) відкритого ключа шифрування випадково перезаписуються нулями через те, що, судячи з технічного аналізу Veeam, є типовою помилкою програмування «off-by-one». Оскільки відкриті та закриті ключі функціонують як пари, пошкодження відкритого ключа означає, що відповідного закритого ключа не існує — або його неможливо обчислити — для розшифрування даних, що робить вимоги зловмисників про викуп безглуздими, оскільки вони самі не можуть відновити зашифровані файли…

Тому жертви цього конкретного штаму не мають підстав платити викуп; їх єдиним виходом є відновлення даних з останніх резервних копій, а якщо резервних копій немає, дані втрачаються назавжди. Кампанія з використанням програм-вимагачів Nitrogen триває з 2023 року і спрямована проти північноамериканських фінансових установ, механічних і промислових компаній, а також навіть проти Red Barrels, розробника серії відеоігор Outlast, хоча у звіті Veeam не вказано, які саме жертви постраждали від цього конкретного варіанту ESXi. Цей інцидент є яскравим прикладом ненавмисного взаємного знищення, коли, ймовірно, проста помилка розробника фактично зірвала операцію зловмисників, у результаті чого жодна зі сторін не отримала доступу до зашифрованих даних». ***(Bruno Ferreira. Nitrogen ransomware programmers lock themselves out of a payment — key management bug encrypts victims' data forever // Future US, Inc. (https://www.tomshardware.com/tech-industry/cyber-security/nitrogen-ransomware-programmers-lock-themselves-out-of-a-payment-key-management-bug-encrypts-victims-data-forever). 07.02.2026).***

***

«…Атаки програм-вимагачів становлять серйозну загрозу для швейцарських компаній, змушуючи їх балансувати між юридичними ризиками та нагальною потребою відновити зашифровані дані. Хоча такі органи, як Федеральне управління з кібербезпеки, не рекомендують платити викуп, сам факт виплати за швейцарським законодавством не є кримінальним злочином, за

умови, що це не порушує санкцій, не підтримує злочинні організації та не пов'язано з відмиванням грошей. В екстремальних випадках виплата може бути виправдана відповідно до положень про надзвичайні ситуації (ст. 17 або 18 StGB), якщо це дозволяє уникнути безпосередньої небезпеки для більш цінних інтересів, таких як життя або критична інфраструктура, хоча економічних збитків само по собі недостатньо…

Однак компанії також повинні дотримуватися суворих вимог щодо захисту даних. Швейцарський закон про захист даних (DSG) зобов'язує «якнайшвидше» повідомляти Федеральному комісару з питань захисту даних та інформації (FDPIC) про порушення, які становлять високий ризик для фізичних осіб. Невиконання цієї вимоги або невжиття відповідних технічних заходів, таких як резервне копіювання та багатофакторна автентифікація (MFA), може призвести до регуляторних наслідків та цивільної відповідальності. Крім того, виплата викупу не гарантує відновлення даних і може спричинити подальше вимагання. Щоб зменшити ці ризики, компанії повинні надавати пріоритет резервному копіюванню, консультуватися з юридичними експертами, подавати кримінальні скарги та ретельно документувати всі рішення, щоб продемонструвати належну обачність і мінімізувати відповідальність…» ***(Nicole Beranek Zanon, Corinna Stubenvoll and Anastasia Käslin. Between ransom and legality: The legal handling of ransomware attacks // HÄRTING Rechtsanwälte AG (https://haerting.ch/en/insights/between-ransom-and-legality-the-legal-handling-of-ransomware-attacks/). 12.02.2026).***

***

«Advantest, відомий японський виробник обладнання для тестування напівпровідників, підтвердив, що реагує на інцидент з кібербезпекою, пов'язаний з програмним забезпеченням-вимагачем, після виявлення незвичайної активності в своїй IT-середовищі 15 лютого. Компанія негайно активувала протоколи реагування на інциденти, ізолювала уражені системи та залучила сторонніх експертів з кібербезпеки для управління ситуацією. Хоча попередні висновки вказують на те, що зловмисник міг отримати доступ до мережі та розгорнути програмне забезпечення для вимагання викупу, Advantest ще не підтвердила жодного випадку крадіжки даних і не отримала конкретних вимог про викуп, хоча планує безпосередньо повідомити постраждалих осіб, якщо в ході розслідування буде виявлено компрометацію даних клієнтів або співробітників… Цей інцидент підкреслює ескалацію кіберзагроз, з якими стикаються японські галузі промисловості. Ця тенденція спонукала Японію прийняти більш агресивну оборонну позицію в рамках закону «Активна кіберзахист» 2025 року, який спрямований на руйнування ворожої інфраструктури та посилення координації між урядовими установами з метою захисту критично важливих активів». ***(Anna Zhadan. Japanese chip testing firm Advantest investigates ransomware incident // Cybernews (https://cybernews.com/cybercrime/japanese-chip-testing-firm-advantest-investigates-ransomware-incident/). 22.02.2026).***

***

«…В Австралії кіберінциденти відбуваються кожні шість хвилин, і, за словами Компанії «Arthur J. Gallagher & Co.», перші 48 годин після порушення є вирішальними для обмеження або посилення збитків. Сучасні атаки з використанням програм-вимагачів часто супроводжуються витоком даних, причому злочинці погрожують оприлюднити конфіденційну інформацію навіть після відновлення систем, що збільшує юридичні ризики та ризики для репутації. Відразу після інциденту організації повинні стабілізувати свою діяльність, ізолювавши системи, забезпечивши резервне копіювання, зберігши докази для судового розслідування та залучивши спеціалістів з реагування, одночасно координуючи технічні, регуляторні та комунікаційні рішення, щоб уникнути суперечливих дій…

У разі вимагання викупу переговорники можуть оцінити вимоги щодо дешифрування та крадіжки даних перед будь-якою виплатою, зважаючи на австралійське законодавство, включаючи санкції та обов'язкові вимоги щодо повідомлення про виплати на суму понад 3 мільйони доларів протягом 72 годин. Відповідно до Закону про конфіденційність, компанії повинні швидко визначити, чи загрожує порушення серйозною шкодою, та повідомити про це органи влади та постраждалих осіб, оскільки затримки можуть збільшити ризик. Gallagher наголошує, що заздалегідь розроблені плани реагування, консультації фахівців та кіберстрахування мають вирішальне значення, оскільки швидкість, координація та внесок експертів є тим, що в кінцевому підсумку визначає результат дедалі складніших кіберкриз». ***(Mav Rodriguez. The first 48 hours that define a cyber crisis // KM Business Information Australia Pty Ltd (https://www.insurancebusinessmag.com/au/news/cyber/the-first-48-hours-that-define-a-cyber-crisis-566105.aspx). 21.02.2026).***

***

«Атака програм-вимагачів на урядового підрядника в галузі технологій Conduent, яка спочатку була оцінена як незначна, переросла в одну з найбільших витоків даних в новітній історії США, що потенційно може торкнутися десятків мільйонів людей у багатьох штатах. Інцидент, що стався в січні 2025 року, відповідальність за який взяла на себе група хакерів Safeway, супроводжувався викраденням понад 8 терабайтів даних, включаючи номери соціального страхування, медичні записи та дані про медичне страхування…

Тільки в Техасі, як вважається, постраждали 15,4 мільйона жителів — майже половина населення штату, що є різким збільшенням порівняно з початковою оцінкою в 4 мільйони. Орегон повідомив про 10,5 мільйона постраждалих осіб, а додаткові повідомлення були надіслані сотням тисяч людей у таких штатах, як Делавер, Массачусетс і Нью-Гемпшир. Компанія Conduent, яка обробляє дані для державних програм охорони здоров'я та державних служб по всій країні, ще не підтвердила загальну кількість жертв, але визнає, що порушення стосується «значної кількості» персональних даних осіб…

Компанія повідомила про інцидент у квітні 2025 року, через кілька місяців після того, як атака порушила роботу сервісів, і досі повідомляє про це постраждалих осіб. Очікується, що процес повідомлення буде завершено на

початку 2026 року. Оскільки Conduent працює за лаштунками для державних органів, багато жертв можуть не знати, що їхні дані зберігалися в цій компанії. Витік номерів соціального страхування та медичної інформації створює серйозні довгострокові ризики, зокрема крадіжку особистих даних, медичне шахрайство та цілеспрямовані афери…

Компанія Conduent заявила, що на даний момент немає доказів зловживання даними в даркнеті, і створила спеціальний call-центр для відповідей на запитання. Цей випадок підкреслює вразливість важливих урядових підрядників і ланцюговий ефект, який виникає, коли конфіденційні дані державного сектора потрапляють у руки зловмисників. Особам, які користуються державними медичними або урядовими послугами, рекомендується стежити за своїм кредитом, розглянути можливість його заморожування та слідкувати за ознаками шахрайства». ***(Kurt Knutsson. Conduent data breach hits millions across multiple states // FOX News Network, LLC. (https://www.foxnews.com/tech/conduent-data-breach-hits-millions-across-multiple-states). 22.02.2026).***

***

«Відома північнокорейська хакерська група Lazarus, що фінансується державою, почала використовувати готове програмне забезпечення для вимагання викупу Medusa в атаках на організації охорони здоров'я та некомерційні організації, переважно в США та на Близькому Сході. Згідно зі спільним дослідженням Symantec і Carbon Black, з листопада 2025 року було атаковано щонайменше чотири організації, розташовані в США, включаючи некомерційну організацію з охорони психічного здоров'я та навчальний заклад для дітей з аутизмом, із середньою сумою викупу близько 260 000 доларів…

У цих атаках використовуються ексклюзивні інструменти Lazarus, такі як бекдор/завантажувач Comebacker і RAT Blindingcan, а також широко доступний дампер облікових даних Mimikatz, що підкреслює, що навіть просунуті державні актори все частіше покладаються на стандартні програми-вимагачі як послугу, а не на спеціальне шкідливе програмне забезпечення. Хоча приналежність кожного інциденту Medusa залишається невизначеною, використання інструментів, характерних для Lazarus, міцно пов'язує ці атаки на медичні установи з північнокорейськими агентами…

Експерти відзначають, що перехід Lazarus до готових програм-вимагачів відображає індустріалізацію кіберзлочинності, що підтримується державою, що дозволяє швидше масштабувати та фінансувати більш широкі шпигунські операції. Націленість на недофінансованих, емоційно вразливих постачальників медичних послуг — у поєднанні з постійною ефективністю таких десятирічних інструментів, як Mimikatz — підкреслює постійні слабкі місця в гігієні ідентифікації та нагальну потребу в посиленні захисту облікових даних, зменшенні площі атаки та швидкому виправленні в усьому секторі». ***(Steve Zurier. North Korea's Lazarus Group targets US, Middle East healthcare sectors // CyberRisk Alliance (https://www.scworld.com/news/north-koreas-lazarus-group-targets-us-middle-east-healthcare-sectors). 24.02.2026).***

***

«Незважаючи на 50% зростання кількості випадків використання програм-вимагачів у 2025 році, що принесло кіберзлочинцям 820 мільйонів доларів, новий звіт аналітиків ринку Chainalysis показує, що все менше жертв платять викуп. Кількість підприємств, які вирішили заплатити, впала до рекордно низького рівня 28% у 2025 році, продовжуючи чотирирічну тенденцію до зниження з максимуму 78,9% у 2022 році. Це зниження пояснюється кількома факторами, серед яких покращення реагування на інциденти, посилення регуляторного контролю та ефективні міжнародні правоохоронні заходи проти операторів програм-вимагачів та їх інфраструктури…

Однак, хоча все менше компаній платять викуп, ті, що платять, стикаються з набагато вищими вимогами. Середній розмір викупу зріс на 368% у порівнянні з попереднім роком, з 12 738 доларів у 2024 році до 59 556 доларів у 2025 році. Це свідчить про зміну тактики, коли зловмисники вимагають більше від жертв, які все-таки капітулюють. Вимагання викупу залишається популярним і активним кримінальним бізнесом, в якому зараз діє 85 активних груп з вимагання, що націлені переважно на підприємства в США, Канаді, Німеччині та Великій Британії». ***(Sead Fadilpašić. Ransomware payments drop to record low, even as attacks surge // Future US, Inc. (https://www.techradar.com/pro/security/ransomware-payments-drop-to-record-low-even-as-attacks-surge). 27.02.2026).***

***

Фішингові атаки

«Фішинг залишається одним із найпоширеніших і найефективніших методів кібератак не тому, що захист є недостатнім, а тому, що зловмисники постійно адаптують свої тактики, щоб атакувати критично важливі підрозділи, такі як відділи кадрів, фінансів та IT-підтримки. Команди центру безпеки (SOC) працюють над виявленням і розслідуванням цих високоспеціалізованих фішингових листів, а команди з підвищення обізнаності в питаннях безпеки навчають співробітників розпізнавати такі загрози та реагувати на них. Однак відсутність інтегрованого робочого процесу між цими командами часто призводить до неефективних ручних процесів і затримок у проведенні відповідних тренінгів, що робить організації вразливими…

AI ThreatFlip Workflow від Proofpoint вирішує цю проблему, автоматизуючи перетворення реальних фішингових електронних листів у безпечні, відповідні ролі навчальні симуляції. Вбудований у платформу Proofpoint Collaboration Security Prime, ThreatFlip дозволяє аналітикам SOC вибрати виявлений фішинговий електронний лист і одним клацанням миші перетворити його на очищену, настроювану симуляцію для негайного використання командою з підвищення обізнаності про безпеку. Це усуває необхідність ручного передання, скорочує затримки та гарантує, що навчальний контент відображає найновіші тактики атак, з якими можуть зіткнутися співробітники…

ThreatFlip працює шляхом клонування реальних фішингових електронних листів, видалення шкідливих елементів та інформації, що дозволяє ідентифікувати особу, а також виділення ключових ознак фішингу (фішингових гачків) для створення навчальних моментів. Результатом є своєчасне, реалістичне навчання, яке допомагає співробітникам ефективніше розпізнавати загрози та реагувати на них. Платформа також надає інформаційні панелі для миттєвого перегляду ефективності фішингових кампаній.

Система розроблена з урахуванням безпеки та конфіденційності, що гарантує безризиковість та відповідність симуляцій. Людський контроль та інформація про загрози від Proofpoint підтверджують результати, забезпечуючи баланс між автоматизацією та управлінням.

Завдяки автоматизації процесу від виявлення до навчання ThreatFlip дозволяє організаціям перейти від ручної праці до операційної ефективності, скорочуючи розрив між виявленням загроз і готовністю співробітників. Такий підхід не тільки підвищує обізнаність і стійкість, але й сприяє вимірюваним змінам у поведінці, роблячи обізнаність у питаннях безпеки динамічною дисципліною, що базується на аналітичних даних. Для організацій, що використовують платформу Proofpoint, ThreatFlip пропонує потужний інструмент для зміцнення захисту та формування культури проактивної кібербезпеки…» ***(Paul Wiederkehr. Turn real phishing attacks into real behavior change with Proofpoint's AI ThreatFlip Workflow // Proofpoint (https://www.proofpoint.com/us/blog/security-awareness-training/threatflip-turning-phishing-attacks-into-behavior-change). 02.02.2026).***

***

«Федеральне відомство Німеччини з охорони конституції (BfV) та Федеральне відомство з інформаційної безпеки (BSI) опублікували спільне попередження про триваючу, спонсоровану державою фішингову кампанію, яка зловживає законними функціями Signal, а не шкідливим програмним забезпеченням або вразливостями. Видаючи себе за «Signal Support» або «Signal Security ChatBot», зловмисники, які зосереджуються на високопоставлених політичних, військових і дипломатичних діячах, а також журналістах-розслідувачах у Німеччині та Європі, переконують жертв передати SMS-код підтвердження або PIN-код, або просканувати шкідливий QR-код. За допомогою цієї інформації вони або перереєструють обліковий запис жертви на пристрої, який вони контролюють, або непомітно підключають новий пристрій, що дозволяє їм читати вхідні повідомлення, видавати себе за користувача та збирати списки контактів, тим самим ставлячи під загрозу цілі мережі групових чатів. Хоча минулі розмови не розкриваються, за допомогою QR-коду можна синхронізувати до 45 днів останніх чатів, і подібні тактики можуть бути перенесені на WhatsApp, який використовує аналогічні механізми PIN-коду та підключення пристроїв. BfV та BSI закликають користувачів не взаємодіяти з передбачуваними чатами підтримки, ніколи не вводити свій PIN-код Signal у текстовому чаті, увімкнути «Блокування реєстрації» та регулярно перевіряти підключені пристрої…

Ця рекомендація з'явилася на тлі широкого розголосу про агресивну кіберактивність, що підтримується державою, в Європі: Норвегія звинуватила

китайські угруповання, такі як Salt Typhoon, у використанні мережевих пристроїв з метою вербування норвежців для шпигунства, звинуватила Росію у стеженні за військовими об'єктами та попередила, що іранські суб'єкти компрометують акаунти дисидентів. Окремо CERT Polska приписала скоординовані вторгнення в понад 30 польських об'єктів відновлюваної енергетики та велику теплоелектростанцію російській групі «Static Tundra», яка використовувала незахищені інтерфейси FortiGate VPN, що не мали багатофакторної автентифікації…» ***(Ravie Lakshmanan. German Agencies Warn of Signal Phishing Targeting Politicians, Military, Journalists // The Hacker News (https://thehackernews.com/2026/02/german-agencies-warn-of-signal-phishing.html). 07.02.2026).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Офіс шерифа округу Явапай повідомляє, що слідчі допомогли повернути 850 000 доларів США після запобігання кібератаці, яка намагалася перенаправити кошти округу.

Атака сталася після того, як, як повідомляється, злочинці отримали доступ через стороннього постачальника та перенаправили запланований прямий депозит на щойно створений шахрайський банківський рахунок.

Після виявлення цього факту офіс шерифа округу Явапай співпрацював з банками, щоб відстежити гроші.

Слідчі виявили, що кошти були надіслані до банку, який позначив транзакцію як підозрілу та заморозив її до перевірки джерела, яке злочинці не змогли надати, повідомляє офіс шерифа.

Правоохоронці вилучили рахунок і повернули майже всі гроші. Слідчі працюють над тим, щоб переконатися, що повна сума врахована, поки вони шукають підозрюваних…» ***(Brian Petersheim Jr. Yavapai County recovers $850K after hackers used cyberattack to divert funds // A Gray Local Media Station (https://www.azfamily.com/2026/02/03/yavapai-county-recovers-850k-after-hackers-used-cyberattack-divert-funds/). 03.02.2026).***

***

«Складна платформа фішингу як послуги (PhaaS), націлена на сектор вантажних перевезень та логістики, була ліквідована після того, як дослідники з Have I Been Squatted та Ctrl-Alt-Int3l виявили її діяльність через відкритий каталог .git. Російськомовна платформа, яка отримала від дослідників кодову назву Diesel Vortex, внутрішньо називалася GlobalProfit і продавалася під назвою MC Profit Always. Вона продавалася на підпільних форумах за криптовалюту і давала можливість передплатникам запускати цілеспрямовані фішингові кампанії проти великих логістичних платформ, включаючи DAT Truckstop, Penske Logistics, EFS і Timocom…

Протягом п'яти місяців в рамках операції було задіяно 52 фішингові домени, викрадено облікові дані понад 1600 користувачів та здійснено 35 спроб шахрайства з чеками EFS. Зловмисники використовували скомпрометовані спільноти Telegram, підроблені телефонні номери та схеми подвійного посередництва, щоб видавати себе за перевізників і перенаправляти вантажі або платежі. Оператори платформи, які, ймовірно, пов'язані з російськими оптовими та транспортними компаніями і включають членів, що розмовляють вірменською мовою, створили галузеві фішингові набори, які знизили бар'єр кваліфікації для шахраїв…

Це відкриття підкреслює зростаючу тенденцію до створення спеціалізованих платформ PhaaS, призначених для високодохідних, менш захищених галузей з віддаленими працівниками та великими обсягами транзакцій. Дослідники підкреслюють, що стійкі до фішингу засоби багатофакторної автентифікації (MFA), такі як ключі безпеки FIDO2 або паролі-ключі, могли б повністю заблокувати ці атаки, оскільки традиційні методи на основі TOTP та SMS залишаються вразливими до перехоплення в режимі реального часу. Цей випадок також демонструє, що навіть просунуті злочинні операції можуть бути зірвані, коли порушується оперативна безпека, що підкреслює цінність спільної розвідки загроз у боротьбі з новими екосистемами кіберзлочинності як послуги». ***(Mathew J. Schwartz. Phishing Platform Targeting Trucking and Logistics Disrupted // Information Security Media Group, Corp. (https://www.govinfosecurity.com/phishing-platform-targeting-trucking-logistics-disrupted-a-30846). 25.02.2026).***

***

«В результаті річної операції під назвою «Проект Компас», координованої Європолом, було заарештовано 30 осіб та ідентифіковано 179 підозрюваних, пов'язаних з «The Com» – децентралізованим та нігілістичним угрупованням кіберзлочинців, яке відоме тим, що націлює свою діяльність на дітей та підлітків. Спільна операція, розпочата в січні 2025 року під керівництвом Європейського центру боротьби з тероризмом Європолу, залучила правоохоронні органи з 28 країн і призвела до виявлення 62 жертв, чотирьох з яких було безпосередньо захищено. The Com, неформальна мережа англомовних кіберзлочинців, діє на різних онлайн-платформах, включаючи соціальні мережі, ігрові середовища та месенджери, з метою вербування та експлуатації молодих людей для вимагання, насильства та виробництва матеріалів із сексуальною експлуатацією дітей (CSAM)…

Колектив організований у кілька підгруп, таких як «Offline Com», яка пропагує пошкодження майна та тероризм; «Cyber Com», яка організовує вторгнення в мережі та атаки з використанням програм-вимагачів; та «(S)extortion Com», яка примушує неповнолітніх до сексуальних злочинів та заохочує до самоушкодження. Особливо відома підгрупа під назвою «764» вербує молодих людей для створення відвертого контенту з метою шантажу. Двоє її ймовірних лідерів були заарештовані у квітні 2025 року і зараз їм загрожує довічне ув'язнення. Com також пов'язують із гучними атаками програм-вимагачів на такі великі компанії, як Marks & Spencer і казино Лас-Вегаса. Європол наголосив, що ця міжнародна співпраця має вирішальне значення для вчасного втручання, захисту

жертв і боротьби зі злочинцями, які експлуатують вразливість молодих людей у цифровому просторі». ***(Sergiu Gatlan. Europol-led crackdown on The Com hackers leads to 30 arrests // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/police-crackdown-on-the-com-cybercrime-gang-leads-to-30-arrests/). 27.02.2026).***

***

Технічні аспекти кібербезпеки

Виявлені вразливості технічних засобів та програмного забезпечення

«Управління вразливістю є важливою дисципліною кібербезпеки, яка виходить за межі традиційного управління вразливістю, зосереджуючись не тільки на пошуку слабких місць, але й на виявленні та зменшенні вразливостей, які насправді доступні та можуть бути використані зловмисником. Вразливість можна уявити як двері зі слабким замком, тоді як вразливість — це ті самі двері, залишені широко відкритими на жвавій вулиці… Це розрізнення є надзвичайно важливим, оскільки, хоча організації можуть мати тисячі вразливостей, лише частина з них представляє реальну, безпосередню загрозу. Управління вразливостями визначає пріоритетність усунення на основі можливості експлуатації та контексту виконання, такого як доступ до Інтернету, надмірні дозволи та доступ до конфіденційних даних, а не покладається виключно на необроблені оцінки CVSS…

Застосування стратегії управління вразливістю дає значні переваги, включаючи проактивне зниження ризиків шляхом обмеження площі атаки, полегшення дотримання нормативних вимог (GDPR, HIPAA тощо), підвищення безперебійності роботи шляхом запобігання простою та значну економію коштів завдяки уникненню значних витрат, пов'язаних з інцидентами безпеки. Процес включає п'ять ключових етапів: ідентифікація всіх активів у всьому середовищі (включаючи хмарні, локальні та тіньові IT-ресурси); оцінка для визначення пріоритетності ризиків на основі ймовірності їх використання та впливу на бізнес; пом'якшення ризиків шляхом встановлення виправлень, переконфігурації засобів контролю безпеки та сегментації мережі; постійний моніторинг для виявлення нових ризиків у режимі реального часу в міру зміни середовища; використання інформації про загрози для передбачення та захисту від нових загроз…

Ефективне управління вразливістю здійснюється за допомогою таких передових практик, як постійний внутрішній моніторинг, впровадження принципу мінімальних привілеїв (PoLP) та рольового контролю доступу (RBAC), автоматизація сповіщень для оперативного реагування, проведення регулярних аудитів безпеки, розробка надійного плану реагування на інциденти, використання передових інструментів на основі штучного інтелекту та регулярне навчання

співробітників передовим практикам у сфері кібербезпеки. Такі платформи, як Wiz for Exposure Management, централізують результати різних інструментів сканування в єдиній платформі, використовуючи графік безпеки для виявлення «токсичних комбінацій» ризиків, які представляють реальну загрозу для бізнесу, та забезпечуючи автоматизоване комплексне усунення недоліків». ***(Nicolas Ehrman. Exposure management in cybersecurity explained // Wiz, Inc. (https://www.wiz.io/academy/cloud-security/exposure-management-in-cybersecurity). 23.02.2026).***

***

«У NGINX, широко використовуваному зворотньому проксі-сервері та балансувальнику навантаження, який обслуговує близько 33,8% усіх веб-сайтів, виявлено вразливість високого рівня небезпеки. Ця вразливість, оцінена в 8,2 бала з 10 за рівнем серйозності, дозволяє зловмисникам, які знаходяться в позиції «людина посередині» (MITM) між проксі-сервером NGINX і серверами бекенду, вводити шкідливі дані у відповіді сервера. Це може призвести до зміни вмісту, перенаправлення або навіть повного захоплення сайту, що дозволить зловмисникам викрасти облікові дані, розповсюджувати шкідливе програмне забезпечення або здійснювати подальші атаки…

Вразливість впливає як на відкриті, так і на платні версії NGINX, особливо коли сервери налаштовані на пересилання трафіку, зашифрованого за допомогою TLS, на сервери бекенду. Зловмисники можуть скористатися коротким проміжком часу до завершення TLS-рукостискання, щоб ввести дані у вигляді звичайного тексту, які NGINX потім пересилає користувачам. Компанія F5, яка виявила цю проблему внутрішньо, випустила виправлені версії (nginx-1.28.2 stable та nginx-1.29.5 mainline) і закликає користувачів негайно оновити програмне забезпечення…

Тим часом дослідники в галузі безпеки виявили активну кампанію з експлуатації вразливостей, спрямовану на установки NGINX, особливо ті, що використовують панелі управління, такі як Baota. Зловмисники використовують автоматизовані скрипти для введення шкідливих правил проксі, перехоплення веб-трафіку та перенаправлення користувачів — часто з урядових та освітніх сайтів — на сайти азартних ігор та шахрайські сайти. Це підкреслює нагальну необхідність для організацій оновлювати свої установки NGINX та переглядати їх конфігурації, щоб запобігти експлуатації вразливостей». ***(Ernestas Naprys. Severe vulnerability affects NGINX: websites visitors in danger // Cybernews (https://cybernews.com/security/high-severity-vulnerability-affects-nginx/). 05.02.2026).***

***

«CISA випустила термінове попередження для користувачів SolarWinds Web Help Desk про критичну вразливість віддаленого виконання коду (RCE), CVE-2025-40551, яка активно експлуатується. Ця вразливість, з оцінкою CVSS 9,8, дозволяє неавторизованим зловмисникам отримати доступ на рівні адміністратора та виконувати команди на хост-машині через вразливість, пов'язану

з десеріалізацією ненадійних даних. Це може бути використано в атаках низької складності без аутентифікації…

Федеральним цивільним агентствам було надано лише три дні для усунення вразливості, що свідчить про високий операційний ризик, коли такі недоліки переходять від теоретичного до активного використання. SolarWinds Web Help Desk широко використовується у федеральному уряді США, а також у приватних секторах освіти та охорони здоров'я.

Експерти підкреслюють, що зловмисники часто використовують недооцінені вразливості в надійних платформах, а справжня небезпека полягає в можливості побічного переміщення та повного компрометації системи після отримання адміністративного доступу. Швидкий перехід від перевірки концепції до активного використання означає, що організації повинні діяти швидко, використовуючи постійний контроль та проактивну перевірку для збереження стійкості…

CVE-2025-40551 — одна з чотирьох критичних вразливостей, виявлених Horizon3.ai та виправлених SolarWinds 28 січня. Всім користувачам та адміністраторам настійно рекомендується негайно оновити систему до останньої версії, дотримуючись вказівок CISA, щоб мінімізувати ризик атак та запобігти компрометації». ***(Gintaras Radauskas. SolarWinds Web Help Desk users under threat as vulnerability actively exploited // Cybernews (https://cybernews.com/security/solarwinds-web-help-desk-vulnerability-exploited/). 05.02.2026).***

***

«Китайська група Amaranth Dragon, що фінансується державою, приєдналася до списку зловмисників, які використовують нещодавно виявлену вразливість WinRAR високого рівня небезпеки (CVE-2025-8088), яка дозволяє зловмисникам виконувати довільний код на скомпрометованих системах. Ця вразливість, що впливає на версії WinRAR 7.12 і старіші, має рівень небезпеки 8,4/10 і активно використовується з середини 2025 року…

Дослідники Check Point повідомляють, що Amaranth Dragon, який, як вважається, пов'язаний з APT41, атакував організації в Сінгапурі, Таїланді, Індонезії, Камбоджі, Лаосі та на Філіппінах. Група використовує комбінацію легальних інструментів і спеціального завантажувача для розгортання зашифрованих корисних даних із серверів, прихованих за інфраструктурою Cloudflare. Атака часто передбачає розміщення в архіві фальшивого документа, тоді як шкідливі записи Alternate Data Streams (ADS) доставляють приховані корисні дані.

Інші групи, включаючи проросійські RomCom, APT44, Turla, Carpathian та інші китайські суб'єкти, також використовували цю вразливість для розповсюдження різних шкідливих програм, таких як NESTPACKER і POISONIVY. Група Threat Intelligence Group компанії Google зазначила, що перше зловживання було виявлено в середині липня 2025 року, а Amaranth Dragon розпочав свої кампанії незабаром після випуску першого публічного експлойта. Широке поширення зловживань підкреслює нагальну необхідність для користувачів оновити WinRAR до останньої версії, щоб зменшити ці загрози…»

(Sead Fadilpašić. Dangerous new malware exploits WinRAR flaw - here's what we know // Future US, Inc. (https://www.techradar.com/pro/security/dangerous-new-malware-exploits-winrar-flaw-heres-what-we-know). 05.02.2026).

***

«Агентство з кібербезпеки та безпеки інфраструктури США (CISA) наказало федеральним агентствам терміново виправити п'ятирічну вразливість GitLab (CVE-2021-39935), яка активно використовується в кібератаках. Ця вразливість серверної сторони запиту (SSRF), виправлена GitLab у грудні 2021 року, дозволяє неавторизованим зловмисникам отримати доступ до CI Lint API і потенційно виконувати несанкціоновані запити на стороні сервера, навіть якщо реєстрація користувачів обмежена…

Ця вразливість впливає на декілька версій GitLab Community та Enterprise Editions, і CISA додала її до свого Каталогу відомих вразливостей, що експлуатуються, вимагаючи від федеральних цивільних виконавчих органів виправити свої системи до 24 лютого 2026 року відповідно до Обов'язкової оперативної директиви (BOD) 22-01. Хоча директива є обов'язковою для федеральних агентств, CISA настійно закликає всі організації, включаючи приватний сектор, надати пріоритет виправленню цієї вразливості через її часте використання зловмисниками…

В даний час в мережі знаходиться понад 49 000 пристроїв, що мають доступ до GitLab, більшість з яких розташована в Китаї. Платформа DevSecOps від GitLab широко використовується, в тому числі більш ніж половиною компаній зі списку Fortune 100. Попередження CISA з'явилося на тлі більш широких зусиль щодо усунення активно експлуатованих вразливостей, включаючи недавню критичну уразливість SolarWinds Web Help Desk, що підкреслює постійний ризик, який представляє незахищене програмне забезпечення в критичній інфраструктурі та корпоративних середовищах». ***(Sergiu Gatlan. CISA warns of five-year-old GitLab flaw exploited in attacks // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/cisa-warns-of-five-year-old-gitlab-flaw-exploited-in-attacks/). 04.02.2026).***

****

«Критична вразливість (CVE-2025-11953) у сервері розробки React Native Metro активно використовується зловмисниками для доставки шкідливого програмного забезпечення як на системи Windows, так і на Linux, проте ця загроза не отримала широкого розголосу. Ця вразливість впливає на командний рядок React Native Community, популярний пакет npm, який щотижня завантажують майже 2,5 мільйона разів, і дозволяє зловмисникам без аутентифікації виконувати довільні команди на вразливих серверах за допомогою введення команд ОС.

Виявлена дослідниками JFrog і оцінена в 9,8 (критична) за шкалою CVSS, ця помилка була розкрита на початку листопада після того, як Meta випустила виправлення. Експлойти для підтвердження концепції з'явилися на GitHub того ж

дня, а спроби експлуатації були помічені вже в грудні, задовго до того, як вразливість була широко визнана як реальна загроза…

Зловмисники використовували багатоступеневі завантажувачі на базі PowerShell для вимкнення Microsoft Defender і розгортання шкідливого програмного забезпечення на базі Rust з функціями захисту від аналізу. Атаки були відстежені до декількох IP-адрес і були спрямовані як на комп'ютери з Windows, так і на комп'ютери з Linux, а корисні дані розміщувалися на певних серверах.

Експерти з безпеки попереджають, що інструменти для розробників, такі як React Native, які широко використовуються, але не підлягають постійному моніторингу, є привабливими цілями для раннього використання. Відсутність широкого публічного визнання та низькі показники ймовірності використання в системах, таких як EPSS (Система оцінки прогнозування експлойтів), підкреслюють небезпечну розбіжність між фактичною активністю загроз та обізнаністю спільноти. Розробникам настійно рекомендується своєчасно оновлювати свої інструменти та ставитися до середовищ розробки з такою ж суворістю в питаннях безпеки, як і до виробничих систем…» ***(Jessica Lyons. Critical React Native Metro dev server bug under attack as researchers scream into the void // The Register (https://www.theregister.com/2026/02/03/critical_react_native_metro_server/). 03.02.2026).***

***

«Звіт Black Duck «Аналіз безпеки та ризиків відкритого програмного забезпечення (OSSRA) за 2026 рік» показує різке зростання кількості вразливостей відкритого програмного забезпечення в комерційних кодових базах. Середня кількість вразливостей відкритого програмного забезпечення зросла на 107% у 2024 році, що було спричинено збільшенням розміру кодової бази на 74% та зростанням кількості компонентів відкритого програмного забезпечення на 30%. В середньому кодові бази зараз містять 581 вразливість (більше, ніж у попередні роки) і 237 унікальних вразливостей, а деякі досягають майже 39 000 вразливостей загалом. Звіт пояснює частину цього зростання швидким генеруванням коду за допомогою AI-асистентів кодування, які прискорюють розробку, але також посилюють розширення залежностей і успадковують відомі недоліки з популярних бібліотек…

Незважаючи на загальне збільшення, частка кодових баз з високим рівнем серйозності та критичними вразливостями дещо зменшилася, хоча 78% все ще містять проблеми високого рівня серйозності, а 44% — критичні. Найпоширенішими вразливостями залишаються старі недоліки міжсайтового скриптингу в jQuery (CVE-2020-11022 та CVE-2020-11023), кожна з яких присутня в 28% кодових баз. Крім того, 92% кодових баз містять компоненти, які застаріли щонайменше на чотири роки, 93% мають компоненти, що не підтримуються, а 92% відстають на 10 або більше версій, що створює значний «борг з технічного обслуговування» напередодні введення в дію Закону ЄС про кіберстійкість у вересні 2026 року…

У звіті міститься застереження, що організації повинні впровадити точні, постійно оновлювані специфікації програмного забезпечення (SBOM), надійне управління вразливостями та проактивну заміну або виправлення «зомбі-компонентів», щоб відповідати майбутнім нормам та зменшити зростаючі ризики, пов'язані з відкритим кодом. Експерти з безпеки наголошують, що поєднання швидкості розробки на основі штучного інтелекту та розширення залежності від застарілих технологій випереджає традиційне управління, що робить прозорість та автоматизоване управління ризиками обов'язковими». ***(Laura French. Open-source vulnerabilities per codebase surge by 107% // CyberRisk Alliance (https://www.scworld.com/news/open-source-vulnerabilities-per-codebase-surge-by-107). 26.02.2026).***

***

«…Дослідники з Каліфорнійського університету в Ріверсайді виявили вразливості «AirSnitch», які підривають ізоляцію клієнтів WiFi — ключову функцію безпеки, призначену для запобігання комунікації між пристроями в одній мережі — і наражають мільярди пристроїв IoT на атаки типу «людина посередині» (MitM) попри шифрування WPA2/WPA3. Оскільки кількість підключених до мережі домашніх і комерційних пристроїв IoT, як очікується, подвоїться з 18,5 млрд у 2024 році до 39 млрд у 2030 році (а незабаром перевищить 50 млрд), розгалужені мережі WiFi стають головними цілями, проте 94% з них не мають навіть базового захисту від деавторизації…

Ізоляція клієнтів, яка не стандартизована в IEEE 802.11, не працює в різних реалізаціях через спільні групові ключі шифрування, розбіжності між рівнем 2 (MAC/link) і рівнем 3 (IP) та слабке прив'язування ідентичності пристроїв, що дозволяє зловмисникам підробляти MAC-адреси, вводити шкідливий трафік, перехоплювати дані, що надходять з Інтернету, маніпулювати пакетами або підробляти позиції MitM. Команда продемонструвала чотири практичні експлойти на 11 маршрутизаторах від Cisco, Netgear, D-Link, Asus та Ubiquiti, які були вразливі принаймні до одного з них, що давало змогу здійснювати атаки на вищих рівнях, такі як дешифрування HTTPS через невиправлені недоліки (D)TLS, крадіжку файлів cookie або отруєння DNS. Головний автор Xin’an Zhou назвав це «фізичним прослуховуванням», яке загрожує глобальній безпеці мережі, та закликав постачальників стандартизувати та посилити ізоляцію на всіх рівнях». ***(Jeffrey Burt. Scientists Intro AirSnitch, Which Bypasses WiFi Isolation to Launch Attacks on Networks // Techstrong Group Inc. (https://securityboulevard.com/2026/02/scientists-intro-airsnitch-which-bypasses-wifi-isolation-to-launch-attacks-on-networks/). 27.02.2026).***

***

«Claude Code Security, нова функція, вбудована в Claude Code, тепер доступна в обмеженому дослідному попередньому перегляді для корпоративних клієнтів і клієнтів Team, з прискореним доступом для розробників відкритого програмного забезпечення. Розроблена для вирішення проблеми постійно зростаючого обсягу вразливостей програмного забезпечення, Claude Code Security сканує кодові бази на наявність проблем безпеки, які часто пропускають традиційні інструменти статичного аналізу, засновані на правилах. На відміну від цих інструментів, які шукають відомі шаблони, Claude Code Security читає та аналізує код, як людський дослідник безпеки, розуміючи взаємодію компонентів та відстежуючи потік даних, щоб виявити складні, залежні від контексту вразливості…

Система використовує багатоступеневий процес перевірки, в ході якого Claude повторно перевіряє власні висновки, щоб відфільтрувати помилкові спрацьовування, і присвоює рейтинги серйозності, щоб допомогти командам визначити пріоритетність виправлень. Усі підтверджені висновки, разом із запропонованими програмними виправленнями та рейтингом надійності, представлені на інформаційній панелі для перевірки та затвердження людиною — остаточне рішення завжди приймають розробники. Цей інструмент є результатом понад річної роботи дослідницької групи Frontier Red Team компанії Anthropic, яка провела стрес-тестування можливостей Claude в галузі кібербезпеки в різних сценаріях, зокрема виявила понад 500 вразливостей у виробничих кодових базах з відкритим кодом за допомогою нещодавно випущеного Claude Opus 4.6. У міру зростання ролі ШІ в кібербезпеці, Claude Code Security прагне надати захисникам можливість знаходити та виправляти слабкі місця швидше, ніж зловмисники можуть ними скористатися, що в кінцевому підсумку підвищить базовий рівень безпеки в усій галузі». ***(Making frontier cybersecurity capabilities available to defenders // Anthropic PBC (https://www.anthropic.com/news/claude-code-security). 20.02.2026).***

***

Основи кібергігієни

«Нове дослідження компанії Plasma визначило найвразливіші паролі 2026 року, проаналізувавши списки поширених паролів від Comparitech і NordPass та співвіднісши їх із глобальними обсягами пошуку для оцінки популярності. На першому місці в списку найнебезпечніших паролів знаходиться «password» (пароль), який за останній рік шукали понад 10,3 мільйона разів, за ним йдуть інші легко вгадувані комбінації, такі як «admin» (адміністратор), «qwerty» (кверті) та послідовні цифри, наприклад «123456» і «111111». Дослідження також виявило категорії найвразливіших паролів, серед яких найбільш вразливими до

атак є паролі, засновані на зростаючих/спадаючих послідовностях, клавіатурних шаблонах та простих буквено-цифрових комбінаціях… Представник Plasma підкреслив, що багато користувачів помилково вважають, що прості комбінації літер, символів і цифр створюють надійний пароль, тоді як насправді передбачувані шаблони легко зламати методом грубої сили. Щоб ефективно зменшити ризик несанкціонованого доступу, надійний пароль повинен бути розроблений таким чином, щоб протистояти систематичним атакам, а не бути легким для запам'ятовування, і завжди повинен поєднуватися з багатофакторною автентифікацією». ***(The 25 Most Vulnerable Passwords of 2026 // BNP Media (https://www.securitymagazine.com/articles/102132-the-25-most-vulnerable-passwords-of-2026). 20.02.2026).***

***