**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

№ 1 (січень)

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. № 1 (січень). 139 с.

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

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

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

ЗМІСТ

Кібервійна проти України та операції у відповідь

«Проросійський зловмисник UAC-0184 (також відомий як Hive0156) продовжує свою інтенсивну кампанію зі збору розвідданих проти українських військових і урядових структур у 2025 році, вдосконалюючи свою тактику і використовуючи месенджер Viber для поширення шкідливого програмного забезпечення. Спираючись на попередні кампанії, в яких використовувалися Signal і Telegram, група поширює шкідливі ZIP-архіви, що містять підроблені файли ярликів Windows (LNK), замасковані під легітимні документи…

При відкритті ці LNK-файли відображають фальшивий документ, одночасно тихо виконуючи скрипт PowerShell для завантаження другого ZIP-архіву та розгортання Hijack Loader за допомогою просунутих методів ухилення, таких як бічне завантаження DLL та модульне стемпінг. Потім Hijack Loader сканує систему на наявність програмного забезпечення для забезпечення безпеки (такого як Kaspersky і Microsoft Defender), встановлює стійкість і вводить Remcos RAT у легітимний процес (chime.exe). Цей потужний інструмент віддаленого адміністрування надає зловмисникам повний контроль над ураженою кінцевою точкою, що дозволяє здійснювати кібершпигунство, крадіжку даних і точні ручні операції через графічну панель управління…» ***(Ravie Lakshmanan. Russia-Aligned Hackers Abuse Viber to Target Ukrainian Military and Government // The Hacker News (https://thehackernews.com/2026/01/russia-aligned-hackers-abuse-viber-to.html). 05.01.2026).***

***

«…Кадри в галузі кібербезпеки зазнають швидких змін під впливом штучного інтелекту, нових ІТ-можливостей та зростаючих геополітичних загроз. Учасники панельної дискусії на конференції The Cyber Guild 2025 погодилися, що виклик зараз виходить далеко за межі простого «дефіциту кваліфікованих кадрів». Штучний інтелект сортує низькорівневі сповіщення та пише базовий код, змушуючи центри безпеки переходити від аналітиків першого рівня до ролей вищого рівня, які вимагають критичного мислення, аналізу ланцюжків загроз та адаптивності. Такі компанії, як DXC Technology, вже планують, як перерозподілити або підвищити кваліфікацію персоналу, оскільки штучний інтелект зменшує кількість рутинних завдань…

Традиційні фільтри при наймі на роботу — чотирирічна вища освіта, сертифікати, суто технічні резюме — більше не відповідають сучасним загрозам, заявила заступник директора з інформаційної безпеки Mastercard Алісса Абдулла. Натомість компанії шукають здібності, допитливість і «стійкі» м'які навички:

вміння співпрацювати, вирішувати проблеми та швидко навчатися. ISC2, найбільш відома завдяки CISSP, підтримала цю думку, закликаючи менеджерів наймати співробітників за їхнім потенціалом, а не за паперовими дипломами. Водночас команди з найму повинні стежити за витонченими шахрайськими діями: зараз зловмисники використовують дипфейки та аутсорсингові співбесіди, щоб проникнути в організації…

Практичні заняття мають вирішальне значення. DXC та інші роботодавці створюють кіберполігони, які відтворюють реальні атаки, щоб навчати студентів і перевіряти кандидатів особисто — це протиотрута від фальсифікації резюме та шахрайства за допомогою штучного інтелекту. Учасники дискусії стверджували, що університети повинні інтегрувати такі полігони, щоб вивести навчальні програми за межі статичних «книжкових знань»…

Розвиток м'яких навичок та просвітницька діяльність також мають значення. Такі впливові особи, як «CyberSecurity Girl» Кейтлін Саріан, використовують соціальні мережі, щоб розвіяти міфи про кар'єру в галузі кібербезпеки та залучити різноманітних молодих талантів. Нетрадиційний досвід — домашні лабораторії, робота в поліції у сфері боротьби з підробкою документів — може перетворитися на цінні знання для управління ідентифікацією або пошуку загроз.

Зрештою, керівники повинні ставитися до безпеки як до необхідності для збереження доходів, а не як до центру витрат. Організації, які застосовують гнучке наймання, постійне підвищення кваліфікації та робочі процеси, доповнені штучним інтелектом, будуть йти в ногу з зловмисниками, які безперервно повторюють свої дії. Ті, хто дотримується застарілих посадових інструкцій та вимог до освіти, ризикують як нестачею талантів, так і порушеннями безпеки». ***(Kimberly Underwood. The Modern Cyber Workforce // AFCEA International (https://www.afcea.org/signal-media/cyber-edge/modern-cyber-workforce). 01.01.2026).***

***

«…Аналіз прогнозів експертів з кібербезпеки на 2025 рік показує, що найточніші прогнози стосувалися не нових загроз, а того, що існуючі атаки стануть простішими, швидшими та масштабнішими, насамперед завдяки штучному інтелекту. З понад 90 різних прогнозів, загальна думка була такою, що 2025 рік буде характеризуватися підвищенням ефективності зловмисників, а найдомінантнішою темою буде штучний інтелект, що дозволить здійснювати більш складні кібератаки (58% прогнозів)…

Реальність 2025 року підтвердила цю тенденцію: атаки на основі штучного інтелекту, включаючи фішинг із використанням штучного інтелекту та автоматизовану розвідку, прискорили весь цикл кібератак і знизили бар'єр для входу в цю сферу для менш кваліфікованих злочинців. Зокрема, аналітика загроз Google підтвердила, що зловмисники використовували інструменти штучного інтелекту для вдосконалення всіх етапів атак, включаючи появу першого в своєму роді шкідливого програмного забезпечення на базі штучного інтелекту, здатного «на льоту» переписувати код, щоб уникнути виявлення…

Інші точно передбачені тенденції включали те, що SaaS і хмарні ризики затьмарять периметральну безпеку (передбачено 29%), з гучними випадками відключення хмарних сервісів і нульовими днями експлуатації, що виникають через неправильні налаштування та проблеми з ідентифікацією доступу. Також було правильно передбачено, що програмне забезпечення для вимагання викупу стане проблемою фрагментованої екосистеми, а тиск з боку правоохоронних органів призведе до 30-40% зростання кількості невеликих, важко відстежуваних груп, які займаються «переходом з однієї банди в іншу». Крім того, захист даних та управління ними були визнані основними пріоритетами, а дані стали головним полем битви, що лежить в основі більшості проблем безпеки, особливо в контексті навчання штучного інтелекту та витоку паролів.

І навпаки, хоча регулювання увійшло до топ-10 прогнозів, воно не змогло істотно змінити ситуацію з загрозами, виявившись скоріше фактором, що ускладнює ситуацію, ніж рішенням. Зрештою, 2025 рік продемонстрував, що найбільшими ризиками для кібербезпеки були відомі загрози, з якими організації не змогли впоратися належним чином, створивши передумови для 2026 року, де підготовка до цих прискорюваних, підсилених штучним інтелектом ризиків стане критичним випробуванням…» ***(Stefanie Schappert. What cybersecurity experts predicted for 2025 - and what actually happened // Cybernews (https://cybernews.com/news/did-cybersecurity-expert-predictions-2025-come-true/). 01.01.2026).***

***

«Прогнози щодо кібербезпеки на 2026 рік вказують на критичну зміну, коли традиційні засоби захисту периметра стануть недостатніми, а виживання організацій залежатиме від надійної аутентифікації та стратегії захисту, що базується на електронній пошті, проти швидко розвиваючихся загроз. Глобальна кіберзлочинність посилиться, оскільки зловмисники використовуватимуть генеративну та агентивну штучну інтелігенцію для автоматизації кампаній та створення фішингу на основі штучного інтелекту, який буде гіперперсоналізованим, багатоканальним і практично не відрізнятиметься від законного спілкування, що зробить традиційні шлюзи безпеки та базове навчання з питань безпеки застарілими…

Основним прогнозом на 2026 рік є те, що застосування Аутентифікація, звітність та відповідність повідомлень на основі домену (DMARC) стане глобальною базовою вимогою, переходячи від політики, що передбачає лише моніторинг (p=none), до повного застосування з метою припинення підроблених електронних листів та зменшення профілю ризику домену у основних постачальників поштових скриньок. Це буде доповнено стрімким зростанням популярності Індикаторів бренду для ідентифікації повідомлень (BIMI), що допоможе клієнтам візуально перевіряти надійні повідомлення за допомогою логотипу бренду, підвищуючи як безпеку, так і надійність доставки…

Незважаючи на свою фундаментальність, Структура політики відправника (SPF) та ідентифікована пошта DomainKeys (DKIM) досягнуть своїх меж через складність роботи з декількома сторонніми відправниками, що вимагатиме більш

широкого використання Authenticated Received Chain (ARC) та послуг автоматизації, таких як SPF flattening. Ця увага до ідентичності є частиною більш широкої тенденції: модель Zero Trust вийде на перший план, ставлячи сильну багатофакторну автентифікацію та умовний доступ в основу стратегій захисту. Нарешті, автоматизація стає необхідною, а не опціональною, оскільки ручні операції з безпеки не можуть йти в ногу з атаками, що базуються на штучному інтелекті, що вимагає автоматизованих інструментів для аналізу звітів DMARC, обслуговування SPF та оповіщення про несанкціоноване використання домену…

Щоб підготуватися до 2026 року, компанії повинні провести аудит усіх доменів, перейти до впровадження DMARC, стабілізувати записи SPF/DKIM, спланувати впровадження BIMI, привести свою діяльність у відповідність до принципів Zero Trust та поступово впроваджувати автоматизацію, змінюючи свою позицію з реактивної на автоматизовану, орієнтовану на електронну пошту». ***(Kiara Saloojee. Email-first cybersecurity predictions for 2026 // Techstrong Group Inc. (https://securityboulevard.com/2026/01/email-first-cybersecurity-predictions-for-2026/). 02.01.2026).***

***

«Середовище кібербезпеки в 2026 році буде визначатися трьома глибоко взаємопов'язаними тенденціями, що вимагатимуть переходу від реактивної безпеки до проактивної, заснованої на розвідці стійкості…

По-перше, геополітичні суперечності залишатимуться фактором, що посилює кіберризики. Глобальні конфлікти, такі як війна в Україні та стратегічне суперництво в Східній Азії, поширюються на кіберпростір. Напівпровідникова промисловість, яка залежить від таких регіонів, як Тайвань і рідкісні землі Китаю, відіграє центральну роль у цій динаміці. Для підприємств це вимагає інтеграції геополітичної розвідки в планування стійкості, постійного відстеження залежності від постачальників та передбачення того, як політичні зміни або санкції можуть спровокувати нові кампанії загроз…

По-друге, морські перевезення та морська логістика стануть головними цілями. Як основа міжнародної торгівлі, морська галузь представляє великі можливості для зловмисників, про що свідчить зростання кількості інцидентів, про які повідомляє Кіберкомандування берегової охорони. З огляду на те, що глобальні конфлікти змінюють торговельні маршрути, очікується, що зловмисники посилять кампанії, спрямовані на логістичну видимість, портові операції та суднову комунікацію, що вимагатиме моніторингу в режимі реального часу та сегментації мережі операційних технологій…

Нарешті, тіньова ШІ стане наступною некерованою поверхнею ризику. Поспіх із впровадженням генеративної ШІ створює значну внутрішню вразливість, оскільки співробітники використовують неперевірені інструменти ШІ без чіткого управління. Ця тіньова ШІ, яка, за прогнозами Gartner, вплине на 40% компаній, створює серйозні проблеми з видимістю та наражає на ризик конфіденційні дані, особливо з огляду на те, що багато організацій не мають чітко визначених процесів уразливості ШІ та інструкцій з реагування на інциденти. Перспективні організації повинні інтегрувати засоби управління ШІ в існуючі кіберпрограми, розглядаючи

доступ до моделей та походження даних як основні пріоритети управління ризиками на 2026 рік». ***(Yuval Wollman. Cyber Risk In 2026: How Geopolitics, Supply Chains and Shadow AI Will Test Resilience // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/opinions/geopolitics-supply-chains-shadow/). 02.01.2026).***

***

«Дослідження ISC2 «Кадри в галузі кібербезпеки до 2025 року», проведене на основі відповідей понад 16 000 фахівців з усього світу, показує, що головним болючим питанням для команд з безпеки зараз є не брак кадрів, а брак навичок. Хоча економічний тиск, який спричинив звільнення та скорочення бюджетів у 2024 році, стабілізувався (про скорочення повідомили 36% респондентів, про звільнення — 24%), 33% організацій все ще не мають достатніх коштів для належного укомплектування команд, а 29% заявляють, що не можуть собі дозволити наймати фахівців з відповідною кваліфікацією. Майже дев'ять з десяти респондентів (88%) зазнали принаймні одного серйозного інциденту безпеки, пов'язаного з браком кваліфікованих кадрів; 59% описують свої прогалини як «критичні або значні»…

Основними технічними недоліками є штучний інтелект і безпека хмарних технологій: 41% респондентів називають штучний інтелект і 36% — хмарні технології як нагальні потреби. Впровадження штучного інтелекту відбувається стрімкими темпами: 28% вже інтегрували інструменти штучного інтелекту, а 69% використовують, тестують або оцінюють їх, тоді як 48% практиків самостійно навчаються, щоб отримати знання в галузі штучного інтелекту. Більшість вважає, що штучний інтелект створить нові спеціалізовані ролі (73%), вимагатиме більш стратегічного мислення (72%) і розширить необхідні навички (66%).

Настрої серед працівників залишаються позитивними: 87% вважають, що фахівці з кібербезпеки завжди будуть потрібні; 81% впевнені в майбутньому цієї професії; 68% задоволені своєю поточною роботою, а 80% відчувають пристрасть до своєї справи. Проте майже половина відчуває виснаження від необхідності постійно стежити за загрозами та технологіями, а 47% перевантажені роботою…

ISC2 робить висновок, що розвиток потенціалу — навчання, перехресне навчання, підвищення кваліфікації в галузі ШІ та реалістичне управління робочим навантаженням — зараз є більш важливим, ніж просто наймання більшої кількості людей. Правління та керівники служб інформаційної безпеки повинні постійно інвестувати в навички, узгоджувати бюджети з реальними даними про загрози та розглядати експертизу в галузі ШІ як стратегічну необхідність для усунення зростаючого дефіциту талантів та зменшення ризику порушень». ***(Cybersecurity skills matter more than headcount in the AI era // FoundryCo, Inc. (https://www.csoonline.com/article/4108270/cybersecurity-skills-matter-more-than-headcount-in-the-ai-era.html). 02.01.2026).***

***

«…У 2026 році керівники служб інформаційної безпеки перейдуть від «більшого контролю» до вимірюваної стійкості, при цьому в різних галузях сформується дванадцять пріоритетів…

Проектуйте з урахуванням стійкості, а не реакції. Нові проекти будуть починатися з ретельних архітектурних креслень, що відображають залежності та точки відмови, щоб перебої в роботі передбачалися, а не сортувалися.

Поставте ШІ в центр — в наступальному та оборонному плані. Керівники служб інформаційної безпеки (CISO) зміцнять нові поверхні атак, що базуються на ШІ, використовуючи ШІ для швидшого виявлення, координації та сортування SOC, перетворюючи технологію з наукового проекту на двигун бізнесу.

Відновіть видимість та контроль. Тіньовий SaaS, несанкціоновані чат-боти та неформальне використання ШІ будуть виявлятися за допомогою інструментів виявлення, а автоматизація дотримання вимог, канали інформації про загрози та управління вразливостями будуть йти в ногу зі змінами…

Майстер ідентичності — людина і машина. Сервісні облікові записи, API та «нелюдські ідентичності» агентного ШІ повинні регулюватися з такою ж суворістю, як і входи користувачів, що робить управління ідентичністю та привілеями новим периметром.

Вбудуйте безпеку в продукти на основі агентного ШІ. Команди вбудують захисні бар'єри безпосередньо в код, щоб «безпечний шлях був найшвидшим шляхом», і використовуватимуть ШІ для автоматизації тестування контролю та сортування інцидентів.

Перетворіть безпеку на видимий сигнал довіри. Сертифікати, такі як FedRAMP High та ISO 42001, будуть розглядатися як диференціатори виходу на ринок; прозорість щодо обробки даних та управління ШІ приверне клієнтів…

Складіть план підготовки до квантової ери. Інвентаризація криптографії, анкетування постачальників та плани щодо постквантових алгоритмів почнуться вже зараз, до того, як сучасні засоби шифрування втратять свою ефективність.

Захищайте людей, а не тільки системи. З огляду на вигорання, зміни навичок під впливом штучного інтелекту та незмінні бюджети, керівники служб інформаційної безпеки інвестуватимуть у добробут персоналу та постійне підвищення кваліфікації.

Виявляйте порушення першими. Сама лише профілактика вже не актуальна; у світі, насиченому SaaS та штучним інтелектом, гіпервидимість та швидке реагування будуть важливішими за неприступні стіни…

Подивіться за горизонт. Керівники служб інформаційної безпеки узгодять бюджети з прогнозами загроз від WEF, ENISA та ISF, щоб заздалегідь розробити заходи контролю на 12–36 місяців вперед.

Усуньте мовний бар'єр у раді директорів. Керівники служб безпеки перетворять технічні ризики на фінансові та операційні наслідки, а ради директорів будуть розглядати кіберстійкість як конкурентну перевагу, а не витрати.

Вимагайте результатів, а не емоцій. Кожна ініціатива, особливо в галузі штучного інтелекту, повинна демонструвати рентабельність інвестицій та вимірюване зниження ризиків; управління, прозорість та дисципліноване виконання замінять ажіотаж…

Разом ці теми знаменують перехід від реактивної, орієнтованої на інструменти безпеки до інтегрованої стійкості, де архітектура, ідентичність, управління штучним інтелектом та чітка ділова комунікація визначають успіх». ***(Rosalyn Page. Cybersecurity leaders' resolutions for 2026 // FoundryCo, Inc. (https://www.csoonline.com/article/4110151/cybersecurity-leaders-resolutions-for-2026.html). 05.01.2026).***

***

«…Оскільки кібератаки тепер є питанням часу, а не ймовірності, організації повинні перейти від простої профілактики до багаторівневої системи безпеки, що забезпечує швидке реагування. Ось вісім ключових кроків, які допоможуть британським організаціям отримати найсильнішу позицію для швидкого та ефективного реагування на будь-яку кібератаку.

• Цілодобовий моніторинг загроз. Впровадьте SIEM, EDR та автоматичне встановлення виправлень в архітектурі Zero-Trust; шифруйте дані; зміцнюйте хмарні та сторонні ланцюги постачання за допомогою аудитів та положень про мінімальний рівень безпеки.

• Людський брандмауер. Обов'язкове навчання з підвищення обізнаності, регулярні симуляції фішингу, MFA та чіткі шляхи ескалації зменшують ризик помилок співробітників, який все ще залишається домінуючим; порушення політики повинні мати наслідки.

• План реагування на інциденти NIST/SANS. Підготовка, виявлення, локалізація, ліквідація, відновлення та аналіз; підтримка офлайн-резервних копій 3-2-1-1-0 та репетиції за допомогою настільних та кібер-вправ.

• План дій у разі конкретних атак. Заздалегідь затверджені кроки, шляхи ескалації та шаблони комунікацій для випадків використання програм-вимагачів, компрометації ділової електронної пошти, DDoS-атак та отруєння даних скорочують час реагування.

• Кризові комунікації. Своєчасні та послідовні оновлення від призначеного речника зберігають довіру; готові повідомлення запобігають затримкам.

• Юридична та нормативна відповідність. Повідомляйте про порушення до ICO протягом 72 годин, залучайте NCSC та Action Fraud і забезпечуйте постійну конфіденційність, цілісність та доступність персональних даних.

• Адаптивні трудові договори. Пункти про перерозподіл ролей, зміну режиму роботи та тимчасове звільнення надають керівництву гнучкість під час кіберзбоїв, дозволяючи при цьому зберегти ключових співробітників.

• Додаткові засоби захисту. Сегментація мережі, виявлення кінцевих точок, захисні заходи на основі моделей штучного інтелекту, щоквартальні оцінки ризиків, посилення конфігурації та кіберстрахування доповнюють багаторівневий захист…

Гучні інциденти, що сталися з такими брендами, як M&S, Harrods і Jaguar Land Rover, демонструють фінансові збитки та репутаційні втрати, до яких може призвести недостатня підготовка. Організації, які вже зараз інвестують у постійний моніторинг, навчання персоналу, відпрацювання реагування на надзвичайні ситуації та чітке управління, зможуть обмежити час простою, захистити

конфіденційні дані та зберегти довіру клієнтів у умовах дедалі більш цифрової економіки…» ***(Eleanore Beard. Cyber-attacks — 8 essential steps to strengthen your response before it's too late // Brabners (https://www.brabners.com/insights/technology-media-telecoms/cyber-attacks-8-essential-steps-to-strengthen-your-response-before-its-too-late). 12.01.2026).***

***

«У 2026 році кібербезпека зазнає змін під впливом тих самих технологій, які покликані сприяти цифровій трансформації. IBM попереджає, що прогрес у галузі штучного інтелекту, квантових обчислень та дипфейків одночасно створює потужні засоби захисту та безпрецедентні можливості для атак. Основною проблемою є «тіньовий штучний інтелект» — несанкціоновані або неліцензовані системи штучного інтелекту, що функціонують в організаціях поза межами належного управління та контролю безпеки. За оцінками, ці приховані інструменти додають приблизно 670 000 доларів до середньої вартості порушення безпеки даних, проте близько 60% організацій все ще не мають політик для управління ними. Водночас між 2023 і 2025 роками кількість дипфейків зросла на 1500%, що дозволяє створювати дуже переконливі підробки, які сприяють соціальній інженерії, шахрайству з ідентифікацією та дезінформації. Кіберзлочинці все частіше використовують штучний інтелект для створення адаптивного, поліморфного шкідливого програмного забезпечення, експлуатації вразливостей у великих мовних моделях за допомогою швидкого введення та автоматизації значної частини операцій з фішингу, викрадення даних та шахрайства, змушуючи захисників застосовувати власні інструменти на основі штучного інтелекту для виявлення, реагування та постійної оцінки загроз…

Квантові обчислення додають ще один рівень ризику: їхня майбутня здатність зламати широко використовувану криптографію з відкритим ключем може зробити сучасне шифрування застарілим і викрити величезні масиви конфіденційних даних, що робить необхідним завчасне планування квантово-безпечної криптографії та довгострокової стійкості. Тим часом автономні агенти штучного інтелекту та нелюдські цифрові ідентичності поширюються, пропонуючи операційні переваги, але також створюючи нові можливості для експлойтів без кліків, підвищення привілеїв та важко відстежуваних автоматизованих атак у разі компрометації. Штучний інтелект та дипфейки разом підсилюють соціальну інженерію, роблячи обманні комунікації набагато складнішими для виявлення людьми. У відповідь на це організації змушені посилювати управління штучним інтелектом, надійно контролювати всі впровадження штучного інтелекту, посилювати управління ідентифікацією та доступом як для людей, так і для агентів штучного інтелекту, а також проводити постійне навчання співробітників, зосереджене на скептицизмі та перевірці. Паролі-ключі стають ключовим захисним противагою: як альтернатива паролям, стійка до фішингу та крадіжки облікових даних, вони, як очікується, стануть новим стандартом аутентифікації. Загалом, у 2026 році інновації та вразливість будуть тісно пов'язані між собою; щоб досягти успіху в таких умовах, необхідно проактивно впроваджувати засоби захисту на основі ШІ, ретельно контролювати використання ШІ, готуватися до квантової ери

та перейти від реактивних контрольних списків відповідності до безперервної кібербезпеки, заснованої на ризиках». ***(Julian Horsey. Cybersecurity Trends 2026 : From Unapproved AI to Passkeys, Clear Steps to Stay Safe // Geeky Gadgets (https://www.geeky-gadgets.com/cybersecurity-trends-2026/). 14.01.2026).***

***

«Вісім із десяти хедж-фондів та інших інвестиційних фірм збільшили витрати на кібербезпеку у 2025 році, згідно зі звітом Асоціації хедж-фондів та SeaGlass Technology, опублікованим у вівторок.

Близько половини цих фірм заявили, що протягом останніх 12 місяців їхня система зазнала порушень. Опитування базується на відповідях 400 керівників цих фірм, включаючи менеджерів хедж-фондів, інституційних інвесторів та постачальників галузевих послуг.

Фішинг був головною проблемою приблизно двох третин опитаних.

Близько половини респондентів заявили, що інциденти пов'язані з ризиком для третіх осіб, що викликає дедалі більше занепокоєння в різних галузях, оскільки компанії стають більш взаємопов'язаними.

Ці фірми планують збільшити витрати протягом наступних 12–24 місяців для підвищення стійкості. Пріоритети включають реагування на інциденти, виявлення загроз, безпеку хмарних технологій та кінцевих точок, а також управління ідентифікацією та доступом…» ***(David Jones. Majority of hedge funds boosted cybersecurity spending in 2025 // TechTarget, Inc. (https://www.cybersecuritydive.com/news/hedge-funds-cybersecurity-spending-2025/809488/). 13.01.2026).***

***

«Кібербезпека в 2026 році переживає перетворення під впливом шести ключових тенденцій, які ставлять на перший план довіру, інтелектуальну автоматизацію та конфіденційність даних.

По-перше, штучний інтелект буде визначати як наступальні, так і оборонні дії. Зловмисники використовують штучний інтелект для більш витончених і ефективних атак, а захисники — для проактивного управління вразливостями та автоматичного виявлення загроз. Однак людський контроль залишається вирішальним для контексту та прийняття стратегічних рішень…

По-друге, постійний моніторинг та хмарні архітектури стануть стандартом. У міру прискорення впровадження хмарних технологій стратегії безпеки зміщуються в бік аналізу даних у реальному часі та автоматизованого захисту, що робить постійний моніторинг безпеки та відповідності вимогам більш доступним і необхідним.

По-третє, на перший план вийде питання конфіденційності даних. На відміну від абстрактних порушень систем, порушення конфіденційності, що розкривають особисті дані про здоров'я або фінансові дані, мають прямий і безпосередній вплив на споживачів, що призводить до зростання суспільного попиту на більш жорстке регулювання, розширення вимог щодо згоди та посилення заходів з забезпечення дотримання вимог…

По-четверте, управління розширюється, навіть незважаючи на відставання в регулюванні штучного інтелекту. Хоча конкретні закони про штучний інтелект ще розробляються, існуючі рамки управління даними, такі як GDPR та NIST AI Risk Management Framework, стають все більш суворими, змушуючи організації створювати системи штучного інтелекту з прозорістю та підзвітністю з самого початку.

По-п'яте, інтелектуальні інструменти допоможуть вирішити проблему нестачі талановитих фахівців. ШІ стає «другим пілотом» для команд з кібербезпеки, автоматизуючи повторювані завдання та покращуючи процес прийняття рішень, щоб допомогти організаціям, які борються з постійною нестачею робочої сили. Однак він не може замінити тонке розуміння, необхідне для прийняття стратегічних рішень з безпеки…

Нарешті, довіра стане головним критерієм зрілості безпеки. У 2026 році організації будуть оцінюватися не за періодичними оцінками, а за їхньою здатністю постійно демонструвати стійкість, прозорість і надійність перед клієнтами, регуляторними органами та зацікавленими сторонами. Щоб підготуватися до цього, керівники служб безпеки повинні відповідально інтегрувати штучний інтелект, посилити контроль за хмарними технологіями та моніторингом, включити питання конфіденційності до своїх стратегій і сформувати культуру постійної, очевидної безпеки». ***(Justin Rende. The 6 Cybersecurity Trends That Will Shape 2026 // ISACA (https://www.isaca.org/resources/news-and-trends/industry-news/2026/the-6-cybersecurity-trends-that-will-shape-2026). 14.01.2026).***

***

«Кількісна оцінка кіберризиків перетворює абстрактні загрози безпеці на конкретні грошові суми, що дозволяє фінансовим директорам та іншим керівникам приймати обґрунтовані та виправдані рішення щодо інвестицій у безпеку. Це досягається за допомогою трьох основних методів: розрахунку очікуваного річного збитку (ALE), застосування структурованих моделей, таких як факторний аналіз інформаційних ризиків (FAIR), та проведення аналізу ймовірності та впливу. Оцінюючи ймовірність та фінансовий вплив потенційних інцидентів, включаючи втрату доходів, судові витрати та шкоду репутації, організації можуть визначити обґрунтовані діапазони збитків, які безпосередньо впливають на формування бюджету, стратегічне планування та розкриття інформації, що вимагається, наприклад, правилами SEC 2023 року…

Для ефективного інформування фінансового директора про ці ризики рекомендується використовувати п'ятикроковий план:

Оцініть очікувані річні збитки (ALE): Розрахуйте очікувані фінансові збитки від конкретного ризику протягом одного року, помноживши вартість одного інциденту на його річну частоту (ALE = SLE x ARO).

Використовуйте такі рамки, як FAIR: Проаналізуйте частоту та масштаб збитків, щоб створити криві розподілу ризиків, які показують не тільки середній збиток, але й ймовірність більш екстремальних сценаріїв «хвостового ризику».

Врахуйте витрати на регулювання та дотримання вимог: визначте суттєвість інцидентів на основі термінів розкриття інформації (наприклад, правило чотирьох

днів SEC) та інтегруйте кіберризики в більш широку систему управління ризиками підприємства (ERM), щоб продемонструвати комплексний нагляд.

Продемонструйте рентабельність інвестицій: сформулюйте заходи безпеки як інвестиції, кількісно оцінивши їхню віддачу. Наприклад, покажіть, як проект багатофакторної автентифікації вартістю 200 тис. доларів може зменшити ALE від фішингу на 1,5 млн доларів, приносячи значну віддачу.

Завоюйте довіру зацікавлених сторін: представте результати у вигляді чіткого звіту, орієнтованого на фінансового директора, що включає виконавче резюме, основні кількісно оцінені сценарії, відображені наслідки для бізнесу та план заходів із зменшення ризиків із зазначенням витрат і очікуваного зниження ризиків…

Перетворюючи технічні дані на фінансову інформацію, керівники служб кібербезпеки можуть змінити сприйняття своєї функції з центру витрат на стратегічний актив, який захищає цінність підприємства та формує довіру інвесторів, регуляторних органів та ради директорів». ***(Erin Nelson. Cyber Risk Quantification: How to Report Risks to Your CFO // Hyperproof (https://hyperproof.io/resource/cyber-risk-quantification/). 13.12.2026).***

***

«Багато організацій реагують на інциденти кібербезпеки панікою, а не процесом, що призводить до хаотичних, неефективних і дорогих результатів. Така «панічна» реакція характеризується неструктурованими командами, надмірними зусиллями та порушенням комунікації, що є наслідком недостатньої підготовки та надмірної залежності від інстинктів. Хоча така бурхлива діяльність може створювати ілюзію прогресу, вона в кінцевому підсумку збільшує ризик, виснажує команди та не вирішує основну проблему, оскільки аналіз після інциденту постійно виявляє ті самі помилки: відсутність плану, документації та ясності…

Протиотрутою від цього хаосу є не додаткові інструменти, а дисциплінована культура, орієнтована на процеси. Чітко визначений план реагування на інциденти з чіткими ролями, шляхами ескалації та протоколами комунікації усуває вагання і дозволяє командам зосередитися на вирішенні проблем, а не на обговоренні наступних кроків. Така структура перетворює реагування на «м'язову пам'ять», де спокій замінює плутанину…

Щоб досягти такого рівня зрілості, організації повинні вийти за межі базових настільних вправ і проводити тренування, що імітують реальні стресові ситуації, навчаючи команди керувати адреналіном і зберігати логіку. Вони також повинні автоматизувати повторювані завдання, залишаючи людей у циклі для остаточної перевірки, і розглядати постмортальні аналізи як плани для вдосконалення, відпрацьовуючи вдосконалення, поки вони не стануть другою натурою…

Зрештою, тон задає керівництво. Культура, яка цінує стабільну координацію більше, ніж відчайдушні героїчні вчинки, і яка розглядає інциденти як можливості для навчання, а не як приводи для звинувачень, формує стійку стійкість. Інвестуючи в процеси, репетиції та культуру спокою, організації можуть перетворити свою реакцію на інциденти з реактивної пожежної тренування на обдуману, точну та ефективну стратегію контролю кризових ситуацій». ***(Cyber***

Incident Response Done Right: Moving from Panic to Process // Cyber Management Alliance (https://www.cm-alliance.com/cybersecurity-blog/cyber-incident-response-done-right-moving-from-panic-to-process). 16.01.2026).

***

«Найм фахівців з кібербезпеки став серйозною оперативною проблемою, оскільки загрози зростають швидше, ніж кількість робочої сили, через що багато організацій не можуть укомплектувати критично важливі підрозділи. Згідно з доповіддю Всесвітнього економічного форуму «Глобальний прогноз у сфері кібербезпеки на 2024 рік», 71% організацій мають вакансії у сфері кібербезпеки, і цей дефіцит залишається головною перешкодою для посилення безпеки, що відображає не тільки нестачу кадрів, але й брак кваліфікованих фахівців, здатних захистити складні системи. Ця проблема ускладнюється застарілими практиками найму: у вакансіях часто вимагають нереалістичного досвіду роботи, довгого переліку інструментів та непотрібних дипломів, що відсіває сильних кандидатів, чий досвід не відповідає жорстким шаблонам, а повільні, багатоетапні процеси найму змушують найкращих кандидатів відмовлятися від роботи, що призводить до перевантаження існуючих команд…

Роботодавці все частіше віддають перевагу практичним навичкам, а не дипломам, використовуючи інтерв'ю на основі сценаріїв, щоб оцінити, як кандидати думають під тиском, визначають пріоритетність ризиків і перевіряють контроль, а не покладаються на переліки сертифікатів. Гнучка та дистанційна робота також стала базовою вимогою в галузі, де інциденти не прив'язані до місця розташування; організації, які наполягають на роботі виключно в офісі, звужують свій кадровий резерв і без необхідності уповільнюють процес найму… Водночас компанії потребують фахівців, які володіють такими сферами, як хмарна безпека, реагування на інциденти, безпека додатків або управління, що відображає довгострокове зростання кількості вакансій — кількість вакансій у сфері кібербезпеки у світі зросла з приблизно 1 мільйона у 2013 році до 3,5 мільйона у 2021 році і залишається на рівні близько 3,5 мільйона до 2023 року, включаючи понад 750 000 у США. У міру зростання конкуренції процеси найму стають коротшими та більш цілеспрямованими, з меншою кількістю раундів співбесід та чіткішими описами посад, що визначають відповідальність, контекст роботи в команді та початкові очікування. Основний посил полягає в тому, що кожна незайнята посада збільшує ризик для організації, а найм покращується, коли вимоги є реалістичними, терміни є жорсткими, обсяг посадових обов'язків є конкретним, а гнучкість вважається стандартом». ***(How Employers Are Rethinking Cybersecurity Jobs Recruitment // Cyber Management Alliance (https://www.cm-alliance.com/cybersecurity-blog/how-employers-are-rethinking-cybersecurity-jobs-recruitment). 12.01.2026).***

***

«Перше комплексне дослідження Absolute Security щодо кіберстійкості підприємств, в якому взяли участь 750 глобальних керівників служб інформаційної безпеки (CISO) у США та Великобританії, показало, що

організації небезпечно не готові до серйозних кіберінцидентів і зазнають значних простоїв та фінансових втрат у разі атак. Більшість організацій (57%) повідомили, що повне усунення наслідків і відновлення після кібератаки, зараження програмним забезпеченням-вимагачем або порушення безпеки даних зайняло в середньому більше 4,5 днів, а 19% зазнали перебоїв у роботі, які тривали до двох тижнів. Важливо, що жодна організація не змогла відновити свою діяльність протягом одного дня. Фінансові витрати на відновлення є значними і становлять в середньому 2,5 мільйона доларів за інцидент, а 98% організацій витратили від 1 до 5 мільйонів доларів на відновлення — ці цифри не враховують загальні бізнес-втрати, понесені під час тривалого простою…

Таке середовище кардинально змінило роль керівника служби інформаційної безпеки (CISO). 72% CISO зараз повідомляють, що їхні повноваження розширилися і тепер не обмежуються лише управлінням безпекою та ризиками, а включають активне керівництво діяльністю організації з забезпечення безперебійної роботи та відновлення після будь-яких інцидентів, що порушують нормальний хід роботи. На додаток до цього, 61% CISO стикаються з нереалістичними очікуваннями від ради директорів та вищого керівництва щодо гарантування повної відсутності порушень, а 59% стурбовані тим, що значні простої можуть призвести до втрати роботи, особистої відповідальності або юридичних санкцій…

Незважаючи на ескалацію загрози, пріоритетність кіберстійкості для CISO небезпечно знижується: хоча 68% респондентів заявляють, що мають стратегію кіберстійкості, цей показник різко знизився порівняно з аналогічним опитуванням, проведеним менше року тому, коли 90% респондентів повідомили про наявність такої стратегії. Тим не менш, 67% керівників служб інформаційної безпеки зараз заявляють про свою основну відповідальність за забезпечення кіберстійкості, а 65% надають їй пріоритет над традиційними методами запобігання, виявлення та реагування...» ***(Cyber Incidents and Attacks Disrupt Enterprise Business Operations for Two Weeks, Reveals First Comprehensive Global Cyber Resilience Survey // yahoo! finance (https://finance.yahoo.com/news/cyber-incidents-attacks-disrupt-enterprise-131500647.html). 08.01.2026).***

***

«У секторі фінансових послуг, де довіра є основою кожної транзакції та відносин, кібербезпека стала прямим фактором, що впливає на довіру інвесторів та вартість активів. Останні дослідження підкреслюють серйозність цього зв'язку: 88% фінансових керівників і 94% фінансових директорів визнають, що успішна кібератака спричинить відтік клієнтів, занепокоєння інвесторів або пряму втрату активів під управлінням. 93% компаній зазнали принаймні одного інциденту протягом останнього року, а такі поширені загрози, як програми-вимагачі та компрометація хмарних сервісів, спрямовані на дані, системи та ланцюги постачання, ставлять галузь під загрозу. Однак критичною слабкістю є видимість: 57% компаній не мають системи моніторингу загроз у режимі реального часу, а більше третини потребують тижня або більше, щоб виявити та локалізувати порушення. Така затримка є дорогою, оскільки середня вартість порушення безпеки даних у фінансовій галузі становить 5,56 млн доларів — на 26% вище за

середній світовий показник — що підриває довіру, відновлення якої займає набагато більше часу, ніж відновлення систем…

Загрозу посилює залежність від застарілої інфраструктури: половина компаній називає локальні системи перешкодою для відновлення, 28% не мають актуальних резервних копій, а 24% не мають підготовки з реагування на інциденти. Дані показують різкий розрив між компаніями, які покладаються виключно на внутрішні IT-ресурси, та тими, які співпрацюють з постачальниками керованих послуг безпеки (MSSP). Внутрішні команди на 56% частіше стикаються з частими атаками і набагато менш впевнені у виявленні загроз, пов'язаних з штучним інтелектом (лише 10% проти 30% для компаній, що співпрацюють з MSSP), а також витрачають більше часу на усунення порушень. Оскільки 78% компаній збільшують витрати на модернізацію інфраструктури та поліпшення виявлення, повідомлення є чітким: кіберризик тепер є бізнес-ризиком. Щоб зберегти впевненість, яка забезпечує рух капіталу, фінансові установи повинні перейти від реактивної оборони до операційної стійкості, скоротивши розрив між відповідністю вимогам та реальними можливостями…» ***(Warren Finkel. Cyber Risk Is Investor Risk For The Financial Sector // Cyber Defense Media Group (https://www.cyberdefensemagazine.com/cyber-risk-is-investor-risk-for-the-financial-sector/). 10.01.2026).***

***

«Кіберризики стали однією з головних проблем бізнесу, особливо з огляду на зростання вразливості ланцюгів постачання: за даними, у 2024 році 75% ланцюгів постачання програмного забезпечення зазнали атак, а прогнозовані глобальні збитки до 2031 року зростуть до 138 мільярдів доларів. У міру того, як загрози стають все більш витонченими, юридичні команди відіграють все більш важливу роль у забезпеченні стійкості організацій, формуючи контракти на закупівлю та постачання, які виходять за рамки загальних формулювань на кшталт «дотримуватися політики безпеки» і замість цього передбачають управління, прозорість, зобов'язання щодо реагування на інциденти та конкретні технічні заходи контролю…

Ефективна кіберстійкість починається ще до підписання договору, коли юридичні команди спільно з технічними та бізнес-зацікавленими сторонами визначають застосовні закони та рамки, розуміють, як послуги постачальника пов'язані з більш широкими системами (що часто є більшим фактором ризику, ніж «критичність»), оцінюють прозорість постачальника щодо його власних залежностей на нижчих рівнях, уточнюють спільну відповідальність на різних технологічних рівнях (особливо в хмарних середовищах) та визначають схильність організації до ризику. Таке раннє залучення запобігає необхідності модернізації та забезпечує більш узгоджене управління ризиками…

Умови контракту повинні бути зосереджені на практичних механізмах, що забезпечують постійну підзвітність, зокрема: права на аудит та інформацію, а також зобов'язання щодо виправлення недоліків; контроль субпідрядників та повне відображення ланцюга поставок із зазначенням основних обов'язків субпідрядників; офіційні процедури управління та звітності з зазначенням

контактних осіб; чіткі обов'язки щодо захисту від вірусів та реагування на тривожні сигнали, пов'язані з кодексами практики, а не з розмитими «найкращими практиками галузі»; вимоги щодо своєчасного встановлення виправлень та оновлень програмного забезпечення, а також заборона використання програмного забезпечення, що не підтримується; терміни реагування на інциденти та звітування, що також охоплюють «небезпечні ситуації»; суворі принципи контролю доступу, такі як мінімальні привілеї та розподіл обов'язків; чітке посилання на визнані рамки (наприклад, ISO 27001, Cyber Essentials/Plus, NIST, Cyber Assessment Framework) та відображення між рамками, де сторони мають розбіжності; та стандарти перевірки та навчання персоналу (наприклад, BPSS для багатьох урядових контрактів) поряд з усвідомленням ризиків, пов'язаних з наймом внутрішніх співробітників. Загалом, добре сформульовані кібер-клаузули допомагають ставитися до постачальників як до стратегічних партнерів у сфері оборони, узгоджуючи зобов'язання з рівнем ризику активів і постачальників, охоплюючи весь життєвий цикл від залучення до моніторингу та звільнення, а також чітко розділяючи юридичне управління та оперативну відповідальність». ***(Jocelyn S Paulley. How to strengthen cyber resilience through supply chain contracts // techUK (https://www.techuk.org/resource/how-to-strengthen-cyber-resilience-through-supply-chain-contracts.html). 14.01.2026).***

***

«Квантові обчислення швидко розвиваються: чіп Willow від Google демонструє швидкість моделювання, яка в 13 000 разів перевищує швидкість найкращих суперкомп'ютерів, а Китай інвестує в цю галузь 15 мільярдів доларів. Хоча універсальні квантові комп'ютери ще не доступні, NIST попереджає, що до 2030 року можуть з'явитися системи, здатні зламати сучасне шифрування…

Квантові обчислення швидко розвиваються: чіп Willow від Google демонструє швидкість моделювання, яка в 13 000 разів перевищує швидкість найкращих суперкомп'ютерів, а Китай інвестує в цю галузь 15 мільярдів доларів. Хоча універсальні квантові комп'ютери ще не доступні, NIST попереджає, що до 2030 року можуть з'явитися системи, здатні зламати сучасне шифрування.

Постквантова готовність означає захист усіх шифрувань від квантових загроз, що вимагає оновлення всієї інфраструктури відкритих ключів (браузерів, серверів, мережевих пристроїв). Підхід, заснований на ризиках, надає пріоритет конфіденційним даним, передбачаючи триетапний план: інвентаризація криптографічних систем, уможливлення заміни алгоритмів та оновлення до квантово-стійких стандартів. NIST рекомендує відмовитися від RSA/ECDSA до 2030 року та заборонити їх до 2035 року, що є графіком, прийнятим США, Австралією та іншими країнами…

Cloudflare прискорює підготовку, модернізуючи інфраструктуру до TLS1.3 (використовуючи квантово-безпечні алгоритми, такі як ML-KEM), пропонуючи безкоштовні квантово-безпечні сертифікати TLS та інтегруючи PQC у послуги Zero Trust. Повна стійкість вимагає, щоб весь ланцюжок з'єднання (від браузера до сервера) був готовий до квантових технологій; розміщення чутливої інфраструктури за мережею Cloudflare знижує ризики для критично важливих активів, звільняючи ресурси для інших загроз. Готовність до постквантових

технологій повинна відповідати стратегіям Zero Trust і глибокої оборони». ***(Bill Tanner. Preparing for the post-quantum era of cybersecurity // A Intelligent Global Media Brand (https://www.intelligentciso.com/2026/01/22/preparing-for-the-post-quantum-era-of-cybersecurity/). 22.01.2026).***

***

«Ми перебуваємо в епіцентрі інтенсивної глобальної промислової революції, спричиненої конвергенцією штучного інтелекту та квантових обчислень — технологій, які вже не є теоретичними, а активно переформатовують управління ризиками, кібербезпеку та економічну конкурентоспроможність. Головним викликом є те, що технологічний прогрес випереджає інституційну адаптацію, розробку політик та підготовку робочої сили. Кібербезпека ніколи не була частиною початкового задуму цифрового світу, а зараз штучний інтелект знизив бар'єр для вторгнення супротивників, розширивши площу атаки, тоді як квантові обчислення загрожують підірвати криптографічні основи уряду та фінансів за допомогою стратегій «збирай зараз, розшифровуй пізніше», які вже застосовуються національними державами…

Квантові обчислення є двосічним мечем: хоча «Q-Day» — поява систем, достатньо потужних, щоб зламати шифрування RSA — становить існувальну загрозу, ця технологія також обіцяє прориви в області сенсорики, оптимізації та безпечних комунікацій. Організації повинні розглядати квантову готовність як постійне поширення можливостей, а не як окрему подію, оскільки очікування повної зрілості призведе до стратегічної нерівності. Одночасно штучний інтелект став технологією подвійного призначення, що діє як мультиплікатор сили як для зловмисників, які використовують його для автоматизованого фішингу та створення фейкових відео, так і для захисників, які використовують його для аналізу загроз та автоматизованого виправлення. Ключовим чинником, що відрізняє стійкість від катастрофи, буде управління та людський нагляд, особливо з огляду на те, що «агентні» системи штучного інтелекту, які працюють автономно, впроваджуються швидше, ніж розуміються їхні наслідки. З огляду на 2030 рік, космічна інфраструктура стає критично важливою, але недостатньо керованою кіберціллю…

Це нове рівняння ризику — загроза × вразливість × наслідок — кардинально змінило роль директора з інформаційної безпеки (CISO), який перетворився з технічного спеціаліста на керівника вищої ланки, відповідального за цінність підприємства, але часто не має відповідних повноважень щодо бюджету. Рішення полягає не просто в придбанні додаткових технологій, а в удосконаленні управління ризиками та узгодженні безпеки з бізнес-стратегією. Зрештою, успіх залежить від культури, а не тільки від технологій; без злагодженої стратегії та обґрунтованого управління інновації випереджають відповідальність. Оскільки ми вже живемо в цьому майбутньому, термінові інвестиції в квантово-стійку криптографію, системи управління штучним інтелектом та підвищення кваліфікації персоналу більше не є опціональними, а є необхідними». ***(Chuck Brooks. How AI and Quantum, And Space Are Redefining Cybersecurity // Forbes Media LLC***

(https://www.forbes.com/sites/chuckbrooks/2026/01/19/how-ai-and-quantum-and-space-are-redefining-cybersecurity/). 19.01.2026).

***

«Малі та середні підприємства (МСП) і стартапи стають все більш вразливими до кіберзагроз, але часто не мають бюджету, IT-експертизи та лідерства для впровадження надійних стратегій безпеки. Ця вразливість є критичною, оскільки одне порушення, яке в середньому коштує щонайменше 120 000 доларів, може стати фатальним для невеликої компанії. На відміну від великих підприємств, які можуть відновитися, МСП часто стикаються з банкрутством через фінансові, репутаційні та операційні збитки…

Штучний інтелект (ШІ) змінив ландшафт загроз, знизивши бар'єр для вторгнення зловмисників. Зараз зловмисники використовують методики рівня підприємств, застосовуючи ШІ для здійснення складних фішингових атак з урахуванням контексту, автоматизації вторгнень та експлуатації вразливостей у великих масштабах. Найпоширенішими загрозами є атаки на основі ідентифікації, під час яких злочинці входять у систему за допомогою викрадених облікових даних, та програми-вимагачі, які швидко поширюються, оскільки малі та середні підприємства не мають інструментів для їх раннього виявлення. Інші небезпеки включають DDoS-атаки, перехоплення типу «людина посередині», завантаження «на ходу» та вразливості програмного забезпечення.

Експерти радять малим і середнім підприємствам відмовитися від складних контрольних списків на користь «мінімально необхідної конфігурації кібербезпеки», орієнтованої на вплив. Стратегія повинна починатися із забезпечення безпеки браузера — основного пункту взаємодії в сучасній роботі — а потім переходити до захисту ідентичності, оскільки більшість порушень починаються з компрометації облікових даних. Підприємства також повинні отримати можливість контролювати свої пристрої, додатки та потік даних, оскільки неможливо захистити те, чого не бачиш…

Кібербезпеку слід розглядати як страхування бізнесу: інвестицію, яка захищає здатність до функціонування. Замість того, щоб нав'язувати невеликим командам складні корпоративні стеки, галузь починає пропонувати доступні рішення на основі штучного інтелекту. Мета полягає в тому, щоб зупинити порушення безпеки якомога ближче до користувача, захистивши «вхідні двері» (ідентичність), кінцеві точки (пристрої) та точки доступу до хмари, забезпечуючи малим і середнім підприємствам можливість вижити в цифровому середовищі, де зловмисники націлюються на найслабші місця захисту…» ***(Jordan Scott. What's the Minimum Viable Cybersecurity Setup for an SMB With Limited Cash Flow? // CDW LLC (https://biztechmagazine.com/article/2026/01/whats-minimum-viable-cybersecurity-setup-smb-limited-cash-flow). 20.01.2026).***

***

«У 2025 році кібербезпека зазнала значних потрясінь, що супроводжувалися гучними порушеннями, популяризацією безпеки космічних систем та зростанням геополітичної напруженості. Цей рік ознаменувався

подією CyberSat у листопаді, на яку, незважаючи на закриття уряду США в останній момент, прийшли сотні людей. Визначальним моментом став запуск NRO спеціальної космічної кіберпрограми, яка з першого дня інтегрувала кібербезпеку в космічні системи та оптимізувала процес прийняття рішень. Тим часом конфлікт між Україною та Росією продовжував демонструвати кібервійну, а Україна підтвердила кібератаку 2023 року на російську компанію «Дозор-Телепорт» під час перевороту Вагнера, розкривши важливі деталі про кібероперації проти супутникових мереж…

Вразливість супутникової інфраструктури була яскраво продемонстрована дослідниками з UCSD та UMD, які використовували приймач вартістю 800 доларів для перехоплення незашифрованих повідомлень від супутників GSO, що викликало занепокоєння в галузі. Великі атаки на корпорації також викликали резонанс: Jaguar Land Rover зазнав фінансових збитків у розмірі 1,9 млрд фунтів стерлінгів від кібератаки, найбільшої в історії Великобританії, що підкреслило вразливість ланцюга поставок. Аналогічно, SK Telecom зіткнулася з масовим порушенням безпеки, яке торкнулося 27 мільйонів клієнтів, що спонукало компанію інвестувати 475 млн доларів у модернізацію систем безпеки. Роль штучного інтелекту в кібератаках різко зросла, перейшовши від розвідки до оперативних наступальних кампаній, причому шкідливе програмне забезпечення, таке як Promptlock, динамічно уникає виявлення…

У геополітичному плані Китай посилив свою кібератаку на Тайвань, здійснюючи понад 2,6 мільйона спроб вторгнення щодня, а північнокорейські IT-фахівці проникли в глобальні технологічні компанії, стираючи межі між внутрішніми загрозами та шпигунством. Ера космічної співпраці фактично закінчилася, а постійне залучення та інспекції на орбіті свідчать про те, що космос є спірною сферою. Нестабільність інфраструктури ще більше підкреслила серйозна аварія Cloudflare, спричинена помилками в конфігурації, та широкомасштабне вторгнення в ланцюг поставок, спрямована проти Salesforce через скомпрометовані інтеграції Salesloft Drift, що зачепило понад 700 організацій. Ці події в сукупності підкреслили, що 2025 рік став поворотним моментом, коли кіберзагрози стали більш витонченими, поширеними та невід'ємною частиною як виживання корпорацій, так і національної оборони». ***(Mark Holmes. 10 Defining Moments in Cybersecurity and Space in 2025 // Via Satellite (https://interactive.satellitetoday.com/via/january-february-2026/10-defining-moments-in-space-and-cybersecurity-in-2025). 20.01.2026).***

***

«Недавній звіт Vodafone Business малює жахливу картину кіберстійкості корпорацій, показуючи, що понад 10% компаній вважають, що не виживуть після серйозної кібератаки. Цей екзистенційний ризик зумовлений тривожною непідготовленістю: понад 70% керівників підприємств побоюються, що їхні співробітники вразливі до фішингу. Хоча гучні атаки на такі бренди, як Jaguar Land Rover і Marks & Spencer, підвищили обізнаність — що спонукало 45% організацій запровадити базове навчання з питань безпеки — загальна ситуація з ризиками погіршується. Вражаючі 63% респондентів відчувають себе більш вразливими, ніж

рік тому, в основному через погану гігієну паролів; співробітники повторно використовують облікові дані в середньому в 11 особистих облікових записах, створюючи легкі точки входу для зловмисників. Ситуацію ускладнює розвиток штучного інтелекту та технології deepfake, що підсилює побоювання щодо складних атак соціального інжинірингу, коли злочинці видають себе за керівників, щоб авторизувати шахрайські платежі, змушуючи організації терміново посилювати як технічні засоби захисту, так і обізнаність персоналу…» ***(Naveen Goud. Over 10% of UK businesses unlikely to survive a Cyber Attack // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/over-10-of-uk-businesses-unlikely-to-survive-a-cyber-attack/). 21.01.2026).***

***

«Згідно з доповіддю KPMG Global Tech Report 2026, в якій було опитано лідерів технологічної галузі з усього світу, включаючи 151 компанію з Великої Британії, кібербезпека стала головним пріоритетом для значного збільшення бюджетів протягом наступних 12 місяців. Більше половини британських організацій (57%) планують збільшити витрати на кібербезпеку на понад 10%, порівняно з 41% у всьому світі, що підкреслює особливо сильний акцент на кіберстійкості у Великобританії. Значні інвестиції також плануються в штучний інтелект, дані та аналітику: 46% і 48% респондентів відповідно очікують двозначного збільшення бюджету в цих сферах. Загалом, штучний інтелект залишається найбільш фінансуваною сферою: 84% компаній планують збільшити інвестиції в штучний інтелект, за ним слідують кібербезпека (83%) та дані й аналітика (82%). Примітно, що 91% респондентів вважають, що до кінця 2026 року штучний інтелект перетвориться з інструменту підвищення ефективності на інновацію, що приносить дохід, що свідчить про перехід від експериментів до вимірюваної бізнес-цінності…

Однак багато організацій стикаються з труднощами у масштабуванні цих технологій. У Великобританії лише 3% лідерів у сфері технологій вважають, що штучний інтелект сьогодні повністю масштабований (прогнозується зростання до 51% протягом року), і лише 13% вважають те саме щодо кібербезпеки (очікується зростання до 54%). Майже половина респондентів повідомляють про перешкоди у масштабуванні як ШІ (47%), так і кібербезпеки (45%), незважаючи на наявність фінансування та стратегічної підтримки. Пол Хеннінгер з KPMG зазначає, що масштабування — це не «більші пілотні проекти», а створення повторюваних платформ, міцних основ для даних та операційних моделей, що інтегрують IT, безпеку та бізнес. Водночас 89% британських організацій вже інвестують в агентний ШІ для підтримки гібридної людсько-цифрової робочої сили, 92% очікують, що управління агентами ШІ стане ключовою навичкою протягом п'яти років, а 90% планують наймати фахівців, таких як інженери-програмісти, етики ШІ та експерти MLOps. 93% опитаних погоджуються, що IT-команди, команди з безпеки та ризиків співпрацюють для безпечного розгортання та моніторингу систем ШІ, а управління та таланти вважаються критичними факторами диференціації. Хеннінгер стверджує, що успіх залежатиме від вбудовування безпеки в хмару та ШІ з першого дня, встановлення чітких обмежень — контролю

ідентичності та доступу, аудиторських слідів, людського нагляду, постійного моніторингу — та ставлення до кібербезпеки не як до центру витрат, а як до чинника зростання та операційної стійкості…» ***(Cybersecurity emerges as a top spending priority for UK organisations' tech strategies in 2026 while AI still dominates // KPMG LLP (https://kpmg.com/uk/en/media/press-releases/2026/01/cybersecurity-emerges-as-a-top-spending-priority.html). 22.01.2026).***

***

«З початком 2026 року глобальна кібербезпека вступила у фазу гіперприскорення, а витрати кінцевих користувачів на інформаційну безпеку, за прогнозами, досягнуть 240 мільярдів доларів — це на 12,5% більше, ніж у 2025 році (213 мільярдів доларів) — що свідчить про рішучий перехід від IT-витрат до стратегічного пріоритету на рівні правління. Головним рушієм є подвійне використання ШІ: захисники покладаються на нього для автоматизованого пошуку загроз і швидшого виявлення, тоді як супротивники використовують «агентний» ШІ як зброю для запуску автономних атак зі швидкістю машини, від шахрайства на основі фейкових відео до автоматизованого введення коду. До 2027 року, за оцінками, 17% всіх кібератак будуть пов'язані зі штучним інтелектом, що змусить організації інвестувати в стійкість до штучного інтелекту: захист неструктурованих даних, які живлять корпоративні моделі штучного інтелекту, та впровадження інструментів, які можуть виявляти аномалії в поведінці та трафіку, спричинені штучним інтелектом…

Витрати зосереджуються в трьох сферах: 121,1 млрд доларів на програмне забезпечення для безпеки (зростання на 14,2%, зосередження на хмарних та API-екосистемах), 92,8 млрд доларів на послуги з безпеки (через брак кваліфікованих кадрів та зростання аутсорсингу MDR/SOC) та 25,9 млрд доларів на мережеву безпеку, з особливим акцентом на архітектурах Zero Trust. У регіональному розрізі лідирує Північна Америка, що зумовлено трансформацією фінансового сектору та суворими правилами HIPAA/SEC; Європа надає пріоритет дотриманню вимог та прозорості штучного інтелекту відповідно до GDPR та Закону ЄС про штучний інтелект; а ринки, що розвиваються в регіоні Близького Сходу та Північної Африки та Південно-Східної Азії, стрімко переходять на моделі безпеки, орієнтовані на хмарні технології. На керівників служб інформаційної безпеки чиниться все більший тиск з метою продемонструвати вимірюваний ROI за допомогою «оцінок стійкості», просуваючи такі цілі, як середній час виявлення менше однієї години, різке скорочення середнього часу реагування та рівень помилкових спрацьовувань нижче 5%, щоб дефіцитні кадри могли зосередитися на реальних загрозах. 63% компаній інвестують значні кошти у внутрішнє навчання, тому людський брандмауер модернізується разом з інструментами. У перспективі автоматизація та проактивне виявлення загроз, коли агенти штучного інтелекту постійно сканують, виправляють та тестують системи на стійкість, стають єдиним життєздатним шляхом до захисту. У глобальній економіці, що базується на даних, ці витрати у розмірі 240 мільярдів доларів є не стільки витратами, скільки страховим полісом та конкурентною перевагою, що робить кібербезпеку основою цифрової довіри…» ***(MANOJ MILANI. The $240 Billion Shield: Navigating the Global Cybersecurity***

Surge of 2026 // IoT For All (https://www.iotforall.com/iot-ai-cybersecurity-2026). 22.01.2026).

***

«У 2025 році McDonald's надав яскравий приклад того, наскільки ресторанні мережі вразливі до кіберризиків з боку третіх осіб, коли хакери-«білі капелюхи» легко зламали систему чат-бота McHire, Olivia, виявивши базові недоліки, такі як стандартний пароль адміністратора «123456», залишений постачальником Paradox.ai. McHire використовується більшістю франчайзингових ресторанів McDonald's, що означає, що особисті дані близько 64 мільйонів претендентів на роботу потенційно були розкриті. Незабаром після цього інша команда етичних хакерів виявила «катастрофічні» вразливості, включаючи жорстко закодовані паролі, в системах Restaurant Brands International, які використовуються Burger King і Popeyes. Що робить ці інциденти такими тривожними, це не тільки їх масштаб, але й те, наскільки тривіальними були ці слабкі місця, які можна було виявити під час рутинного тестування, що дає підстави припустити, що зловмисники вже знайшли і використали подібні прогалини в усьому секторі. В середньому, порушення безпеки в ресторанах залишаються невиявленими протягом 212 днів, що дає злочинцям достатньо часу для викачування даних платіжних карток з тисяч транзакцій, перш ніж оператори зрозуміють, що щось не так…

Ці проблеми посилюються, оскільки технології стають центральним елементом діяльності ресторанів: 99% ресторанів зараз використовують принаймні одну платформу для онлайн-замовлень, а більшість програмного забезпечення інтегровано в точки продажу (POS), тоді як кількість порушень, пов'язаних із третіми сторонами, подвоїлася і становить 30% від усіх інцидентів. Тому управління кіберризиками стало критично важливим, і ресторани повинні ретельно перевіряти безпеку постачальників так само, як і свою власну. Відповідальність за перевірку системних постачальників несе франчайзер, але франчайзі все одно повинні дотримуватися корпоративних стандартів безпеки та ретельно перевіряти всіх місцевих постачальників, яких вони залучають. Це означає перевірку політики безпеки даних та конфіденційності постачальників, планів реагування на інциденти та відновлення, програм навчання персоналу, технічних засобів контролю та заходів щодо дотримання вимог, а також доказів проведення постійних оцінок ризиків та протоколів звітності. У контрактах повинні бути чітко прописані умови відшкодування збитків; співпраця з брокером, який має досвід у сфері кіберризиків та франчайзингу, є надзвичайно цінною…

Страхування ще більше ускладнює ситуацію в умовах франчайзингу. Франчайзі, незалежно від того, чи володіють вони двома або 200 точками продажу, стикаються з однаковими ризиками, але часто просто виконують мінімальні вимоги франчайзера, не оцінюючи реальний ризик, як показує випадок, коли кіберзбитки на суму 3,7 млн доларів призвели до виплати лише 400 000 доларів. Франчайзі повинні зважити, чи приєднатися до загальної кіберполітики франчайзера, розділивши сукупний ліміт (наприклад, 5 мільйонів доларів на сотні магазинів) за нижчою вартістю, чи забезпечити додаткове спеціальне покриття, щоб гарантувати

повне відшкодування власних збитків. Кожен новий магазин і кожна нова інтеграція системи розширюють площу атаки, і оператори все частіше визнають, що кіберінцидент — це питання часу, а не ймовірності. У цьому контексті кібербезпека, включаючи комплексну перевірку постачальників, індивідуальне страхування та послуги експертів-брокерів, більше не є питанням внутрішньої адміністрації, а питанням виживання: одна слабка ланка в системі третьої сторони може поставити під загрозу весь франчайзинговий бізнес…» ***(Patrick Ryder. How Restaurants, Especially Franchises, Should Look at Cyber Security // WTWH Media, LLC. (https://www.qsrmagazine.com/story/how-restaurants-especially-franchises-should-look-at-cyber-security/). 21.01.2026).***

***

Сполучені Штати Америки, Канада та країни Латинської та Південної Америки

«Закон про національну оборону 2026 року (NDAA) сигналізує про зміну для компаній, що продають штучний інтелект американським оборонним та розвідувальним агентствам, встановлюючи суворі вимоги до ланцюгів постачання та безпеки, подібні до чисток «закритих» технологій, що спостерігалися протягом останнього десятиліття. Це створює як ризик недотримання вимог, зокрема щодо виконання Закону про неправдиві заяви (FCA), так і конкурентну можливість для компаній, які адаптують свої продукти до цих стандартів…

NDAA створює ключові органи управління, такі як «Керівний комітет з питань майбутнього штучного інтелекту» та «Міжфункціональна команда», які будуть керувати стратегією та політикою, включаючи розробку стандартів ефективності та безпеки штучного інтелекту. Важливо, що закон вводить широкі обмеження ланцюга поставок, забороняючи використання «охопленого ШІ» в оборонних контрактах, зокрема, спрямованих на ШІ, розроблений DeepSeek, High Flyer або організаціями, пов'язаними з «охопленими країнами», такими як Китай, Росія, Північна Корея та Іран. Ця заборона поширюється на «наступний ШІ» та ШІ, «підтримуваний» High Flyer, що вимагає ретельної перевірки та сертифікації від підрядників…

Крім того, Конгрес доручає розробити систему кібербезпеки та фізичної безпеки для технологій ШІ, чітко вказуючи, що вона має бути впроваджена як розширення існуючої програми сертифікації зрілості кібербезпеки (CMMC). Ця система повинна враховувати такі ризики, як вразливість ланцюгів постачання (наприклад, отруєння даних), ворожі втручання, крадіжки та управління станом безпеки. Отже, компанії оборонно-промислової бази повинні очікувати, що CMMC не буде скасована, а навпаки, розширена для охоплення штучного інтелекту, проникаючи глибоко в ланцюг поставок. Ті, хто проактивно пристосовує свої бізнес-моделі до цих майбутніх вимог, будуть у найкращому становищі, щоб скористатися зростаючим попитом на штучний інтелект в оборонному секторі, тоді як ті, хто не дотримається вимог, ризикують бути виключеними з ринку…» ***(Beth***

George, Anna Gressel and Nathan Castellano. AI Supply Chain and Security: Congress Mandates Strict Controls for AI acquired by the U.S. Defense Agencies and Intelligence Community // Freshfields (https://blog.freshfields.us/post/102lzgo/ai-supply-chain-and-security-congress-mandates-strict-controls-for-ai-acquired-b#page=1). 05.01.2026).

***

«Конгрес розглядає кілька законопроектів, спрямованих на зміцнення національної електромережі проти кіберзагроз, приділяючи особливу увагу допомозі комунальним підприємствам з обмеженими ресурсами та сільським комунальним підприємствам. На слуханнях підкомітету з енергетики Комітету з енергетики та торгівлі Палати представників законодавці розглянули пропозиції щодо поновлення програми з підвищення рівня кібербезпеки сільських та муніципальних комунальних підприємств (RMUC) та зобов'язання державних енергетичних відомств включати більш детальну інформацію про вразливість та ланцюги постачання до своїх планів енергетичної безпеки. Агентство оборонної розвідки попередило, що енергосистема є головним об'єктом кібератак з боку національних держав, спрямованих на спричинення масштабних збоїв, а голова підкомітету, конгресмен Боб Латта, наголосив, що зростаюча цифровізація, ресурси нового покоління та взаємопов'язані газові та енергетичні системи розширюють можливості для зловмисних дій. Спочатку фінансуючись у розмірі 250 мільйонів доларів протягом п'яти років відповідно до закону про інфраструктуру 2021 року, RMUC підтримує кооперативи, муніципальні комунальні підприємства та невеликі комунальні підприємства, що належать інвесторам, у зміцненні систем, навчанні персоналу та реагуванні на інциденти. Натаніель Мелбі, директор з інформаційних технологій Dairyland Power Cooperative, свідчив, що RMUC «подолає розрив у ресурсах сільських районів» і допоможе забезпечити, щоб кібербезпека в сільській Америці відповідала рівню більш забезпечених ресурсами регіонів, але розкритикував Міністерство енергетики за те, що воно ще не виділило приблизно 80 мільйонів доларів грантів, оголошених восени минулого року для понад 400 кооперативів. Він закликав до швидшого впровадження, більш гнучкого дизайну програми та розширення критеріїв для отримання грантів і технічної допомоги, стверджуючи, що потенціал програми є «безперечним»…

Представники адміністрації висловили готовність тісніше співпрацювати з штатами та місцевими органами влади. Алекс Фіцсіммонс, виконуючий обов'язки заступника міністра енергетики та керівник Управління кібербезпеки, енергетичної безпеки та реагування на надзвичайні ситуації Міністерства енергетики США, заявив, що складні атаки на сільські комунальні підприємства підкреслюють необхідність прискорення підготовки до кіберзагроз та усунення розриву в ресурсах сільських районів. Інший законопроект, Закон про Центр аналізу енергетичних загроз, передбачає поновлення повноважень та посилення Центру аналізу енергетичних загроз (ETAC) Міністерства енергетики, який є центром обміну інформацією відомства. Скотт Ааронсон з Інституту Едісона заявив, що ETAC «неодноразово доводив свою цінність», і закликав до додаткових правових гарантій, щоб забезпечити відверте обговорення надзвичайно чутливих питань

безпеки та експлуатації. Свідки, серед яких Адрієнн Лотто з Американської асоціації громадських енергетичних компаній, також підтримали вимоги до штатів щодо вирішення питань безпеки ланцюгів постачання та загроз для місцевих розподільчих систем у своїх енергетичних планах, наголосивши, що тісна координація між федеральними, штатними, місцевими, племінними, територіальними та галузевими партнерами є надзвичайно важливою для запобігання та готовності до надзвичайних ситуацій. Фіцсіммонс заявив, що адміністрація прагне надати урядам нижчого рівня більш активну роль у забезпеченні стійкості енергомереж, щоб вони могли краще оцінювати та реагувати на кібернетичні, фізичні та пов'язані з погодою ризики. Очікується, що голосування щодо пакету законів про безпеку енергомереж відбудеться найближчим часом». ***(Chris Teale. House explores grid cybersecurity boosts amid growing threats // route fifty (https://www.route-fifty.com/cybersecurity/2026/01/house-explores-grid-cybersecurity-boosts-amid-growing-threats/410672/). 14.01.2026).***

***

«З огляду на те, що лише у 2024 році в США сталося майже 3200 випадків порушення безпеки даних, які торкнулися понад 1,3 мільярда людей, надійний план реагування на інциденти кібербезпеки (CSIRP) вже не є опцією, а необхідністю для бізнесу. CSIRP надає структурований посібник для IT- та безпекових команд з управління інцидентами безпеки, такими як порушення безпеки даних, програмне забезпечення-вимагач та витік даних, мінімізуючи збитки та забезпечуючи швидке відновлення. Окрім того, що CSIRP є найкращою практикою, його наявність часто є нормативною вимогою згідно з такими законами, як CCPA та GDPR, а також необхідною умовою для отримання сертифікатів, таких як ISO 27001. Чітко визначений план допомагає організаціям уникнути дорогих помилок, скоротити час простою та зберегти довіру клієнтів і зацікавлених сторін…

Національний інститут стандартів і технологій (NIST) окреслює комплексну шестиетапну структуру реагування на інциденти:

Управління: Встановити та донести політику управління ризиками, визначити стратегічний напрямок кібербезпеки та забезпечити підзвітність у всій організації.

Ідентифікація: Скласти каталог критично важливих систем і даних, оцінити загрози та вразливі місця, а також визначити пріоритетність ризиків для інформування про заходи реагування.

Захист: Впровадити засоби контролю безпеки, такі як управління ідентифікацією та доступом, шифрування та сегментація мережі, щоб зменшити частоту та вплив інцидентів…

Виявлення: постійно моніторьте системи за допомогою таких інструментів, як SIEM та SOAR, щоб якомога раніше виявляти аномалії та ознаки компрометації.

Реагування: вживайте негайних, скоординованих заходів для стримування та усунення загроз, одночасно керуючи внутрішніми та зовнішніми комунікаціями відповідно до заздалегідь визначених протоколів.

Відновлення: відновлення уражених систем із чистих резервних копій, виправлення вразливостей та впровадження отриманого досвіду для підвищення стійкості в майбутньому…

CSIRP слід переглядати щонайменше раз на рік та оновлювати відповідно до нових технологій, загроз або змін у законодавстві. Практичний перелік заходів для створення CSIRP включає проведення оцінки ризиків, визначення ключових членів команди, визначення типів інцидентів, інвентаризацію активів, окреслення інформаційних потоків, підготовку публічних заяв та ведення детального журналу подій. Застосовуючи проактивний та структурований підхід до реагування на інциденти, організації можуть не тільки виконати вимоги щодо дотримання нормативних вимог, але й створити більш стійке та надійне цифрове середовище». ***(Matt Kelly. How to Create a Cybersecurity Incident Response Plan That Works // Hyperproof (https://hyperproof.io/resource/cybersecurity-incident-response-plan/). 14.01.2026).***

***

«Комітет Палати представників США з питань внутрішньої безпеки нещодавно провів наглядове слухання, щоб розглянути, як Міністерство внутрішньої безпеки, а саме CISA, TSA та Управління науки і технологій, реагує на дедалі складнішу ситуацію з загрозами, з якими стикаються цивільні та урядові мережі, транспортні системи та критична інфраструктура. Свідки, серед яких був і виконуючий обов'язки директора CISA Мадху Готтумуккала, наголосили на зростаючій витонченості супротивників, впливі нових технологій, таких як штучний інтелект, та викликах, пов'язаних із закінченням повноважень федеральних органів влади та неефективністю бюрократичної системи…

Голова Ендрю Гарбаріно підкреслив, що кібербезпека зараз є центральним елементом національної безпеки, оскільки супротивники націлюються на транспорт і критичну інфраструктуру за допомогою цифрових засобів і нових загроз, таких як атаки на основі штучного інтелекту та порушення роботи дронів. Місія CISA стала більш важливою, оскільки супротивники протягом тривалого часу діють всередині мереж США, що робить безперебійність роботи персоналу та готовність до виконання місій надзвичайно важливими…

Слухання ознаменувало зміну пріоритетів федерального уряду: CISA зосереджується на захисті трубопроводів, фінансових систем та інших критично важливих об'єктів, усуненні прогалин у кіберфізичних ризиках та запуску цільових ініціатив для усунення найнагальніших вразливостей. Агентство також адаптується до більш жорстких регуляторних вимог, таких як ті, що передбачені Законом про повідомлення про кіберінциденти та критичну інфраструктуру (CIRCIA), та розширює можливості виявлення та реагування на кінцевих точках.

Підхід CISA тепер більше орієнтований на оперативну діяльність, надаючи пріоритет ефективності, підзвітності та впливу. Агентство посилює захист федеральної мережі, підтримує критичну інфраструктуру та надає ресурси безпеки державним і місцевим органам влади. Воно також поглиблює співпрацю з промисловістю та швидше обмінюється інформацією про загрози…

У перспективі CISA планує продовжувати ребалансування свого персоналу, надаючи пріоритет висококваліфікованим технічним фахівцям та оптимізуючи державні операції, одночасно доопрацьовуючи правила CIRCIA для гармонізації федеральної системи повідомлення про кіберінциденти. Слухання підкреслює, що тиск з боку органів контролю, координація між федеральними органами та промисловістю, а також вимоги до стійкості будуть посилюватися для власників та операторів критичної інфраструктури, оскільки США адаптуються до швидко мінливого середовища кіберзагроз». ***(Anna Ribeiro. House Homeland Security hearing probes escalating cyber, drone, AI threats to US transportation, critical infrastructure // Industrial Cyber (https://industrialcyber.co/critical-infrastructure/house-homeland-security-hearing-probes-escalating-cyber-drone-ai-threats-to-us-transportation-critical-infrastructure/). 23.01.2026).***

***

«Латинська Америка та Карибський басейн намагаються прискорити економічне зростання за допомогою швидкої цифровізації, але прогрес гальмується низьким рівнем довіри до кіберзахисту уряду та гострою нестачею фахівців у галузі кібербезпеки. Згідно з доповіддю Всесвітнього економічного форуму «Глобальний прогноз у галузі кібербезпеки до 2026 року», організації в цьому регіоні мають найнижчий рівень довіри у світі до здатності своїх країн захищати критичну інфраструктуру: лише 13% впевнені в цьому, а 49% — ні, порівняно з 37% впевнених у всьому світі. ВЕФ стверджує, що «кібернерівність» у регіоні зумовлена прогалинами в управлінні, обмеженими фінансовими ресурсами та нерівним доступом до цифрової інфраструктури, але що нестача фахівців з кібербезпеки є найпоширенішим і системним обмежувачем кіберстійкості та ефективного реагування на інциденти…

Ці слабкі місця посилюються різким зростанням кількості атак. Check Point Research повідомляє, що минулого року в Латинській Америці кількість кібератак зросла на 53% порівняно з попереднім роком, що приблизно на 40% перевищує середній світовий показник, а кіберзлочинні угруповання, пов'язані з Південно-Східною Азією та Китаєм, розширили свою діяльність у регіоні. Серед конкретних гарячих точок — Мексика, яка намагається зміцнити інфраструктуру напередодні Чемпіонату світу з футболу 2026 року, Венесуела, яка стикається з посиленою атакою з боку національних держав на тлі військової активності США, та Бразилія, фінансова система якої залишається постійною мішенню для злочинців…

Найбільшим обмеженням у регіоні є потенціал робочої сили: більше двох третин організацій не мають достатньої кількості персоналу та можливостей для підвищення стійкості, і лише 31% вважають, що мають достатню кількість кваліфікованих співробітників. Ця проблема ускладнюється більш загальними проблемами стійкості, такими як перебої в електропостачанні та ненадійне підключення до Інтернету, що може підірвати безперервний моніторинг безпеки та швидке реагування. Штучний інтелект має як перспективи, так і ризики: він може допомогти захисникам масштабувати виявлення та реагування, але також дає злочинцям можливість здійснювати більш переконливі шахрайські дії на рідній мові у великих масштабах. Опитування ВЕФ показує, що кібершахрайство

поширене в усіх регіонах: 77% респондентів у Латинській Америці та Карибському басейні стикалися з шахрайством або знають когось, хто постраждав від нього.

Щоб подолати цю прогалину, ВЕФ вказує на необхідність скоординованих інвестицій та нарощування потенціалу і наголошує на важливості своєї програми «Cybersecurity Talent Framework», яка спрямована на залучення людей до сфери кібербезпеки, розширення можливостей навчання, поліпшення процесу найму та підбору кваліфікованих кадрів, а також утримання фахівців шляхом вирішення таких проблем, як обмежене визнання та високий рівень стресу на роботі. ВЕФ попереджає, що без цілеспрямованих дій швидка цифрова експансія може призвести до системної вразливості, а не до інклюзивного економічного зростання». ***(Robert Lemos. Latin American Orgs Lack Confidence in Cyber Defenses, Skills // TechTarget, Inc. (https://www.darkreading.com/cyber-risk/latin-american-confidence-cyber-defenses-skills). 22.01.2026).***

***

«…Оскільки США під керівництвом президента Трампа взяли на себе зобов'язання «керувати» Венесуелою, традиційні військові засоби примусу виявляються нестійкими, юридично сумнівними та гуманітарними з точки зору високої вартості. …тривала кампанія кібертиску — потенційно навіть атака типу «вимагання викупу» з вимогою 1 мільярда доларів і виконання політичних вимог — може бути більш ефективною, гуманною і доступною альтернативою. Хоча науковці часто відкидають кібероперації як неефективні для примусу через уразливості, які можна виправити, і нечіткі загрози, жахлива кіберзахист Венесуели (107-е місце в світі) робить її особливо вразливою до постійних і недорогих зривів…

Замість того, щоб прагнути до екзистенційних змін, таких як вільні вибори, кіберпримус може бути спрямований на «невеликі» вимоги, такі як повернення 1,8 мільярда доларів боргу за нафту або звільнення політичних в'язнів, що відображає фінансовий успіх злочинного програмного забезпечення для вимагання викупу. Такий підхід перетворює кібероперації з таємного саботажу на відкриту державну політику, де загроза дестабілізації підкріплюється постійною можливістю застосування військової сили — комбінація, яку минулі теорії про кіберпримус проігнорували. Хоча пропагування державного програмного забезпечення для вимагання викупу є незручним, воно подається як менше зло порівняно зі смертельними ударами або вторгненням, пропонуючи оборотний, нелетальний важіль для забезпечення інтересів США…» ***(Jason Healey. The Case for Cyber Pressure Against Venezuela // The Lawfare Institute (https://www.lawfaremedia.org/article/the-case-for-cyber-pressure-against-venezuela). 22.01.2026).***

***

«У міру того як кібератаки стають все більш витонченими і частими, а також з огляду на нещодавні гучні порушення безпеки та сплеск інцидентів під час закриття уряду США в 2025 році, кібербезпека стала одним з головних бізнес-ризиків для організацій. Хоча технічна підготовленість має вирішальне

значення, багато компаній нехтують важливою роллю комунікацій до, під час і після порушення безпеки. Ефективне реагування на інциденти тепер вимагає проактивного, міжфункціонального підходу, який інтегрує комунікації в основу кіберпідготовленості…

Щоб створити міцну основу для управління кіберінцидентами, організації повинні:

Сформувати основну команду та визначити радників: Створити мультидисциплінарну команду, до складу якої входять керівники бізнесу, члени вищого керівництва, юридичні радники та зовнішні консультанти, визначивши чіткі ролі та обов'язки щодо реагування на інциденти. Ця команда повинна встановити керівні принципи управління інцидентами, такі як пріоритет репутації над короткостроковими бізнес-показниками.

Визначити ключових зацікавлених сторін: Визначити всіх внутрішніх та зовнішніх зацікавлених сторін, зрозуміти їхні уподобання щодо каналів комунікації, передбачити їхні запитання та забезпечити готовність організації швидко та ефективно зв'язатися з кожною групою під час кризи…

Розробіть план комунікаційних сценаріїв: створіть зручний та практичний план комунікацій, який охоплює різні сценарії порушень, повідомлення для зацікавлених сторін, заяви для ЗМІ та контактну інформацію. Цей план повинен бути переглянутий та затверджений ключовими особами, що приймають рішення, для забезпечення чіткості та узгодженості.

Перевірка реакції на стресові ситуації за допомогою настільних вправ: змоделюйте реалістичні кіберінциденти, щоб перевірити співпрацю команди, прийняття рішень та стратегії реагування. Ці вправи допомагають виявити прогалини, уточнити точки прийняття рішень (такі як виплата викупу або розкриття інформації регуляторним органам) та забезпечити готовність організації діяти швидко та злагоджено…

Оскільки очікується поширення атак з фінансовою мотивацією, таких як крадіжка даних, вимагання та використання програм-вимагачів, фахівці з комунікацій відіграють вирішальну роль в об'єднанні організації, формуванні планів реагування та забезпеченні готовності. Регулярний перегляд та оновлення плану, а також постійна співпраця між різними підрозділами допоможуть організаціям ефективно реагувати на кіберінциденти та захищати як свою репутацію, так і діяльність». ***(Ashley Grund, Michael Landau, Lauren Odell. Proactive Cyber Preparedness // J.R. O'Dwyer Company, Inc. (https://www.odwyerpr.com/story/public/24209/2026-01-27/proactive-cyber-preparedness.html). 27.01.2026).***

***

Країни ЄС та Великобританія

«…За словами Мігеля Де Брюйкера, голови Бельгійського центру кібербезпеки, Європа фактично «втратила інтернет» і свою цифрову суверенність через залежність континенту від хмарних сервісів і платформ, на

яких домінують американські технологічні гіганти, такі як Amazon, Microsoft і Google. Ця залежність робить блок вразливим до зовнішнього тиску, що стало особливо очевидним, коли адміністрація Трампа нещодавно ввела візові заборони для відомих європейців, звинувативши ЄС у несправедливому ставленні до американських компаній через регулювання контенту та дезінформації…

Де Брюйкер стверджує, що для ЄС «наразі неможливо» зберігати дані виключно в Європі, зазначаючи, що законодавство США, таке як Cloud Act, може змусити американські компанії надавати дані, що зберігаються на серверах у будь-якій точці світу. Як наслідок, європейські правоохоронні органи та критично важливі служби все більше залежать від систем, що контролюються іноземними державами, що обмежує стратегічну автономію та наражає блок на значні геополітичні ризики та ризики у сфері кібербезпеки.

Щоб відновити контроль, Де Брюйкер пропонує ЄС переглянути такі обмежувальні законодавчі акти, як Закон про штучний інтелект, який, на його думку, гальмує інновації. Натомість він виступає за ініціативу, що віддзеркалює успіх співпраці Airbus, закликаючи ЄС зосередити свої зусилля на «самостійному створенні чогось» у кіберпросторі, а не на спробах регулювати діяльність американських «гіпермасштабних компаній». ***(Gintaras Radauskas. Europe has lost the internet, Belgium's cyber security chief warns // Cybernews (https://cybernews.com/news/europe-internet-control-sovereignty-united-states/). 02.01.2026).***

***

«…Закон ЄС про кібербезпеку (CSA) 2019 року надав Європейському агентству з кібербезпеки (ENISA) статус постійного агентства та створив добровільну систему сертифікації кібербезпеки ЄС (ECCF) для продуктів, послуг та процесів у сфері ІКТ. З того часу кількість кібератак різко зросла, а нові закони — NIS2, Закон про кіберстійкість, майбутні схеми 5G та хмарних технологій тощо — збільшили навантаження на ENISA та ускладнили регуляторну карту. Була прийнята лише одна схема ЄС (Європейська схема кібербезпеки на основі загальних критеріїв (EUCC) для продуктів ІКТ); схеми хмарних технологій (EUCS - European Cybersecurity Certification Scheme for Cloud Services), 5G, цифрових гаманців та керованих послуг безпеки все ще не завершені. Тому CSA проходить свій перший п'ятирічний перегляд, який має відбутися 14 січня 2026 року…

Під час консультацій Комісії зацікавлені сторони в основному погодилися з трьома потребами: (1) раціоналізувати та гармонізувати дублюючі правила та обов'язки щодо повідомлення про інциденти в CSA, NIS2, CRA, AI Act та GDPR — в ідеалі за допомогою єдиної платформи ЄС для повідомлень, запропонованої в новому «цифровому омнібусному» регламенті; (2) посилити та уточнити повноваження, бюджет та штатний склад ENISA, щоб вона могла виконувати функції центрального технічного координатора Союзу; та (3) пришвидшити розробку сертифікації, зробити її більш прозорою та узгодженою з міжнародними стандартами, використовуючи схеми як визнаний доказ відповідності іншим законам ЄС…

Розбіжності стосуються суверенітету та сфери застосування. Декілька держав-членів та провайдери хмарних послуг, орієнтовані на ЄС, хочуть, щоб EUCS та інші схеми включали критерії «цифрової автономії», такі як локалізація даних та власність, що базується в ЄС; американські гіперскалери та прихильники відкритого ринку називають це нетехнічним, протекціоністським та шкідливим для інновацій. Також триває дискусія щодо того, чи сертифікація повинна залишатися добровільною (думка більшості) чи стати обов'язковою для секторів з високим ризиком, а також щодо того, наскільки обов'язковою повинна бути ENISA.

Майбутній законодавчий проект повинен збалансувати ці суперечності, прискорити сертифікацію, об'єднати численні закони ЄС у сфері кібербезпеки та вирішити нетехнічні ризики ланцюга поставок, зберігаючи при цьому інновації та глобальну взаємодію». ***(Polona Car. Cybersecurity Act review: What to expect // European Union (https://epthinktank.eu/2026/01/05/cybersecurity-act-review-what-to-expect/). 05.01.2026).***

***

«…Уряд Великобританії оприлюднив план дій у сфері кібербезпеки вартістю 210 мільйонів фунтів стерлінгів, спрямований на забезпечення безпеки та стійкості всіх онлайн-послуг для населення — соціальних виплат, оподаткування, охорони здоров'я тощо — у зв'язку з прискоренням реалізації державної програми переходу на цифрові технології. План, який буде реалізовуватися під наглядом нового урядового підрозділу з питань кібербезпеки, передбачає:

• картографувати кіберризики у всіх департаментах, щоб ресурси спрямовувалися туди, де вони найбільш потрібні;

• централізовано координувати дії щодо складних загроз, з якими жодна окрема установа не може впоратися самостійно;

• запровадити надійні та оперативні механізми реагування на інциденти;

• підвищити базовий рівень стійкості, усунувши основні прогалини в системі безпеки, які можуть призвести до відключення послуг…

Ця ініціатива підкріплює більш широке прагнення до цифровізації державних послуг, яке, за прогнозами, дозволить заощадити до 45 мільярдів фунтів стерлінгів за рахунок підвищення продуктивності, але успіх якого залежить від довіри громадськості. Вона збігається з законопроектом про кібербезпеку та стійкість, який зараз розглядається в парламенті і який передбачатиме введення більш суворих кіберстандартів для постачальників критично важливих послуг — енергетики, водопостачання, охорони здоров'я, центрів обробки даних — з метою зміцнення всього ланцюжка поставок у державному секторі.

Доповненням до плану є нова програма «Посли безпеки програмного забезпечення», в рамках якої такі компанії, як Cisco, Palo Alto Networks, Sage, Santander та NCC Group, будуть пропагувати добровільні рекомендації Кодексу практики безпеки програмного забезпечення з метою запобігання атакам на ланцюжок постачання програмного забезпечення; 59% організацій зазнали таких атак минулого року…» ***(New cyber action plan to tackle threats and strengthen public***

services // GOV.UK (https://www.gov.uk/government/news/new-cyber-action-plan-to-tackle-threats-and-strengthen-public-services). 06.01.2026).

***

«Національний центр кібербезпеки Ірландії опублікував свою другу Національну оцінку кіберризиків (NCRA) — необов'язковий, але впливовий огляд, який визначає порядок денний для наступної Національної стратегії кібербезпеки та майбутнього нагляду за NIS2. У документі виділено три системні ризики:

• Динамічна геополітична напруга – Ірландія, як центр багатонаціональних технологій та спільної підводної інфраструктури, може зазнати «вторинних» наслідків від атак, що фінансуються державою, на глобальних провайдерів.

• Розвиток технологій – широке поширення штучного інтелекту створює загрози швидкого втручання та отруєння даних, а шпигунство за принципом «збирай зараз, розшифровуй пізніше» передбачає появу квантових комп'ютерів, які до 2035 року зламають сучасні системи шифрування з відкритим ключем.

• Небезпека ланцюгів постачання – кіберзлочинці все частіше компрометують організації критично важливих секторів через недостатньо захищених постачальників та спільні платформи…

Для протидії цим загрозам NCSC рекомендує п'ять напрямків політики: розширити національну видимість та виявлення (більше датчиків, протидія дезінформації, дані про інциденти NIS2); застосування проактивної кіберзахисту (постійне сканування вразливостей та автоматичне блокування); підвищення національної стійкості (повне впровадження NIS2, сертифікація CyFun, готовність до кризових ситуацій, центри кіберсолідарності ЄС); зміцнення критичних ланцюгів постачання (жорсткіші правила закупівель, безпека за замовчуванням для постачальників, прозорість власності); та інвестиції в навички, дослідження та центр передового досвіду…

Для компаній, особливо тих, що класифікуються як критична або цифрова інфраструктура, NCRA є керівництвом з підготовки до NIS2. Правління повинні переглянути заходи з управління ризиками: перевірку постачальників та контракти, регулярні оцінки безпеки, робочі процеси з повідомлення про інциденти, навчання персоналу та керівників. Хоча NIS2 діє на рівні ЄС з жовтня 2024 року, Ірландія ще не транспонувала її; Національний закон про кібербезпеку, який очікується в першому півріччі 2026 року, впровадить директиву та надасть NCSC повноваження з нагляду». ***(Rachel Hayes, Leo Moore and Caroline Keaveny. Cyber Threats Facing Ireland's Critical Services, Systems and Infrastructure // William Fry (https://www.williamfry.com/knowledge/cyber-threats-facing-irelands-critical-services-systems-and-infrastructure/). 06.01.2026).***

***

«Угорщина прийняла Закон CXXXV від 2025 року з метою імплементації Закону ЄС про кіберстійкість (Регламент (ЄС) 2024/2847), який встановлює національну систему зобов'язань у сфері кібербезпеки, пов'язаних з продуктами, що містять цифрові елементи. Закон призначає Наглядовий орган з

питань регулювання (SZTFH) як орган, що здійснює нотифікацію, так і орган, що здійснює нагляд за ринком, та встановлює детальні процедурні правила щодо його діяльності з нотифікації та нагляду…

Він запроваджує багаторівневу систему штрафів: серйозні порушення основних вимог кібербезпеки та певних зобов'язань виробників можуть призвести до штрафів у розмірі від 500 000 форинтів (близько 1285 євро) до 15 мільйонів євро або 2,5% від глобального річного обороту компанії, залежно від того, яка сума є вищою; порушення зобов'язань, таких як декларації про відповідність ЄС, маркування CE та технічна документація виробників, імпортерів та дистриб'юторів, караються штрафами до 10 млн євро або 2% від глобального обороту; надання невірної, неповної або оманливої інформації нотифікованим органам або SZTFH може призвести до штрафів до 5 млн євро або 1% від глобального обороту. За повторні порушення штрафи повинні бути щонайменше в 1,5 рази вищими за попередню суму, з урахуванням встановлених законом максимальних розмірів…

Закон про кіберстійкість гармонізує основні вимоги до кібербезпеки при проектуванні, розробці, виробництві та усуненні вразливостей продуктів з цифровими елементами (наприклад, носимих пристроїв, підключених іграшок, пристроїв для розумного будинку, операційних систем, VPN, антивірусного програмного забезпечення). В Угорщині детальні правила щодо функції SZTFH з повідомлення про порушення набудуть чинності 11 червня 2026 року, а положення про нагляд за ринком та штрафи будуть застосовуватися з 11 грудня 2027 року». ***(Katalin Horváth and János Bálint. EU Cyber Resilience Act's implementing provisions published in the Hungarian Official Journal // CMS Legal (https://cms-lawnow.com/en/ealerts/2026/01/eu-cyber-resilience-act-s-implementing-provisions-published-in-the-hungarian-official-journal). 07.01.2026).***

***

«5 грудня 2025 року, більш ніж через рік після закінчення терміну перенесення директиви NIS 2 до національного законодавства, в Німеччині набув чинності Закон про перенесення директиви NIS 2 та регулювання ключових аспектів управління інформаційною безпекою у федеральній адміністрації (NIS2UmsG). Як «статтевий закон», він вносить зміни до низки існуючих законодавчих актів, зокрема до німецького Закону про Федеральне управління з інформаційної безпеки (BSIG), який тепер називається «новим BSIG». За даними Федерального управління з інформаційної безпеки (BSI), близько 29 500 компаній підпадатимуть під посилений режим кібербезпеки… Основна зміна полягає в розширенні сфери застосування: тепер закон регулює діяльність «особливо важливих підприємств» та «важливих підприємств» у таких секторах, як енергетика, транспорт, фінанси, охорона здоров'я, водопостачання, цифрова інфраструктура, космічна галузь, поштові та кур'єрські послуги, поводження з відходами, хімічна промисловість, харчова промисловість, виробництво, цифрові послуги та наукові дослідження. Класифікація залежить від сектора та розміру (кількість співробітників та фінансові показники). Обидві категорії повинні виконувати однакові суттєві зобов'язання з кібербезпеки, але BSI має ширші повноваження з попереднього нагляду за особливо важливими установами.

Новий BSIG встановлює комплексні зобов'язання з управління ризиками (§ 30), вимагаючи вжиття відповідних, пропорційних та ефективних технічних і організаційних заходів для забезпечення доступності, цілісності та конфіденційності IT-систем, включаючи політику щодо аналізу ризиків та інформаційної безпеки, реагування на інциденти, безперебійної роботи та кризового управління, безпеки ланцюгів постачання, безпечного розвитку та обслуговування, усунення вразливостей, оцінки ефективності, навчання, інформування та управління персоналом, контролю доступу та політики управління ІКТ… Застосовуються суворі обов'язки щодо повідомлення про інциденти (§ 32): первинне повідомлення через портал BSI протягом 24 годин після виявлення значного інциденту безпеки, подальше повідомлення протягом 72 годин з первинною оцінкою, проміжні звіти на запит та остаточний звіт протягом одного місяця (або звіт про хід розслідування, якщо інцидент триває). У серйозних випадках BSI може зобов'язати суб'єктів господарювання інформувати отримувачів послуг та надавати рекомендації щодо пом'якшення наслідків, зокрема у сферах фінансів, цифрової інфраструктури, управління ІКТ та цифрових послуг.

Органи управління (§ 38) несуть пряму відповідальність за впровадження, моніторинг та регулярне оновлення цих заходів з управління ризиками і повинні проходити регулярне навчання; невиконання цих обов'язків може спричинити внутрішню відповідальність згідно з корпоративним правом. Суб'єкти, на яких поширюється дія закону, також повинні зареєструватися в BSI протягом трьох місяців з моменту набуття відповідного статусу (§ 33), надавши через портал BSI дані про ідентифікацію, контакти, діапазон IP-адрес та сектор діяльності. Для перевірки дотримання вимог BSI має право (§§ 61, 62) вимагати докази, проводити аудити та інспекції, отримувати доступ до приміщень та документів, а також вимагати вжиття коригувальних заходів; для важливих установ це, як правило, відбувається постфактум, коли є ознаки недотримання вимог, тоді як особливо важливі установи можуть підлягати попередньому нагляду. В крайньому випадку BSI може спробувати призупинити дію ліцензій або усунути ненадійне керівництво від виконання своїх обов'язків. Оператори «критичних об'єктів» мають ще більш суворі зобов'язання і можуть отримати заборону на використання певних критичних компонентів. Німецький уряд оцінює щорічні витрати на дотримання вимог у розмірі близько 2,3 млрд євро та одноразові витрати на впровадження у розмірі близько 2,2 млрд євро для економіки. Для допомоги організаціям у визначенні того, чи та в якій мірі на них поширюється дія NIS2UmsG, доступний інструмент оцінки впливу BSI…» ***(Moritz Hüsch, Lars Lensdorf and Clemens Jaaks. Germany Transposes NIS 2 Directive - Increased Cybersecurity Requirements for Businesses // Covington & Burling LLP (https://www.insideprivacy.com/cybersecurity-2/germany-transposes-nis-2-directive-increased-cybersecurity-requirements-for-businesses/#page=1). 07.01.2026).***

***

«…З 2026 року кібербезпека в Європі перейде від етапу планування до етапу впровадження. Компанії, що постачають цифрові продукти або надають критично важливі послуги, повинні тепер розглядати кіберризики як питання

дотримання нормативних вимог на рівні правління та інтегрувати їх у систему управління, розробку продуктів, управління ланцюгами постачання та реагування на інциденти. У програмі на 2026 рік домінують вісім пріоритетів:

• Дотримуватися національних законів NIS2. Всі 27 держав ЄС впроваджують Директиву про мережі та інформаційні системи 2 дещо по-різному; штрафи, відповідальність керівництва та обов'язки щодо реєстрації варіюються. Юридичні команди повинні відстежувати законопроекти, лобіювати їх у разі потреби та фіксувати розбіжності.

• Застосовувати режим Німеччини. Закон NIS2 Берліна вже набрав чинності, що спричинило реєстрацію, розробку політики, оновлення заходів безпеки та нові правила повідомлення про інциденти.

• Впроваджувати NIS2 скрізь. Створити узгоджені політики, багатоюрисдикційні робочі процеси звітності, готовність до аудиту, навчання правління та навчальні тренування до того, як регуляторні органи почнуть інспекції у 2026 році.

• Підготуватися до Закону про кіберстійкість. З вересня 2026 року (повна сила дії з грудня 2027 року) майже всі підключені до мережі продукти, що продаються в ЄС — пристрої IoT, програмне забезпечення, маршрутизатори, промислові системи управління — повинні відповідати вимогам щодо безпеки за замовчуванням, усунення вразливостей та документації. Команди, що розробляють продукти, повинні класифікувати товари, перепроектувати архітектуру там, де це необхідно, та створити технічну документацію вже зараз.

• Впровадити DORA для фінансів. Банки, страхові компанії, фінтех-компанії та їхні постачальники ІКТ повинні до січня 2025 року створити системи управління ризиками ІКТ, тести на стійкість, механізми нагляду за постачальниками та конкретні плани дій на випадок інцидентів; у 2026 році буде проведено інтенсивний нагляд.

• Перевірити статус стійкості критичних об'єктів (CER). До липня 2026 року держави-члени повинні визначити операторів, що мають важливе значення. Ймовірні кандидати — постачальники послуг центрів обробки даних та енергії, транспортні вузли — повинні розпочати оцінку ризиків та стійкості типу CER та привести їх у відповідність до NIS2.

• Слідкувати за «Цифровим омнібусом» ЄС. Пакет спрощень змінить звітність NIS2, підвищить поріг порушення GDPR, додасть нові правові основи для обробки чутливих даних (ШІ, дослідження), гармонізує DPIA та спростить правила щодо файлів cookie. Компанії повинні відстежувати та готуватися до коригування політик.

• Слідкувати за законопроектом NIS у Великобританії. Після Brexit Лондон планує розширити сферу застосування (центри обробки даних, MSP), ввести позначку «критичні постачальники» та двоступеневу систему звітності про інциденти, яка відрізняється від NIS2. Транснаціональні компанії повинні визначити відмінності та передбачити обов'язки щодо повідомлення клієнтів…

В сукупності ці заходи передбачають підвищення штрафів, особисту відповідальність керівників, повноваження щодо вилучення продукції з обігу та права на проведення транскордонних аудитів. Юридичні радники та керівники

служб інформаційної безпеки повинні вже зараз співпрацювати над аналізом прогалин, положеннями щодо ланцюгів постачання, інструкціями з управління та брифінгами для правління, щоб забезпечити дотримання вимог кібербезпеки в усій Європі до того, як регуляторні органи почнуть застосовувати ці заходи у 2026 році». ***(Natallia Karniyevich and Rosa Barcelo. Eight European cyber priorities for legal counsel and CISOs in 2026 // McDermott Will & Schulte (https://www.mwe.com/insights/eight-european-cyber-priorities-for-legal-counsel-and-cisos-in-2026/). 08.01.2026).***

***

«6 січня 2026 року уряд Великої Британії оприлюднив новий урядовий план дій у сфері кібербезпеки, визнаючи, що переваги цифровізації державних послуг можуть бути реалізовані лише за умови, що ці послуги є безпечними, надійними та стійкими. Центральним елементом плану є створення урядової кібербезпекової групи, на яку виділено понад 210 мільйонів фунтів стерлінгів, з метою забезпечення більш ефективного централізованого керівництва, експертної підтримки департаментів та досягнення відчутних покращень у сфері кіберстійкості. План переформатує нагляд за постачальниками, визначивши певних постачальників як «стратегічних», якщо вони працюють у великих масштабах або надають послуги, критично важливі для уряду; ці постачальники з підвищеним ризиком будуть підлягати скоординованому міжвідомчому нагляду, а не управлятися окремими департаментами, що дозволить отримати єдине уявлення про системні вразливості…

План буде реалізовано у три етапи: до квітня 2027 року будуть створені такі основоположні елементи, як кіберпідрозділ, чіткі рамки відповідальності, міжвідомча кіберпрофесія та урядовий план реагування на кіберінциденти; з 2027 по 2029 рік основна увага буде зосереджена на масштабуванні прийняття рішень на основі даних, послуг кіберпідтримки та можливостей реагування; з квітня 2029 року акцент буде зроблено на постійному вдосконаленні, використанні централізованих кіберданих, наданні послуг у великих масштабах, використанні кіберпрофесії для трансформації та забезпеченні проактивного управління кіберризиками у ланцюгах постачання департаментів… Ця заява збіглася з другим читанням законопроекту про кібербезпеку та стійкість, який оновить режим мережі та інформаційних систем Великобританії шляхом розширення обов'язків щодо повідомлення про інциденти, введення категорії «критичних постачальників» та поширення регулювання на центри обробки даних, служби контролю навантаження та постачальників керованих послуг. Разом з такими ініціативами, як Програма амбасадорів з безпеки програмного забезпечення, яку підтримують такі компанії, як Cisco, Palo Alto Networks, Sage, Santander та NCC Group, План є частиною більш широких зусиль, спрямованих на підвищення стандартів кібербезпеки як у державному, так і в приватному секторах». ***(Anthony Rosen. UK's Government Cyber Action Plan // Bird & Bird (https://www.twobirds.com/en/insights/2026/uk's-government-cyber-action-plan). 12.01.2026).***

***

«Законопроект Великобританії про кібербезпеку та стійкість (мережеві та інформаційні системи), представлений парламенту 12 листопада 2025 року, має на меті модернізувати систему регулювання кібербезпеки в країні шляхом розширення кола регульованих суб'єктів, посилення зобов'язань щодо повідомлення про інциденти та посилення нагляду в критично важливих секторах. Вперше широке коло постачальників цифрових послуг, включаючи IT-компанії та компанії з кібербезпеки, що підтримують державні та приватні організації, буде підлягати прямому регулюванню. Ці постачальники повинні будуть відповідати мінімальним стандартам безпеки, підтримувати надійні можливості реагування на інциденти та моніторингу, а також негайно повідомляти клієнтів про значні або потенційно значні кіберінциденти…

Законопроект суттєво розширює перелік інцидентів, про які необхідно повідомляти (включаючи програми-вимагачі та невиявлені дії з «попереднього позиціонування»), і встановлює суворі терміни: первинне повідомлення регуляторному органу протягом 24 годин з моменту виявлення інциденту, а потім повне повідомлення протягом 72 годин. Це вимагатиме від страхувальників і страховиків узгодити формулювання полісів кіберстрахування та пункти про повідомлення з встановленими законом обов'язками щодо повідомлення, щоб уникнути конфліктів на етапі розгляду страхових вимог. Правління компаній будуть піддаватися посиленому контролю за виявленням, ескалацією та реагуванням на інциденти і повинні будуть надати страховикам докази ефективного управління та контролю…

Нагляд буде здійснюватися за допомогою секторальної моделі з участю декількох регуляторних органів, в рамках якої 12 регуляторних органів, таких як Управління комісара з питань інформації для середніх і великих постачальників керованих послуг, отримають розширені повноваження з забезпечення дотримання законодавства, включаючи можливість накладати штрафи та санкції за недотримання вимог. Можливість страхування таких санкцій залежатиме від формулювання полісу, правової позиції щодо страхування штрафів та характеру відповідної поведінки (наприклад, умисне правопорушення проти недбалості). Загалом, законопроект підвищує вимоги до кіберстійкості та управління і змінить підхід до покриття, повідомлення про інциденти та регуляторних ризиків у рамках кіберстрахування та пов'язаних страхових полісів. Очікується, що він набуде чинності поетапно, починаючи з першої половини 2026 року, причому деякі повноваження набудуть чинності після затвердження королем, а інші – через вторинне законодавство». ***(Peter Hardy, Eleanor Ruiz and Claudia Gwinn. The UK Cyber Security and Resilience Bill - Policyholder Implications // Reed Smith LLP (https://www.reedsmith.com/our-insights/blogs/the-policyholder-perspective/102m1kv/the-uk-cyber-security-and-resilience-bill-policyholder-implications/#page=1). 13.01.2026).***

***

«Система кібербезпеки та комунікацій Чеської Республіки перебуває у фазі активної трансформації після прийняття низки ключових законів у 2025 році, а практичні зобов'язання мають бути конкретизовані через вторинне

законодавство та посилений нагляд у 2026 році. Новий Закон про кібербезпеку (Закон № 264/2025 Coll.), який набрав чинності 1 листопада 2025 року, впроваджує Директиву ЄС NIS2 та значно розширює коло регульованих суб'єктів. Однак режим ще не є досконалим: ключові урядові нормативні акти, що визначають «основні функції» та «стратегічно важливі послуги», все ще перебувають на стадії розробки… Після прийняття цих правил очікується, що вони запровадять більш суворі правила щодо стійкості ланцюгів постачання та дозволять органам влади обмежувати використання небезпечного обладнання або постачальників з геополітичних міркувань. Тим часом Національне агентство з кібербезпеки та інформаційної безпеки (NÚKIB) опублікувало рекомендації та розробляє спеціальний портал, а компанії очікують на підтвердження своїх реєстрацій NIS2, поданих до кінця грудня 2025 року. Більшість термінів дотримання вимог почнуть діяти з дати офіційного підтвердження реєстрації кожної компанії, що може зайняти деякий час. Іноземні постачальники послуг електронних комунікацій та мереж повинні уважно стежити за будь-якими змінами на порталі NÚKIB та за тим, як NÚKIB застосовує концепцію NIS2 «головного закладу», що може дозволити єдину реєстрацію в ЄС для певних послуг.

Паралельно з цим, впровадження Директиви ЄС про стійкість критичних об'єктів (CER) просувається завдяки новому Закону про критичну інфраструктуру (Закон № 266/2025 Coll.), який також набирає чинності з 1 листопада 2025 року, але його режим стане повністю оперативним лише після остаточного затвердження критеріїв ідентифікації критичних об'єктів та відповідних імплементаційних нормативних актів. У фінансовому секторі очікується, що Чеський національний банк (CNB) посилить нагляд за безпосередньо застосовним Законом про цифрову операційну стійкість (DORA), передбачаючи регуляторні опитування та інспекції; DORA також має побічні наслідки для постачальників фінансових установ, включаючи операторів телекомунікаційних послуг. Окремо, з 1 січня 2026 року Чеське телекомунікаційне управління почало вести Центральний реєстр заблокованих веб-сайтів, об'єднавши раніше окремі списки незаконних гральних сайтів та веб-сайтів, що пропонують незаконні наркотики або ліки, в єдиний реєстр, придатний для машинного зчитування, з метою спрощення нагляду. Загалом, організації, що працюють на чеському ринку, повинні очікувати поступового посилення регуляторного контролю, уважно стежити за вторинним законодавством та практикою нагляду, а також підтримувати конструктивний діалог з NÚKIB, CNB та Чеським телекомунікаційним управлінням, щоб орієнтуватися в цій мінливій ситуації…» ***(Ján Kuklinca. What to expect in 2026 in Czech cybersecurity and telecommunications law // Bird & Bird (https://www.twobirds.com/en/insights/2026/what-to-expect-in-2026-in-czech-cybersecurity-and-telecommunications-law). 12.01.2026).***

***

«31 грудня 2025 року Італійське національне агентство з кібербезпеки (ACN) опублікувало нові оперативні вказівки щодо стандартизації та вдосконалення управління кіберінцидентами, що має на меті підвищити стійкість та безперебійність критично важливих послуг. Вказівки зобов'язують

організації розробити офіційний план управління інцидентами, в якому задокументовано ролі, обов'язки, контактну інформацію та протоколи комунікації. Важливо, що цей план повинен детально описувати процедури подання проміжних, щомісячних та остаточних звітів про інциденти, які вимагаються згідно зі статтею 25 декрету NIS…

Модель ACN відповідає структурованому чотирифазному життєвому циклу. Вона починається з підготовки, яка поділяється на управління (визначення стратегії та ролей), ідентифікацію (аудит систем та картографування загроз) та захист. Захист передбачає як технічні заходи безпеки, такі як аналіз журналів та незмінні резервні копії, так і організаційні заходи, такі як навчання персоналу та періодичні симуляції. Другий етап, виявлення, зосереджується на ідентифікації значущих подій, таких як несанкціоновані адміністративні зміни, повторні невдалі спроби входу або підключення від відомих індикаторів компрометації (IOC). На цьому етапі використовується поєднання реактивних сповіщень та проактивного пошуку загроз із застосуванням методологій на основі IOC, аномалій (статистичних відхилень) та TTP (тактик і процедур) для виявлення зловмисників.

Після підтвердження інциденту починається фаза реагування. Вона включає чотири важливі етапи: негайне повідомлення владі та зацікавленим сторонам, ретельне розслідування для відтворення «ланцюжка кібервбивств», локалізація для зупинки поширення атаки та ліквідація. Під час ліквідації команди повинні очистити облікові дані, видалити шкідливі артефакти та виправити вразливості, які були використані. Процес завершується фазою відновлення, під час якої системи повертаються до свого звичайного стану та перевіряються на стабільність і безпеку…

Ці рекомендації, доповнені технічними додатками щодо заходів безпеки, специфічних для NIS, є еталоном для дотримання вимог. Організації тепер несуть відповідальність за забезпечення не тільки оперативності, але й ефективності цих планів реагування, оскільки ACN оцінюватиме ці плани під час аудитів і може притягнути організації до відповідальності, якщо їхні можливості реагування виявляться недостатніми під час успішного порушення». ***(Matia Campo, Veronica Mazzaferro and Alice Dal Bello. Nuove Linee Guida NIS: definizione del processo di gestione degli incidenti di sicurezza informatica // CMS Law-Now (https://news.cms.law/rv/ff00fe1a7580094bdda72aa4c645a6e4291f9ae6?utm_source=Concep%20Send&utm_medium=email&utm_campaign=CMS+Newsletter+%7c+Nuove+Linee+Guida+NIS%3a+definizione+del+processo+di+gestione+degli+incidenti+di+sicurezza+informatica_01%2f14%2f2026). 14.01.2026).***

***

«…Швейцарські експортери стикаються з «регуляторним цунамі» з боку ЄС, причому Закон про кіберстійкість (CRA) виступає як критична перешкода для доступу до ринку. Згідно з CRA, який набрав чинності в грудні 2024 року, будь-який «продукт з цифровими елементами», включаючи пристрої IoT, смартфони, промислове обладнання і навіть автономне програмне забезпечення, повинен мати маркування CE і повну документацію з кібербезпеки, щоб бути імпортованим в ЄС. Ця документація повинна включати перелік програмного

забезпечення (SBOM) та доказ успішної оцінки відповідності. Хоча деякі сектори, такі як медичні пристрої або автомобільні транспортні засоби, виключені з-під дії закону через існуючі специфічні правила, екстериторіальна дія CRA означає, що швейцарські виробники повинні перепроектувати продукти з урахуванням принципів безпеки за замовчуванням та безпеки за замовленням, проводити ретельну оцінку ризиків та створювати довгострокові системи управління вразливостями, які забезпечують безкоштовні оновлення безпеки протягом усього терміну експлуатації продукту…

Фінансові та операційні ризики, пов'язані з недотриманням вимог, є серйозними: дистриб'ютори ЄС можуть відмовити в імпорті, а національні органи влади мають право відкликати продукцію, проводити позапланові перевірки та накладати штрафи в розмірі до 2,5% від глобального обороту компанії. Крім того, недотримання цих стандартів кібербезпеки може призвести до визнання продукту «дефектним» відповідно до Директиви ЄС про відповідальність за продукцію, що наражає виробників на цивільну відповідальність незалежно від вини. Виробники також повинні дотримуватися суворих вимог щодо прозорості стосовно періодів підтримки та процедур оновлення. Час на дотримання вимог вже йде: повідомлення про вразливість починається 11 вересня 2026 року, а повні загальні зобов'язання застосовуються до 11 грудня 2027 року. Очікується, що швейцарське законодавство піде тим самим шляхом, оскільки Федеральна рада планує до осені 2026 року розробити власний законопроект про кібербезпеку цифрових продуктів. Практична підготовка повинна розпочатися вже зараз з аналізу обсягу, оцінки прогалин та перегляду процесів управління — від контрактів з постачальниками до внутрішнього контролю — щоб забезпечити життєздатність підключених продуктів на європейському ринку». ***(Martin Eckert. The EU Cyber Resilience Act - New Market Entry Barriers for Swiss IoT Products // MME Legal Tax Compliance (https://www.mme.ch/en/magazine/articles/the-eu-cyber-resilience-act-new-market-entry-barriers-for-swiss-iot-products). 14.01.2026).***

***

«Європа вступає в 2026 рік після бурхливого 2025 року, який відзначився широкомасштабними кіберзбоями, включаючи відключення аеропортів, звинувачення у втручанні у вибори, інциденти з підробкою GPS-сигналів, що вплинули на рейси високого рівня, та атаки на космічні системи. На цей регіон припадало близько 22% світової активності програм-вимагачів, а також спостерігався сплеск розподілених атак типу «відмова в обслуговуванні» (DDoS), яких у першій половині року було зафіксовано 3,2 мільйона по всій Європі, Близькому Сходу та Африці. Фінансові збитки були значними: за даними страхової компанії Howden, лише Франція, Німеччина, Італія та Іспанія втратили загалом 300 мільярдів євро за останні п'ять років, що зробило кібербезпеку головним пріоритетом уряду…

Основні прогнози від Forrester, Google та Fortinet вказують на три домінуючі теми на 2026 рік. По-перше, геополітичні кібероперації будуть розширюватися, а суб'єкти, пов'язані з Росією, Китаєм, Іраном та Північною Кореєю, як очікується, посилять кампанії, спрямовані на політичний та економічний вплив. Google

попереджає, що Китай, ймовірно, посилить зусилля проти стратегічно важливих галузей, таких як напівпровідники, тоді як Росія, як очікується, продовжить операції в Україні та розширить довгостроковий вплив і інформаційні операції навколо виборів; також прогнозується, що Іран посилить регіональні кампанії через узгоджені інформаційні сайти. Для посилення скоординованої оборони Forrester очікує, що ЄС розробить власну базу даних «відомих вразливостей, що експлуатуються», щоб поліпшити транскордонний обмін розвідданими.

По-друге, ШІ перетвориться з новинки на базову функцію як атак, так і засобів захисту. Прогнози підкреслюють зростання популярності автономних ШІ-агентів, які використовуються зловмисниками для масштабування та координації кампаній з мінімальним людським наглядом, поряд з такими техніками, як швидке введення для маніпулювання системами ШІ, фішинг, генерований ШІ, та «вішинг» з використанням гіперреалістичного клонування голосу для імітації керівників або ІТ-персоналу. Водночас очікується, що захисники використовуватимуть ШІ для прискорення аналізу інцидентів, декодування шкідливого коду та виявлення тактики зловмисників…

По-третє, кіберпростір як поле бою розширюється у космос, де супутники та системи GPS все частіше стають об'єктами перешкод та підробки. Fortinet прогнозує збільшення кількості атак на навігаційні системи, що залежать від супутників, що підвищує ризики для авіації, судноплавства та оборони, включаючи потенційне неправильне керування дронами та ракетами або порушення роботи літаків. Рекомендовані заходи щодо зменшення ризиків включають посилення безпеки супутників, наприклад додавання рівнів шифрування, щоб зменшити вплив перешкод GPS у міру того, як кібервійна стає все більш поширеною». ***(Anna Desmarais. From AI breaches to rising geopolitical threats, here's what to expect from cybersecurity in 2026 // euronews (https://www.euronews.com/next/2026/01/12/from-ai-breaches-to-rising-geopolitical-threats-heres-what-to-expect-from-cybersecurity-in). 12.01.2026).***

***

«Ландшафт кібербезпеки для телерадіокомпаній та медіакомпаній визначається низкою конвергентних рамок, включаючи R 144 Європейської мовної спілки (EBU), Рамку кібербезпеки 2.0 Національного інституту стандартів і технологій (NIST) та Мережу надійних партнерів (TPN) Асоціації кінопродюсерів (MPA), які всі наголошують на тому, що ефективний захист ґрунтується на управлінні, а не лише на технологіях. Ці стандарти надають медіаорганізаціям дорожню карту для виходу за межі реактивної безпеки та управління серйозними ризиками, пов'язаними з DDoS, програмним забезпеченням-вимагачем та шкодою репутації…

Структура EBU, яка рекомендує медіакомпаніям прагнути до досягнення принаймні рівня 3 («Визначений») зрілості, визначає п'ять стадій зрілості, від «Хаотичного» (рівень 1, відсутність задокументованих ролей) до «Оптимізованого» (рівень 5, сертифікація ISO/IEC 27001). Досягнення рівня 3 вимагає офіційних, затверджених керівництвом політик кібербезпеки, задокументованих стандартних процедур та встановлених ролей безпеки. EBU наголошує, що CISO повинен мати

повноваження приймати рішення та розпоряджатися бюджетом, а пріоритет кібербезпеки повинен охоплювати системи мовлення (трафік, автоматизація, передача) так само, як і традиційні IT…

Основні вимоги для всіх систем включають:

Управління: NIST CSF 2.0 чітко вимагає, щоб організації встановлювали, повідомляли та контролювали комплексні політики управління ризиками в масштабах всієї організації, затверджені керівництвом.

Безпека ланцюга поставок: Організації повинні ретельно перевіряти сторонніх постачальників та постачальників послуг. R 143 EBU та TPN MPA (обов'язкова оцінка для постачальників великих студій) вимагають від постачальників детальних запевнень щодо безпеки, що охоплюють їхні ISMS, безпеку програмного забезпечення та управління субпідрядниками…

Організаційна структура: Основні функції включають спеціального керівника з інформаційної безпеки (CISO), групу реагування на інциденти комп'ютерної безпеки (CSIRT) для аналізу та координації, а також центр безпеки (SOC) для технічного виконання. CSIRT повинна бути функціонально відокремлена від IT-виробництва, але контролювати всі системи, включаючи бізнес-додатки та критичну інфраструктуру мовлення.

Впровадження цих систем вимагає постійних інвестицій, відданості керівництва та усвідомлення того, що вартість проактивних заходів набагато менша, ніж фінансові та репутаційні наслідки успішної атаки. Системи визначають чітку мету; медіакомпанії повинні обрати комплексний, проактивний шлях для досягнення необхідного рівня зрілості». ***(Navigating cybersecurity standards for media companies: NIST, EBU and MPA requirements explained // NCS (https://www.newscaststudio.com/2026/01/15/navigating-cybersecurity-standards-for-media-companies-nist-ebu-and-mpa-requirements-explained/). 15.01.2026).***

***

«Кібератаки, підсилені широкою доступністю інструментів штучного інтелекту, різко зростають як за обсягом, так і за складністю, створюючи існувальну загрозу для державного сектора Великобританії. Після інциденту з JLR, який завдав британській економіці збитків на суму близько 2 мільярдів фунтів стерлінгів, експерти попереджають, що масштабна атака на критично важливі об'єкти Національної служби охорони здоров'я (NHS), центральні урядові служби або місцеві органи влади може призвести до катастрофічних людських жертв, як це було під час атаки Synnovis у 2024 році, та до масштабних економічних збитків. Національна рада з кібербезпеки (NCSC) нещодавно повідомила, що у Великобританії в середньому відбувається чотири атаки національного значення на тиждень…

Захисники стикаються з різноманітними загрозами: ворожими державами (наприклад, проросійськими угрупованнями, які проводять DDoS-атаки з метою підриву демократії), фінансово мотивованими організаціями, що використовують програми-вимагачі (за даними Міністерства фінансів США, таких угруповань налічується понад 267), та неформальними мережами молодих хакерів (наприклад, Scattered Spider та The Com), які використовують такі платформи, як Discord та

Telegram, для обміну інструментами та навичками, що прискорює їх перетворення на серйозну загрозу. Ці молоді хакери, яких іноді готують і експлуатують, стоять за атаками на такі великі компанії, як M&S, Co-op і JLR. Велика різноманітність мотивів — від грошей і шпигунства до слави — означає, що організації державного сектору не можуть зосередитися лише на одному ворогу; вони повинні захищатися від усіх, часто маючи вкрай обмежені ресурси…

Головний інспектор-детектив Джеремі Бенкс зазначив, що правоохоронні органи займаються 50% усіх злочинів (кіберзлочинів та шахрайства), маючи в своєму розпорядженні лише 1% бюджету, тоді як місцеві органи влади з 2010 року стикаються з масовими скороченнями бюджетів. Як наслідок, сектор змушений покладатися на пошук найефективніших інструментів та зосереджуватися на максимальній ефективності. Державні служби особливо вразливі через спільних постачальників, що означає, що компрометація одного постачальника може поширитися на десятки організацій, а також через тактику зловмисників, які атакують поза робочим часом, щоб максимально збільшити час перебування в системі.

Щоб перейти від реактивної до проактивної позиції, організації повинні використовувати інтелектуальну аналітику загроз на основі штучного інтелекту та автоматизацію. Платформи штучного інтелекту можуть аналізувати величезні обсяги даних з відкритого та темного вебу, щоб майже в режимі реального часу виявляти нові кампанії, а автоматизація дозволяє центрам безпеки (SOC), що працюють цілодобово, миттєво реагувати на відомі загрози — ізолюючи пристрої або блокуючи шкідливу інфраструктуру без очікування схвалення з боку людини. Важливо, що штучний інтелект допомагає розставити пріоритети серед сповіщень, забезпечуючи зосередження обмежених людських ресурсів на найкритичніших ризиках. Однак експерти наголосили, що людське судження та контекст залишаються життєво важливими, особливо коли рішення впливають на критично важливі послуги або громадську безпеку…

Людська поверхня атаки, посилена соціальним інжинірингом на основі штучного інтелекту (з використанням індивідуальних повідомлень та імітації голосу), вимагає спеціальних заходів захисту. Оскільки IT-системи постійно змінюються, стираючи межу між законними оновленнями та зловмисними змінами, освіта повинна виходити за межі традиційних тестів на фішинг. Такі практики, як винагорода співробітників обідніми ваучерами за повідомлення про підроблені тестові елементи, які використовує Recorded Future, допомагають сформувати культуру, в якій повідомлення про підозрілу діяльність цінується, що, на думку Бенкса, є необхідним для боротьби з професійними злочинними угрупованнями». ***(Jason Steer. Harness AI driven threat intelligence for proactive cyber defence // Informed Communications Ltd. (https://www.ukauthority.com/articles/harness-ai-driven-threat-intelligence-for-proactive-cyber-defence). 20.01.2026).***

***

«Європейська Комісія запропонувала новий комплексний пакет заходів з кібербезпеки, що включає переглянутий Закон про кібербезпеку та цільові поправки до Директиви NIS2, щоб рішуче посилити стійкість ЄС до

стратегічних загроз, зокрема тих, що походять від постачальників із третіх країн…

Переглянутий Закон про кібербезпеку зосереджується на забезпеченні безпеки ланцюга постачання ІКТ в ЄС шляхом створення горизонтальної структури для надійної безпеки. Ця структура дозволить ЄС та державам-членам спільно проводити оцінку ризиків та вживати заходів щодо їх мінімізації, включаючи, за необхідності, заборону використання компонентів постачальників з високим рівнем ризику в критично важливих ІКТ-активах. Крім того, Закон оновить Європейську систему сертифікації кібербезпеки (ECCF), щоб гарантувати, що продукти, які надходять до громадян ЄС, є «кібербезпечними за своєю конструкцією». ECCF буде спрощена, що дозволить швидше розробляти схеми сертифікації (протягом 12 місяців) і розширити їх для сертифікації загального кіберзахисту суб'єктів, що потім може слугувати доказом відповідності NIS2 та іншим законодавчим актам ЄС.

Зміни до Директиви NIS2 мають на меті зменшити навантаження на підприємства, пов'язане з дотриманням вимог, шляхом уточнення правових норм для понад 28 700 компаній та введення нової категорії «малих середніх підприємств». Ці зміни також спростять збір даних про програми-вимагачі та посилять координаційну роль ENISA у нагляді за транскордонними організаціями…

Агентство ЄС з кібербезпеки (ENISA) отримає розширені повноваження для управління оновленим ECCF, видачі попереджень про загрози, підтримки відновлення після атак з вимаганням викупу, управління єдиною точкою введення повідомлень про інциденти Digital Omnibus та посилення зусиль ЄС у сфері стандартизації кібербезпеки.

В цілому, цей пакет заходів, який доповнює існуючі закони, такі як CRA, DORA та Закон про кіберсолідарність, має на меті забезпечити технологічну незалежність Європи, зменшити стратегічні ризики від іноземного втручання та забезпечити високий рівень безпеки та довіри в критичній інфраструктурі та на цифрових ринках…» ***(Anna Ribeiro. European Commission proposes revised Cybersecurity Act to boost EU cyber resilience, secure ICT supply chains // Industrial Cyber (https://industrialcyber.co/regulation-standards-and-compliance/european-commission-proposes-revised-cybersecurity-act-to-boost-eu-cyber-resilience-secure-ict-supply-chains/). 21.01.2026).***

***

«Нове дослідження Advania UK показує, що середні організації у Великобританії все частіше займаються кібербезпекою самостійно, керуючись скоріше необхідністю, ніж власним вибором. Згідно з доповіддю «Building Core Resilience 2025», 65% середніх британських компаній зараз займаються кібербезпекою внутрішньо, часто без перевірки з боку третіх осіб. Ця зміна відображає зниження довіри до зовнішніх постачальників технологій: 40% IT-керівників вважають, що постачальники надають перевагу більшим корпоративним клієнтам і більше зосереджені на продажу продуктів, ніж на наданні

індивідуальних рішень. Лише 11% вважають, що постачальники дійсно діють в їхніх інтересах…

Незважаючи на увагу до зовнішніх загроз, внутрішні виклики, такі як плинність кадрів, брак кваліфікованих фахівців та невідповідність стратегій, вважаються найбільшими перешкодами для кібербезпеки. Як результат, організації переосмислюють рентабельність інвестицій у кібербезпеку, оскільки репутаційний збиток зараз вважається більш витратним, ніж технічне відновлення після порушень. Хоча щомісячні тренінги з кібербезпеки дещо збільшилися (з 22% до 32%), дві третини компаній все ще проводять навчання співробітників рідше. Advania підкреслює, що ефективна обізнаність з питань безпеки вимагає постійного керівництва та узгодження дій з боку керівництва в режимі реального часу, оскільки сама по собі технологія не може компенсувати внутрішні вразливості та недоліки в комунікації…» ***(Sarah Weston. UK mid-market firms take control of cybersecurity as vendor trust falls // A Intelligent Global Media Brand (https://www.intelligentciso.com/2026/01/22/uk-mid-market-firms-take-control-of-cybersecurity-as-vendor-trust-falls/). 22.01.2026).***

***

«Державний сектор Великобританії стикається з розширенням і ускладненням загроз, що зумовлено розвитком штучного інтелекту, геополітичною напруженістю та поглибленням цифрової залежності. Генеративний штучний інтелект спростив обман, уможлививши створення переконливих фейкових відео, які підривають традиційні методи перевірки особи. Як результат, організації переходять від епізодичної, периметральної безпеки до безперервної, багаторівневої довіри, де кожна взаємодія з високим ризиком, навіть відеодзвінки, вимагає перевірки в режимі реального часу. Ця зміна перетворює цифрову ідентифікацію з зручності на вимогу відповідності, роблячи перевірену, автентифіковану комунікацію необхідною для конфіденційності та можливості аудиту…

Вразливість ланцюгів постачання зараз вважається серйозним ризиком, оскільки порушення з боку третіх осіб можуть підірвати навіть найнадійніші внутрішні кіберстратегії. Інтеграція штучного інтелекту в розробку програмного забезпечення ще більше посилює цей ризик, створюючи загрозу масштабних інцидентів через скомпрометовані оновлення або репозиторії з відкритим кодом. Такі регуляторні заходи, як законопроект про кібербезпеку та стійкість, починають формалізувати відповідальність ланцюгів постачання, але їх виконання залишається складним завданням…

Ризик ідентифікації також стає центральним для національної інфраструктури, особливо з огляду на те, що квантові обчислення загрожують дестабілізувати криптографічну довіру. До 2026 року підготовка до постквантової криптографії стане стратегічним пріоритетом, оскільки критично важливі набори даних повинні залишатися надійними протягом десятиліть. Зближення штучного інтелекту та квантових обчислень обіцяє як оптимізацію, так і нові можливості для супротивників підірвати цифрову довіру.

Ризик для людей також зростає, оскільки очікується збільшення внутрішніх загроз через економічний тиск та доступність інструментів штучного інтелекту. Це спонукає до поновлення уваги до забезпечення ідентичності, включаючи більш сувору перевірку віддалених співробітників та громадян, оскільки Великобританія переходить до національної системи цифрової ідентифікації. Довіра громадськості до таких систем буде залежати від прозорості та надійних заходів забезпечення…

Загалом, державний сектор Великобританії зміщує акцент у сфері кібербезпеки з профілактики на стійкість, швидке виявлення та відновлення, визнаючи, що кібератаки є неминучими і що здатність швидко реагувати є визначальним фактором ефективної оборони». ***(Christine Horton. Cybersecurity and digital identity in 2026: Designing trust for a world built on deception // THINK Digital Partners (https://www.thinkdigitalpartners.com/news/2026/01/21/cybersecurity-and-digital-identity-in-2026-designing-trust-for-a-world-built-on-deception/). 21.01.2026).***

***

«Регламент ЄС щодо машин (MR), який набере чинності в січні 2027 року, представляє собою фундаментальну зміну в галузі промислової безпеки, оскільки робить кібербезпеку обов'язковою вимогою для всіх машин, що продаються в ЄС. На відміну від попереднього, це регулювання застосовується негайно у всіх державах-членах, усуваючи прогалини в обізнаності, коли багато виробників, особливо малі підприємства, недооцінюють необхідність дотримання вимог. Щоб отримати маркування CE, виробники машин тепер повинні розглядати безпеку як невід'ємну частину безпеки, проводячи оцінку ризиків кібербезпеки відповідно до нового гармонізованого стандарту EN50742. Хоча виробники несуть відповідальність за підтвердження стійкості, регулювання дозволяє задокументовану бездіяльність, якщо це виправдано, і модернізує дотримання вимог, дозволяючи повністю цифрову документацію…

Щоб вирішити цю проблему, експерти рекомендують підхід «безпека за замовчуванням», використовуючи такі компоненти, як приводи ACS380-E та PLC AC500 від ABB, які мають вбудовану кібербезпеку з самого початку, а не намагаються додати її пізніше. Це спрощує дотримання вимог і гарантує, що обладнання може протистояти сучасним загрозам. MR не є перешкодою для інновацій, а вважається рушієм прогресу, що формує довіру, необхідну для промислового Інтернету речей. Для виробників найважливішим першим кроком є проведення ретельної оцінки ризиків кібербезпеки, щоб довести належну обачність і забезпечити собі місце на ринку…» ***(Pekka Alasaari, Johanna Schüßler. Why the new Machinery Regulation is a wake-up call on cybersecurity // ABB (https://new.abb.com/news/detail/132811/why-the-new-machinery-regulation-is-a-wake-up-call-on-cybersecurity). 22.01.2026).***

***

«Китай різко розкритикував нову пропозицію Європейського Союзу щодо кібербезпеки, яка дозволить Брюсселю та державам-членам виключити «високоризикових» іноземних постачальників з таких критично важливих секторів, як телекомунікації, енергетика, водопостачання, хмарні та безпекові

послуги. Проект Закону про кібербезпеку, оприлюднений у вівторок в рамках більш широкої ініціативи ЄС щодо «стратегічної автономії» та зменшення ризиків економічного примусу, широко розглядається як спрямований проти китайських постачальників, причому гіганти 5G Huawei і ZTE опинилися в центрі уваги, а такі компанії, як Nuctech, Hikvision і виробник дронів DJI, як очікується, зіткнуться з тиском пізніше. Згідно з планом, Комісія та столиці країн ЄС спільно визначать «країни, що викликають занепокоєння» і вважаються кіберзагрозами, фактично закривши ключові ринки інфраструктури для їхніх постачальників технологій. Речник Європейської комісії Томас Регнієр заявив, що Європа «занадто довго» терпіла постачальників з високим рівнем ризику в стратегічних секторах…

Пекін відреагував гнівно. Речник міністерства закордонних справ Гуо Цзякунь засудив законопроект як «відвертий протекціонізм», стверджуючи, що він використовує «нетехнічні стандарти» та «не має фактичних доказів» для заборони китайським компаніям, і попередив, що Китай вживе «необхідних заходів» для захисту своїх компаній. Аналітики, такі як Тім Рюліг з Інституту досліджень безпеки ЄС, вважають цю заяву нечіткою погрозою, але зазначають, що можливості Китаю обмежені: він сильно залежить від експорту, США в основному закрили свій ринок для чутливих китайських технологій, а європейські компанії мають лише невелику частку стратегічних технологій у Китаї…» ***(Sam Clark. Beijing pledges to defend tech crown jewels against EU cyber rules // POLITICO (https://www.politico.eu/article/china-hit-back-eu-cyber-security-tech-bill/). 21.01.2026).***

***

«Навчання з питань кібербезпеки широко визнається як необхідна умова для забезпечення стійкості бізнесу, проте, згідно з опитуванням «2025 Cybersecurity Breaches Survey», лише 19% британських компаній проводять навчальні та інформаційні заходи. Незважаючи на регуляторні вимоги Закону ЄС про кіберстійкість, Директиви NIS2 та американського закону HIPAA, багато організацій стикаються з труднощами у впровадженні ефективного навчання через надмірну кількість варіантів та невизначеність щодо того, хто і яке навчання потребує…

Експерти сходяться на думці, що всі співробітники організації потребують навчання з питань кібербезпеки, але воно має бути адаптоване до їхніх посадових обов'язків. Усі співробітники повинні мати базові знання щодо виявлення фішингу, захисту облікових даних та повідомлення про підозрілу діяльність. Спеціалізоване навчання необхідне для таких відділів, як фінанси, кадрова служба та розробка, з акцентом на соціальну інженерію, захист даних, безпечне кодування та ризики ланцюга поставок. Керівні команди повинні розуміти стратегічні та фінансові наслідки порушень, а топ-менеджери, включаючи генеральних директорів, не повинні бути звільнені від навчання, оскільки вони є головними цілями для зловмисників.

Найефективнішим є практичне навчання на основі сценаріїв, таке як настільні вправи, симуляції та ігрові сесії, які допомагають сформувати стійкі звички та сприяють командній роботі. Технічний персонал отримує користь від практичних

лабораторних занять та змагань типу «захопи прапор», а керівництво та міжфункціональні команди — від симуляцій прийняття рішень в умовах стресу…

Навчання повинно бути безперервним, а нетехнічний персонал повинен проходити модулі підвищення кваліфікації кожні 6–12 місяців і регулярно брати участь у симуляціях фішингу. Команди з безпеки та IT повинні брати участь у щомісячних або щоквартальних навчаннях, а міжфункціональні команди повинні брати участь у щорічних навчаннях, що відтворюють реальні інциденти. Для співробітників, які потрапляють у пастку симуляцій фішингу, рекомендується навчання «just-in-time».

Найкращі практики включають сприяння культурі спільної відповідальності, забезпечення цікавого та актуального навчання, а також використання помилок як можливості для навчання, а не як приводу для звинувачень. Регулярне спілкування, наприклад щомісячні інформаційні бюлетені з практичними порадами, може зміцнити хороші звички як на роботі, так і вдома. Зрештою, ефективне навчання з питань кібербезпеки повинно дати кожному співробітнику можливість зрозуміти свою роль у захисті та впевнено реагувати на загрози, підтримуючи стійку організаційну культуру…» ***(Kate O'Flaherty. How can businesses make their cybersecurity training stick? // Future US, Inc. (https://www.itpro.com/security/how-businesses-can-make-cybersecurity-training-stick). 26.01.2026).***

***

Австралія та Нова Зеландія

«Кіберризик, який часто розглядають як суто технічну проблему, є, по суті, питанням управління, про що неодноразово свідчили серйозні порушення в таких австралійських компаніях, як Optus, Medibank і Latitude Financial. Хоча захист зазвичай зосереджується на брандмауерах і шифруванні, нові дослідження показують, що фінансові аудитори є тихою, вбудованою лінією захисту. Дослідження, в якому протягом 16 років було проаналізовано понад 2800 американських компаній, виявило чітку закономірність: аудитори, які раніше мали справу з клієнтом, що зазнав кіберзлочину, стали значно пильнішими щодо всіх інших своїх клієнтів, змінивши своє мислення від прийняття результатів роботи системи до активного питання щодо точності та цілісності контролю…

Зокрема, ці аудитори, які мали досвід порушення безпеки, на 21% частіше виявляли серйозні недоліки в системах і засобах контролю у клієнтів, які не зазнали порушення безпеки, причому виявлені недоліки часто були безпосередньо пов'язані з наглядом за технологіями та контролем доступу — сферами, що мають велике значення для кіберризиків. Важливо, що коли ці аудитори видавали позитивний висновок, ці компанії статистично рідше зазнавали кіберпорушень безпеки в подальшому, що підтверджує, що якість аудиту є надійним показником кіберстійкості. Опитані аудитори описали кардинальну зміну в мисленні, перехід від абстрактного поняття ризику до конкретного розуміння, яке можна застосувати до різних клієнтів, що змусило їх приділяти більше часу тестуванню засобів контролю та залученню IT-фахівців на більш ранніх етапах…

Хоча в дослідженні використовувалися дані США, його висновки є дуже актуальними для Австралії, де кіберзлочинність є швидко зростаючою загрозою, а регуляторний контроль з боку ASIC та APRA зробив кіберстійкість основною відповідальністю ради директорів. Оскільки глобальні компанії, такі як «Велика четвірка» (PwC, Deloitte, EY та KPMG), проводять аудит найбільших австралійських компаній, що котируються на біржі, та обмінюються методологіями на міжнародному рівні, висновки з зарубіжних порушень вже впливають на місцеву аудиторську практику. Хоча аудитори не є експертами з кібербезпеки, їхня незалежність, скептицизм та системний підхід забезпечують важливий рівень нагляду, що доповнює внутрішні засоби захисту. Дослідження показує, що якість аудиту є недооціненим аспектом кіберризику, що дає інвесторам сигнал: компанії, які проходять аудит фахівцями, що мають досвід у сфері порушень, статистично є більш захищеними. У міру ескалації кіберзагроз та збереження нестабільної довіри громадськості, постійна еволюція аудиторської професії може виявитися своєчасним захистом від майбутніх гучних випадків порушення безпеки даних». ***(Laura Hood. Research reveals a surprising line of defence against cyber attacks: accountants // The Conversation Media Group Ltd (https://theconversation.com/research-reveals-a-surprising-line-of-defence-against-cyber-attacks-accountants-272428). 19.01.2026).***

***

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

«З 1 січня 2026 року Китай вступив у нову, набагато суворішу фазу кіберрегулювання, внесли значні поправки до Закону про кібербезпеку, що кардинально змінило порядок виявлення, повідомлення та реагування організацій на інциденти, а також розширило можливості Пекіна карати за недотримання вимог як у країні, так і за кордоном. Для операторів мереж у Китаї або через Китай, включаючи іноземні компанії, що продають свою продукцію на китайському ринку або підключені до критичної інфраструктури Китаю через постачальників, повідомлення про інциденти тепер відбувається майже в режимі реального часу: про « особливо серйозні» події повинні повідомлятися протягом однієї години, а «відносно серйозні» інциденти, такі як порушення, що зачіпають понад мільйон осіб або спричиняють збитки понад 5 мільйонів юанів, повинні повідомлятися протягом чотирьох годин, після чого протягом 72 годин проводиться детальна оцінка, а протягом 30 днів — повний аналіз після інциденту. Ці терміни закріплені в нових національних заходах щодо повідомлення про інциденти, прийнятих Адміністрацією кіберпростору Китаю, які застосовуються до всіх операторів мереж у Китаї…

Водночас було різко збільшено штрафи та формалізовано особисту відповідальність. Серйозні порушення можуть призвести до накладення штрафів на підприємства у розмірі до 10 мільйонів юанів та на фізичних осіб у розмірі до 1 мільйона юанів, причому регуляторні органи тепер мають право накладати санкції

без попереднього вимагання виправлення ситуації. Ризик ланцюга поставок є явною мішенню: оператори критичної інфраструктури можуть бути оштрафовані на суму, що в 10 разів перевищує вартість придбання, за використання невідповідних продуктів або послуг. Екстериторіальна дія закону також була розширена і тепер поширюється на будь-яку іноземну діяльність, яка вважається «загрозою для мережевої безпеки Китаю», що відкриває можливість для таких заходів, як заморожування активів закордонних юридичних осіб. Вперше штучний інтелект офіційно включено до структури кібербезпеки: закон заохочує використання штучного інтелекту для посилення кіберзахисту та сигналізує, що алгоритмічні системи будуть підлягати етичному та безпековому нагляду. Детальні порогові значення тепер визначають, що вважається «особливо серйозним» інцидентом, включаючи перебої в роботі основних порталів або інфраструктури протягом декількох годин, перебої в наданні основних послуг для десятків мільйонів людей або порушення, що стосуються понад 100 мільйонів особистих записів. На практиці ці зміни змушують глобальні організації переглянути свої заходи безпеки з точки зору швидкості, документації, делегованих повноважень та доказів, готових для регуляторних органів, перетворюючи першу годину інциденту на юридично зобов'язуючий час для дотримання вимог, а не просто на час розслідування…» ***(Ashish Khaitan. China's New Cybersecurity Law Is Here — And It Changes Everything for Businesses // The Cyber Express LLC (https://thecyberexpress.com/china-cybersecurity-law-2026/). 02.01.2026).***

***

«Національна рада доходів (NBR) запустила Центр операцій безпеки Бангладеш (SOC) для посилення кібербезпеки та зниження ризиків для своєї цифрової інфраструктури, зокрема системи ASYCUDA та інших конфіденційних інформаційних активів.

SOC було створено в рамках реалізації політики кібербезпеки та рамки дотримання вимог, виданих Національним агентством з кібербезпеки (NCSA).

Новостворена SOC забезпечить цілодобовий (24/7) моніторинг, виявлення та запобігання потенційним внутрішнім та зовнішнім кібератак, ризикам, підозрілій діяльності та іншим кіберзагрозам у кіберпросторі митниці Бангладеш…

Ця ініціатива спрямована на покращення загального стану безпеки цифрових систем NBR та забезпечення захисту критично важливих даних, пов'язаних з доходами, в умовах зростаючих кіберзагроз». ***(NBR launches Security Operations Center (SOC) to strengthen cybersecurity // BSS (https://www.bssnews.net/business/347858). 04.01.2026).***

***

«Нова система кібербезпеки Гонконгу для критичної інфраструктури набула чинності 1 січня 2026 року з двома ключовими змінами: офіційним призначенням комісара з критичної інфраструктури (безпека комп'ютерних систем) та публікацією першого Кодексу практики (CoP) відповідно до Постанови про захист критичної інфраструктури (комп'ютерні системи)…

Постанова встановлює широкі законодавчі обов'язки для операторів «критичної інфраструктури» (CI). Кодекс поведінки перетворює ці обов'язки на детальні практичні вимоги та встановлює критерії, на основі яких комісар може видавати обов'язкові вказівки. Недотримання таких вказівок є правопорушенням, тому розуміння Кодексу поведінки є надзвичайно важливим, навіть якщо сам документ не є законодавчим актом…

Основні роз'яснення CoP

• Визначення «критичної комп'ютерної системи»: система підпадає під дію цього визначення, якщо її відмова може серйозно вплинути на основну функцію CI, якщо вона обробляє конфіденційні дані, необхідні для надання важливих послуг, або якщо вона тісно пов'язана з іншими CI. Промислові платформи управління/OT, такі як SCADA, прямо включені до цього визначення.

• План управління CSS: оператори CI повинні подати план, в якому викладено структури управління, методи управління ризиками та детальні технічні заходи контролю (управління активами, контроль доступу та привілейованого доступу, криптографія, встановлення виправлень, резервне копіювання/відновлення після аварій тощо).

• Підрозділ управління CSS: може бути внутрішнім або зовнішнім і очолюватися співробітником з визнаними кваліфікаціями в галузі безпеки (наприклад, CISSP, CISM).

• Альтернативні заходи контролю: якщо стандартні IT-заходи є недоцільними для IT, необхідно задокументувати еквівалентні заходи захисту…

• Повідомлення про зміни та інциденти: про істотні зміни в системі або «зміни оператора» необхідно повідомляти; про інциденти безпеки повідомляти необхідно лише в тому випадку, якщо незаконний доступ спричинив фактичні негативні наслідки. Кодекс поведінки містить зразки форм, приклади того, що є «істотним», та терміни (початкове усне повідомлення, письмовий звіт про першопричини тощо).

• Навчання з питань безпеки: навчання, запропоновані комісаром, проводитимуться в непродуктивних середовищах, але до них має бути залучено вище керівництво.

• Положення щодо ланцюга постачання: у додатку H рекомендуються положення контракту, що зобов'язують зовнішніх постачальників послуг.

Модель забезпечення дотримання

Комісар може видавати письмові вказівки з посиланням на Кодекс поведінки; їх недотримання є правопорушенням. Галузеві регулятори (наразі це НКМА та Управління з питань комунікацій) можуть публікувати додаткові кодекси для зобов'язань категорій 1 та 2.

Наступні кроки для операторів CI

Провести аналіз розбіжностей щодо CoP, посилити технічні заходи контролю, оновити політику, реструктурувати управління, переглянути контракти з постачальниками та підготувати необхідний план управління та процедури повідомлення. Оператори також повинні стежити за майбутніми галузевими кодексами, які можуть додати індивідуальні вимоги…

Запуск офісу комісара та CoP знаменує нову, більш чітку еру відповідальності за кібербезпеку в Гонконзі, приводячи місцеву практику у відповідність до стандартів ISO, NIST та регіональних стандартів і вимагаючи негайного планування дотримання вимог у всіх критично важливих секторах». ***(Albert Yuen and Kenny Tam. Decoding the Code of Practice: Hong Kong publishes guidelines on implementation of cybersecurity law // Eversheds Sutherland (https://www.eversheds-sutherland.com/en/global/insights/decoding-the-code-of-practice-hong-kong-publishes-guidelines-on-implementation-of-cybersecurity-law). 08.01.2026).***

***

«10 грудня 2025 року Національна асамблея В'єтнаму прийняла новий Закон про кібербезпеку № 116/2025/QH15, який набере чинності 1 липня 2026 року і замінить Закон про кібербезпеку 2018 року та Закон про кіберінформаційну безпеку 2015 року. Закон є значним переглядом цифрової правової бази В'єтнаму, що посилює контроль за контентом та захист критичних систем і користувачів. Він встановлює суворі терміни модерації контенту, вимагаючи від постачальників послуг видаляти незаконний контент протягом 24 годин після отримання запиту від Міністерства громадської безпеки або протягом 6 годин у термінових випадках. Він також посилює захист інформаційних систем, що вважаються критичними для національної безпеки, шляхом обов'язкового проведення постійних оцінок кібербезпеки, звітування та координації з робочими групами з кібербезпеки…

Закон чітко регулює нові технології, включаючи сувору заборону використання штучного інтелекту або інших нових технологій для підробки зображень, голосів або відео інших осіб з незаконною метою. Він додає конкретні заходи захисту для вразливих груп, вимагаючи від батьків або опікунів реєструвати онлайн-акаунти додаткових послуг для дітей, використовуючи їхні власні дані, та зобов'язуючи постачальників послуг застосовувати технічні заходи для фільтрування та запобігання шкідливому або експлуататорському контенту, спрямованому на дітей. Закон зберігає вимоги В'єтнаму щодо локалізації даних, але уточнює категорії даних, які повинні зберігатися, такі як імена облікових записів, час використання послуг, платіжна інформація, IP-адреси та пов'язані дані, а також строк зберігання після того, як користувач припинив користуватися послугою, з подальшими деталями, які будуть викладені в майбутньому урядовому декреті…» ***(Oliver Massmann. Vietnam - Law on cybersecurity 2026 - what you must know // Duane Morris LLP (https://blogs.duanemorris.com/vietnam/2026/01/08/vietnam-law-on-cybersecurity-2026-what-you-must-know/#page=1). 08.01.2026).***

***

«Китайські власті наказали вітчизняним компаніям припинити використання програмного забезпечення для кібербезпеки від близько десятка американських та ізраїльських постачальників, включаючи VMware, що належить Broadcom, Palo Alto Networks, Fortinet та Check Point Software Technologies, посилаючись на міркування національної безпеки. За словами

осіб, ознайомлених з цим рішенням, регуляторні органи попередили, що ці продукти можуть збирати та передавати конфіденційні дані за кордон, і доручили компаніям замінити їх на китайські аналоги. Невідомо, скільки компаній отримали це повідомлення, і ні Адміністрація кіберпростору Китаю, ні Міністерство промисловості та інформаційних технологій, ні згадані постачальники не відповіли на запити про коментарі. Цей крок є частиною більш широкої кампанії Пекіна, спрямованої на зменшення залежності від західних технологій на тлі ескалації напруженості між США і Китаєм з приводу торгівлі та технологічної переваги, і є продовженням багаторічних зусиль Китаю щодо заміни іноземного обладнання та програмного забезпечення на продукти вітчизняних постачальників, таких як 360 Security Technology і Neusoft…

Заборона також збігається з підготовкою Вашингтона і Пекіна до візиту президента США Дональда Трампа до Китаю і відбувається на тлі взаємної підозри щодо кібербезпеки. Західні компанії та уряди неодноразово звинувачували пов'язаних з китайською державою суб'єктів у хакерських атаках; компанія Palo Alto нещодавно повідомила про китайську кампанію, спрямовану проти дипломатів у всьому світі, а Check Point детально описала ймовірне вторгнення, пов'язане з Китаєм, до європейського урядового відомства, що Китай заперечує. Водночас китайські аналітики стверджують, що будь-який західний продукт у сфері безпеки — особливо від компаній, у яких часто працюють ветерани розвідки і які тісно пов'язані з установами національної оборони — теоретично може бути використаний для шпигунства або саботажу, з огляду на його глибокий доступ до корпоративних мереж і пристроїв. Компанії, на які поширюється заборона, мають значну присутність у Китаї, маючи численні офіси на материку, а також у Гонконзі та Макао, що підкреслює, наскільки руйнівним може бути цей наказ. Цей крок вписується в більш широку схему взаємної недовіри в галузі технологій: наприклад, Ізраїль заборонив китайські автомобілі на військових базах через побоювання щодо стеження і, як повідомляється, обмежив їх використання старшими офіцерами, підкресливши, як кібербезпека та безпека ланцюгів постачання стали центральними точками геополітичного протистояння обох сторін». ***(Beijing tells local firms to stop using US, Israeli cybersecurity software // The Times of Israel (https://www.timesofisrael.com/beijing-tells-local-firms-to-stop-using-us-israeli-cybersecurity-software/). 14.01.2026).***

***

«Акції декількох великих компаній, що займаються кібербезпекою, впали в середу після того, як агентство Reuters повідомило, що китайська влада наказала вітчизняним компаніям припинити використання продуктів приблизно десятка американських та ізраїльських постачальників програмного забезпечення з міркувань національної безпеки. Акції Palo Alto Networks, Fortinet і Broadcom, яка володіє VMware, торгувалися з пониженням, як і акції ізраїльської компанії Check Point Software Technologies, однієї з названих фірм. Хоча повний список постачальників, яких це стосується, ще не оприлюднено, акції інших відомих американських постачальників послуг у сфері кібербезпеки,

що працюють в Азії, таких як CrowdStrike, Cloudflare і Zscaler, також дещо знизилися в ході передринкових торгів…

Заборона була введена на тлі загострення конкуренції між США і Китаєм у сфері передових технологій, особливо в області напівпровідників, пов'язаних з штучним інтелектом. На початку цього тижня Вашингтон дозволив компанії Nvidia експортувати до Китаю свої менш потужні чіпи H200 на певних умовах після попередньої заборони на експорт, але, за повідомленнями, китайські власті все одно доручили митникам блокувати імпорт цих чіпів. Конфронтація також поширюється на критично важливі сировинні матеріали, оскільки США скликали міністрів фінансів розвинених економік у Вашингтоні для обговорення питання зменшення залежності від китайських поставок рідкісних елементів, необхідних для електромобілів, побутової електроніки та оборонних систем. Хоча ринок кібербезпеки США залишається набагато більшим — за прогнозами, цього року він становитиме близько 81,61 млрд доларів — ринок Китаю, за прогнозами, досягне 13,03 млрд доларів у 2026 році, а ширший Азіатсько-Тихоокеанський регіон, як очікується, буде найшвидше зростаючим ринком кібербезпеки до 2034 року. Азіатсько-Тихоокеанський регіон вже становить значну, хоча і меншу частину доходів провідних американських компаній у сфері кібербезпеки, тому будь-які тривалі обмеження їхнього доступу до китайських клієнтів можуть мати як негайні наслідки для фондового ринку, так і довгострокові стратегічні наслідки». ***(Solomon Oladipupo. AVGO, PANW, FTNT: Cybersecurity Stocks Hit as China Cracks Down on U.S., Israeli Software // TipRanks (https://www.tipranks.com/news/avgo-panw-ftnt-cybersecurity-stocks-hit-as-china-cracks-down-on-u-s-israeli-software). 14.01.2026).***

***

«Координаційний міністр Індонезії з політичних питань та питань безпеки Джамарі Чаніаго оголосив кібербезпеку національною необхідністю, а не опцією, підкресливши її роль як основи безпеки даних та захисту від інформаційних атак. Виступаючи на засіданні Національного агентства з кібербезпеки та криптографії (BSSN) Executive Town Hall 2026 у місті Депок, Західна Ява, Чаніаго наголосив, що кібербезпека є «абсолютною передумовою для збереження політичної стабільності, національної безпеки та сталого розвитку». Він попередив, що кіберзагрози розвиваються швидше, ніж нормативно-правова база, що вимагає адаптивних підходів для передбачення нових небезпек…

Ситуація з загрозами у 2026 році буде безпрецедентно складною. Атаки, що базуються на штучному інтелекті, квантових обчисленнях та фейкових відео, призначених для масової дезінформації, посилять виклики. Чаніаго закликав персонал BSSN швидко реагувати на глобальні виклики у сфері кібербезпеки та будувати міцну національну оборону шляхом взаємної співпраці та націоналістичної відданості. «Я закликаю весь персонал і рядових співробітників BSSN продовжувати служити стратегічною охороною нації», — сказав він. На підтримку цього мандату BSSN і Міністерство національного планування розвитку підписали в грудні 2025 року угоду про співпрацю з метою посилення розвитку людських ресурсів через освіту, навчання та ініціативи з підвищення компетентності в галузі кібербезпеки та криптографії, оснащуючи кіберперсонал

Індонезії для протистояння новим загрозам». ***(Cybersecurity strengthens national defense against information attacks // ANTARA (https://en.antaranews.com/news/400586/cybersecurity-strengthens-national-defense-against-information-attacks). 20.01.2026).***

***

«Філіппіни стикаються з наростаючою і нагальною кризою в галузі кібербезпеки, яка становить більшу безпосередню загрозу, ніж морські напруження в Південно-Китайському морі. У листопаді 2023 року компанія Palo Alto Networks визначила китайську групу Stately Taurus, що фінансується державою, як відповідальну за п'ятиденне проникнення в філіппінське урядове агентство, що збіглося з морськими зіткненнями між Китаєм і Філіппінами, підкресливши, як кібероперації відповідають стратегічним інтересам Пекіна. Незважаючи на складнощі з визначенням винних, масштаби кіберзлочинів на Філіппінах є тривожними: лише у третьому кварталі 2023 року було зламано понад 60 000 облікових записів користувачів, що поставило країну в число 30 найбільш уразливих у світі. Серед найсерйозніших інцидентів — витік даних з Філіппінської корпорації медичного страхування та пошкодження вебсайту Палати представників…

Засоби захисту кібербезпеки Філіппін мають серйозний дефіцит ресурсів, а урядова команда з реагування на кіберзагрози налічує лише 35 членів — кількість, яку експерти вважають небезпечно недостатньою. Через обмежені людські ресурси команда покладається на колишніх хакерів для отримання інформації про загрози, а фінансові обмеження не дозволяють розширити команду до ідеального розміру в близько 200 осіб. Низькі зарплати в урядових установах ускладнюють залучення та утримання кваліфікованих фахівців з кібербезпеки, що підтверджується дослідженням, фінансованим Агентством США з міжнародного розвитку. Визнаючи серйозність загрози, філіппінські військові на чолі з начальником штабу генералом Ромео Браунером-молодшим оголосили про плани набору додаткових кіберфахівців для протидії майже постійним атакам з боку невідомих іноземних суб'єктів…» ***(Philippines Enlists Hackers Amid US Warnings of China Cyber Threats // Maritime Fairtrade (https://maritimefairtrade.org/philippines-enlists-hackers-amid-us-warnings-of-china-cyber-threats/). 24.01.2026).***

***

Ізраїль, Туреччина та країни Близького сходу

«Національний орган з питань кібербезпеки Саудівської Аравії (NCA) видав «Заходи контролю кібербезпеки для приватних суб'єктів господарювання, що не належать до критичної національної інфраструктури» (далі — «Заходи контролю»), в яких встановлено обов'язкові базові та детальні вимоги для приватних суб'єктів господарювання, що не належать до критичної національної інфраструктури, з метою зміцнення національної безпеки та забезпечення безпечної цифрової економіки.

Заходи застосовуються до двох категорій: (A) великі підприємства (250+ штатних співробітників або річний дохід понад 200 000 000 саудівських ріалів) та (B) малі та середні підприємства (6–249 штатних співробітників або річний дохід від 3 000 000 до 200 000 000 саудівських ріалів).

Нові заходи контролю адаптовані до розміру підприємства за трьома компонентами: управління, захист кібербезпеки та кібербезпека сторонніх ресурсів і хмарних обчислень.

Основні заходи захисту включають захист кінцевих точок, класифікацію даних, управління резервним копіюванням та періодичне тестування на проникнення. Заходи контролю також вимагають створення спеціальної керівної функції з кібербезпеки для кожного підприємства.

Хоча заходи контролю не визначають, до якого терміну компанії повинні забезпечити відповідність вимогам, ми радимо суб'єктам господарювання, що підпадають під дію цих заходів, розпочати оцінку своїх поточних заходів контролю відповідно до базових вимог, визначити пріоритетність обов'язкових елементів за категоріями та розробити план виправлення, що враховує вимоги до управління, технічні вимоги та вимоги до сторонніх осіб/хмарних обчислень, з документованими робочими процесами перевірки та звітності». ***(Jana Mrad, Nadim Bardawil. Saudi Arabia Issues New Non-CNI Cybersecurity Controls for the Private Sector // BSA LAW (https://www.bsalaw.com/insight/saudi-arabia-issues-new-non-cni-cybersecurity-controls-for-the-private-sector/). 01.01.2026).***

***

«Катар готується до стрімкого зростання ринку кібербезпеки, оскільки швидка цифровізація, ширше впровадження хмарних технологій та зростання кіберзагроз посилюють необхідність захисту критичної національної інфраструктури та конфіденційних даних. Уряд — через Національний комітет з кібербезпеки та посилення нормативно-правового регулювання — стимулює попит на передові рішення для захисту електростанцій, нафтогазових об'єктів, фінансових та водних систем. Міжнародні аналітики стверджують, що зростаючі інвестиції країни в цифрову трансформацію, штучний інтелект та кібербезпеку (ринок, який, за прогнозами, до 2030 року досягне майже 20 мільярдів доларів) перетворюють Катар на регіональний центр інновацій. Такі ініціативи, як Cyber Security Services Framework Катарського фінансового центру, приваблюють глобальних постачальників до створення місцевих підрозділів, що ще більше зміцнює цей сектор… У міру поширення автоматизованих, програмно-керованих процесів у різних галузях промисловості, підприємства стикаються з більш широкою площиною атак, що робить необхідними постійні витрати на засоби безпеки, таланти та дослідження і розробки. Дослідницька компанія 6Wresearch прогнозує стабільне розширення ринку, при цьому кібербезпека залишиться основою стратегії технологічного зростання Катару в найближчі роки». ***(Joel Johnson. Qatar's cybersecurity market poised for robust growth amid digital push // The Peninsula (https://thepeninsulaqatar.com/article/05/01/2026/qatars-cybersecurity-market-poised-for-robust-growth-amid-digital-push). 05.01.2026).***

***

«Ізраїль готується прийняти свій перший постійний закон про кібербезпеку, який замінить тимчасові надзвичайні правила, що регулювали діяльність Національного кібердиректорату Ізраїлю (INCD) протягом десятиліття. Запропонований закон спрямований на вирішення нагальної потреби захистити критичну інфраструктуру від таких супротивників, як Іран і Хамас, особливо з огляду на те, що Ізраїль став третьою країною у світі за кількістю кібератак. Центральною і суперечливою особливістю законопроекту є вимога до «критичних» приватних і урядових установ повідомляти про кібератаки в режимі реального часу, якщо існує «потенційна серйозна шкода», що є більш суворим стандартом, ніж 24-72-годинний термін, який є звичним в інших демократичних країнах. Хоча це має на меті запобігти поширенню атак, це викликає занепокоєння з приводу конфіденційності та бізнесу, яке закон намагається збалансувати, вимагаючи щорічних звітів про нагляд до Кнесету. Після років невдалих спроб попередників узгодити «національний» закон між різними органами безпеки, нинішній глава INCD Йосі Караді очолює цю ініціативу, стверджуючи, що законодавство є необхідним для національної стійкості, дозволяє швидше реагувати на загрози та встановлює обов'язкові стандарти захисту для 400-600 організацій, які зараз вважаються критично важливими…» ***(YONAH JEREMY BOB. Israel moves forward with potential game-changing cyber law // Jpost Inc (https://www.jpost.com/israel-news/politics-and-diplomacy/article-884510). 25.01.2026).***

***

Країни Африки

«Південна Африка стикається з серйозною та зростаючою кіберзагрозою, про що свідчить 37% зростання кількості атак у 2024 році, що значно перевищує глобальне зростання на 30%. Ця вразливість була підкреслена наприкінці січня 2025 року, коли національна метеорологічна служба була відключена від мережі внаслідок кібератаки, яка порушила роботу її електронної пошти, веб-сайту та важливих авіаційних і морських прогнозів, що вплинуло на інші країни, які залежать від цих послуг. Як найбільш підключена до мережі країна континенту, Південна Африка стала основною мішенню, а організації та урядові установи зазнають в середньому 1450 атак на тиждень…

Ці атаки все частіше спрямовані на критичну інфраструктуру. Нещодавно гучні злами торкнулися Національної служби лабораторних досліджень у галузі охорони здоров'я (припинення аналізу крові), Комісії з питань компаній та інтелектуальної власності, а також найбільшого пенсійного фонду Африки — Пенсійного фонду державних службовців. Навіть Державне агентство безпеки зазнало зломів. Міністр Кхумбудзо Нтшавені визнав «експоненціальне зростання» кількості атак і пообіцяв посилити можливості та прискорити впровадження десятирічної Національної програми кібербезпеки…

Однак критики стверджують, що кібербезпека постійно недооцінюється як пріоритет. Експерти закликають до збільшення стратегічних інвестицій, зазначаючи, що хоча Південна Африка ще не зіткнулася з «справді руйнівною атакою», це «лише питання часу». Рішення вимагає комплексного національного підходу до захисту критичної інфраструктури в поєднанні з обов'язковим навчанням користувачів, оскільки більшість атак починається з обману окремих інтернет-користувачів». ***(South Africa faces increased cyberattacks against government agencies // DefenceWeb (https://defenceweb.co.za/cyber-defence/south-africa-faces-increased-cyberattacks-against-government-agencies/). 02.01.2026).***

***

«Опитування, проведене наприкінці 2025 року серед понад 1000 керівників служб внутрішнього аудиту в 39 африканських країнах, опубліковане під назвою «Africa Risk in Focus 2026» Фондом внутрішнього аудиту та Африканською федерацією інститутів внутрішніх аудиторів, показує, що кіберінциденти є основним бізнес-ризиком для африканських компаній у 2026 році. Загалом 62% респондентів визнали кібератаки, такі як порушення безпеки даних, шкідливе програмне забезпечення та програми-вимагачі, головним викликом для бізнесу на континенті, а 60% заявили, що кіберризики є головним пріоритетом для внутрішнього аудиту. Найбільше занепокоєння спостерігається у Східній Африці (65%), Південній Африці (64%) та Північній Африці (64%), тоді як у Центральній Африці (32%) та Західній Африці (53%) рівень занепокоєння нижчий, проте кіберзлочинність впливає на всі регіони в умовах швидкого зростання штучного інтелекту та мобільних фінансових технологій. За оцінками, у 2023 році кібератаки коштували Африці близько 10 мільярдів доларів, і в звіті зазначається, що інструменти на основі штучного інтелекту роблять атаки більш витонченими і важкими для виявлення, а обмежена обізнаність про кібербезпеку, нижчий рівень грамотності в деяких районах та прогалини в законодавстві про кібербезпеку та захист даних збільшують ризики…

Після кіберризиків на другому місці знаходиться стійкість бізнесу (49%), а «цифрові зриви» піднялися на третє місце з 44%, що значно перевищує 10% у попередньому році, що відображає прискорення темпів технологічних змін; в результаті, два з трьох найбільших ризиків, які сприймаються африканськими підприємствами, зараз пов'язані з технологіями. Фінансовий ризик та ризик ліквідності також займають чільне місце з 43% — вище за середній світовий показник 31% — через залежність від іноземних інвестицій та зовнішнього фінансування, що посилюється волатильністю валютних курсів у декількох країнах». ***(Cyber risks top concerns for African businesses in 2026 report // Mediamania. (https://www.ecofinagency.com/news-digital/1201-51832-cyber-risks-top-concerns-for-african-businesses-in-2026-report). 12.01.2026).***

***

«Національне агентство Камеруну з інформаційних та комунікаційних технологій (ANTIC) отримало нове програмне та апаратне забезпечення на суму приблизно 735 мільйонів камерунських франків (1,3 мільйона доларів

США) для зміцнення інфраструктури кібербезпеки країни. Ця інвестиція, що є частиною фінансуваного Світовим банком Проекту прискорення цифрової трансформації Камеруну (PATNUC), має на меті посилити команду ANTIC з реагування на комп'ютерні інциденти (CIRT) за допомогою сучасних систем виявлення та запобігання вторгненням, серверів, консолей зберігання даних, платформ для розслідувань та інструментів сканування вразливостей…

З січня 2024 року ANTIC виявила понад 8500 вразливостей під час аудитів безпеки в державному та приватному секторах. Нова технологія покращить здатність CIRT проактивно реагувати на кібератаки, спрямовані на критичну інфраструктуру, оскільки наразі вона обробляє 200 ГБ даних щодня та обробляє майже 200 термінових запитів по всій країні. Модернізовані системи також розширять можливості CIRT у боротьбі з кіберзлочинністю, яка є постійною проблемою в процесі цифрової трансформації Камеруну…

Цей крок відображає більш широку тенденцію в Африці, де такі країни, як Буркіна-Фасо, також інвестують у кібербезпеку з метою захисту критичної цифрової інфраструктури та зміцнення цифрового суверенітету. Зусилля ANTIC мають ключове значення для цифрової трансформації Камеруну, забезпечуючи цифрову безпеку та довіру завдяки безпечному онлайн-середовищу та надійній інфраструктурі відкритих ключів». ***(Ayang Macdonald. Cameroon deploys cybersecurity system to protect DPI, boost digital trust // Biometrics Research Group, Inc. (https://www.biometricupdate.com/202601/cameroon-deploys-cybersecurity-system-to-protect-dpi-boost-digital-trust). 27.01.2026).***

***

Кіберстрахування

«Згідно з прогнозом Gallagher's 2026 Cyber Insurance Market Outlook, світовий ринок кіберстрахування майже потроїться в розмірах, зростаючи з приблизно 16-20 млрд доларів у 2025 році до 30-50 млрд доларів до 2030 року. Хоча Північна Америка все ще домінує, очікується, що Азіатсько-Тихоокеанський регіон буде лідирувати за темпами зростання завдяки швидкій цифровізації. Ціни стабілізувалися для більшості секторів, хоча в галузі охорони здоров'я продовжують зростати тарифи через підвищену активність страхових виплат…

Ситуація з загрозами характеризується посиленням серйозності, незважаючи на зменшення кількості заяв про збитки: середня вартість окремих інцидентів, пов'язаних з програмним забезпеченням-вимагачем, зросла на 17% у першій половині 2025 року, що становить 91% від загальної суми заяв про збитки, навіть незважаючи на те, що кількість заяв про збитки зменшилася на 53%. Середня вартість порушення безпеки даних у США у 2025 році досягла 10 мільйонів доларів. Зловмисники переходять від шифрування даних до чистого викрадення даних і вимагання викупу, хоча рівень виплат викупу знизився з 37% до 28–32%, а середня сума виплат впала до 1,2–1,8 мільйона доларів. Серед основних загроз — віддалені працівники Північної Кореї, Scattered Spider та пов'язана з Китаєм Salt Typhoon. Порушення безпеки ланцюга поставок також є провідним фактором у

нових збитках, пов'язаних з штучним інтелектом, і становить 30% від усіх зареєстрованих інцидентів, пов'язаних зі штучним інтелектом…

У відповідь на це регуляторне середовище стає все більш жорстким: у травні 2026 року набуває чинності Закон США про повідомлення про кіберінциденти для критичної інфраструктури (CIRCIA), який вимагає повідомлення про інциденти протягом 72 годин. Перевізники адаптуються, вдосконалюючи формулювання полісів щодо непередбачених перебоїв у діяльності та впроваджуючи окремі поліси або додаткові умови щодо штучного інтелекту для покриття витрат, таких як перенавчання великих навчальних моделей». ***(Kenneth Araullo. Global cyber insurance market could hit new highs by 2030, Gallagher forecasts // KM Business Information US, Inc (https://www.insurancebusinessmag.com/us/news/cyber/global-cyber-insurance-market-could-hit-new-highs-by-2030-gallagher-forecasts-562203.aspx). 16.01.2026).***

***

«Кіберстрахування часто розглядається як запорука безпеки для юридичних фірм та організацій, які стикаються з загрозами кібербезпеки, але реальність є набагато складнішою та ризикованішою. Згідно з доповіддю Delinea «Дослідження кіберстрахування 2025», формулювання полісів містять безліч винятків, обмежень та умов, які можуть легко призвести до втрати страхового покриття. Багато компаній помилково вважають, що вони повністю захищені, але лише 33% опитаних полісів покривають втрачені доходи, а менше половини покривають послуги з реагування на інциденти або викуп. Це залишає організації вразливими до значних втрат, особливо з огляду на те, що 77% респондентів повідомили про інциденти кібербезпеки, що сталися протягом останнього року…

Страхові компанії все частіше вимагають надійних засобів контролю безпеки, таких як управління ідентифікацією, авторизація та політика щодо паролів, як обов'язкову умову для надання страхового покриття. Недотримання цих засобів контролю або такі помилки, як людська помилка, неправильна конфігурація або затримка у повідомленні, можуть призвести до відмови у виплаті страхового відшкодування або анулювання полісу. Фактично, 45% респондентів заявили, що їхні поліси можуть бути анульовані через неналежні засоби контролю безпеки…

Розвиток штучного інтелекту (ШІ) створює додаткові складнощі, оскільки 42% полісів не покривають збитки, пов'язані з неправомірним використанням ШІ або відповідальністю за нього. Оскільки юристи та інші фахівці все частіше використовують генеративні інструменти ШІ, компанії повинні впровадити надійні правила навчання та використання ШІ, щоб уникнути непередбачених зобов'язань.

Щоб вирішити ці проблеми, керівництво компанії повинно ретельно переглянути та зрозуміти свої поліси кіберстрахування, виявити виключення та прогалини, а також забезпечити наявність усіх необхідних засобів контролю безпеки. Щорічні аудити полісів за участю ІТ-експертів та страхових фахівців є надзвичайно важливими, як і постійна співпраця з керівництвом компанії з метою визначення пріоритетності інвестицій у безпеку. Зрештою, ніколи не слід розраховувати на повне покриття — кіберстрахування є складною сферою, яка

постійно розвивається і вимагає проактивного управління та постійного контролю…» ***(Stephen Embry. Think You Are Covered? Better Read Your Cybersecurity Policy — Carefully // Breaking Media, Inc. (https://abovethelaw.com/2026/01/think-you-are-covered-better-read-your-cybersecurity-policy-carefully/). 27.01.2026).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«…Супротивники Америки — Китай, Росія, Іран і Північна Корея — посилюють свої наступальні кібероперації, націлені на критичну інфраструктуру, федеральні системи, лікарні, школи та глобальну торгівлю. Поки ці країни крадуть дані, встановлюють шкідливі програми та готуються до майбутніх зривів, США відстають у кіберзахисті. Створена в 2019 році, Комісія з кіберпростору отримала завдання запобігти кіберкатастрофі та розробила комплексну стратегію зі 116 практичними рекомендаціями, які спочатку посилили федеральну кіберполітику. Однак сьогодні країна стикається зі стратегічним дрейфом: можливості кібербезпеки вичерпуються, співпраця між державним і приватним секторами слабшає, федеральне керівництво нестабільне, а міжнародна координація хитається…

Щоб зупинити цей спад, необхідні негайні та стійкі дії. По-перше, Агентство з кібербезпеки та безпеки інфраструктури (CISA) повинно отримати стабільне керівництво, затверджене Сенатом, та багаторічне фінансування для вирішення проблеми втрати кадрів та зростання загроз. По-друге, криза федеральних кадрів у сфері кібербезпеки повинна розглядатися як надзвичайна ситуація в галузі національної безпеки; застарілі практики найму повинні бути реформовані, а успішні програми, такі як CyberCorps: Scholarship for Service, повинні бути розширені для залучення та утримання талантів. По-третє, необхідно пожвавити співпрацю між державним і приватним секторами шляхом відновлення таких каналів, як Консультативна рада з питань партнерства в галузі критичної інфраструктури, та розширення Закону про обмін інформацією з питань кібербезпеки для сприяння обміну інформацією про загрози. Нарешті, США повинні відновити свою кібердипломатію шляхом призначення та затвердження посла з особливих доручень з питань кіберпростору та цифрової політики, відновлення Бюро з питань кіберпростору та цифрової політики Державного департаменту та збільшення фінансування міжнародних зусиль з нарощування потенціалу…

Як попередила Комісія Solarium у 2020 році, Америка не може собі дозволити чекати катастрофічного кіберінциденту, щоб вжити заходів. Поки ще можлива двопартійна підтримка, Конгрес повинен скористатися нагодою для зміцнення національної кіберзахисту, перш ніж буде запізно». ***(Jim Langevin, Mark Montgomery. Time to restore America's cyberspace security system // CyberScoop (https://cyberscoop.com/us-cyber-defense-falling-behind-cisa-leadership-funding-op-ed/). 05.01.2026).***

***

«Президент Дональд Трамп у суботу натякнув, що США, можливо, використовували кібератаки або інші передові технічні можливості, щоб занурити Каракас у темряву під час військової операції, яка призвела до захоплення президента Венесуели Ніколаса Мадуро. Виступаючи в Мар-а-Лаго, Трамп заявив, що «певні знання» призвели до широкомасштабних відключень електроенергії у столиці Венесуели, описавши ситуацію як «темну і смертельну». Якщо це підтвердиться, це буде одним з найвідкритіших випадків використання кіберможливостей США проти іноземної держави — сфери, в якій США є світовим лідером і операції зазвичай є секретними…

Генерал Марк Міллі (не Ден Кейн), голова Об'єднаного комітету начальників штабів, заявив під час тієї ж прес-конференції, що Кіберкомандування США, Космічне командування США та інші бойові командування «почали застосовувати різні заходи» для забезпечення проведення операції, хоча він не уточнив, про які саме заходи йдеться. Білий дім, Кіберкомандування та Космічне командування відмовилися коментувати повідомлення про кібероперації…» ***(Maggie Miller. Trump suggests US used cyberattacks to turn off lights in Venezuela during strikes // POLITICO LLC (https://www.politico.com/news/2026/01/03/trump-venezuela-cyber-operation-maduro-00709816). 03.01.2026).***

***

«…Згідно з доповіддю Національного бюро безпеки Тайваню, у 2024 році кількість кібератак, спрямованих проти уряду острова, зросла більш ніж удвічі — до 2,4 мільйона інцидентів на день, причому більшість з них пов'язана з діяльністю китайських кібервійськ. Цей стрибок підкреслює, як кіберпростір став центральною ареною напруженості між Китаєм і Тайванем, слугуючи ключовим компонентом стратегії Пекіна «сірої зони утисків» — дій, спрямованих на виснаження оборони Тайваню та підривання довіри громадськості без початку відкритої війни…

У звіті детально описано значне зростання як обсягу, так і складності атак порівняно з 1,2 мільйонами щоденних атак, зафіксованих у 2023 році. Хоча багато вторгнень було заблоковано, сама наполегливість вказує на більш складне середовище загроз. Атаки поширилися за межі урядових мереж і спрямовані на критичну інфраструктуру, включаючи телекомунікації, транспорт і оборонні системи. Тактика еволюціонувала від простих розподілених атак типу «відмова в обслуговуванні» (DDoS) до складних постійних загроз, програмного забезпечення «бекдор» і соціальної інженерії, спрямованих на викрадення конфіденційних даних у державних службовців…

Важливо, що бюро зазначило, що ці кібероперації часто синхронізуються з китайськими військовими навчаннями, такими як «Joint Sword – 2024A і B», щоб посилити залякування та перешкодити реагуванню на надзвичайні ситуації в періоди підвищеної напруженості. Поки Пекін продовжує заперечувати свою причетність, незважаючи на глобальні звинувачення в кібершпигунстві, Тайвань попереджає, що захист від цього невпинного цифрового тиску вимагає постійної адаптації та міжнародної співпраці». ***(China Launched 2.4M Daily Cyberattacks on***

Taiwan in 2024 // TechnologyAdvice (https://www.techrepublic.com/article/news-china-cyberattacks-taiwan/). 05.01.2026).

***

«У грудні 2025 року пов'язана з Іраном хакерська група Handala заявила, що повністю зламала мобільні пристрої двох відомих ізраїльських політичних діячів, включаючи колишнього прем'єр-міністра Нафталі Беннета, опублікувавши понад 200 ГБ нібито внутрішніх даних. Однак аналіз, проведений дослідниками кіберрозвідки Kela, виявив більш обмежений масштаб, підтвердивши, що злом був спрямований конкретно на акаунти Telegram, а не на повний доступ до пристроїв. Виявлено, що витік даних складався переважно з порожніх контактних карток, лише близько 40 розмов містили фактичні повідомлення, що підтверджує походження даних із серверів Telegram…

Цей інцидент висвітлює серйозні вразливості в безпеці облікових записів, які, ймовірно, були досягнуті без повного компрометації пристрою. Handala, ймовірно, використовувала складні методи, такі як підміна SIM-карт або використання слабких місць протоколу SS7 для перехоплення кодів підтвердження входу, складні фішингові кампанії або перехоплення сеансів шляхом копіювання файлів аутентифікації Telegram Desktop для обходу багатофакторної аутентифікації. Стандартні налаштування Telegram посилили ризик, оскільки функція хмарного пароля є опціональною, а стандартні чати не мають наскрізного шифрування. Handala, яка з'явилася наприкінці 2023 року і постійно націлена на ізраїльські організації, за оцінками, має мотивацію, що підтримується державою або симпатизує державі, і ця кампанія підкреслює критичні прогалини в управлінні безпекою облікових записів на платформах шифрованого обміну повідомленнями…» ***(Tushar Subhra Dutta. Handala Hackers Targeted Israeli Officials by Compromising Telegram Accounts // Cyber Security News (https://cybersecuritynews.com/handala-hackers-targeted-israeli-officials/). 02.01.2026).***

***

«Дослідники з компанії Cyfirma, що спеціалізується на кібербезпеці, виявили нову шпигунську операцію APT36 («Transparent Tribe»), групи, пов'язаної з Пакистаном, яка шпигує за індійськими цілями принаймні з 2013 року. Остання кампанія передбачає доставку двох спеціальних імплантів, «ReadOnly» і «WriteOnly», за допомогою фішингових повідомлень, що містять ZIP-файли, замасковані під PDF-файли. Після відкриття шкідливе програмне забезпечення непомітно встановлюється, адаптуючи свою поведінку до будь-якого антивірусного продукту, а потім надає повні функції віддаленого керування: захоплення екрана, моніторинг та заміна буфера обміну (що дозволяє, наприклад, викрасти криптовалюту), витік даних та віддалений доступ до робочого столу…

Cyfirma відзначає, що APT36 вдосконалила свої методи роботи: тепер вона зловживає надійними компонентами Windows, використовує поширені формати документів для введення в оману та застосовує багатоетапне, переважно безфайлове виконання, щоб уникнути виявлення. Мета, як видається, полягає в

довгостроковому спостереженні за індійськими урядовими, військовими, академічними та стратегічними організаціями, що відповідає державній політиці збору розвідувальної інформації, а не швидкому фінансовому зиску.

APT36 перетинається з іншою організацією, пов'язаною з Пакистаном, «Cosmic Leopard», і раніше націлювалася на об'єкти в близько 30 країнах, але її основним напрямком діяльності залишається Індія». ***(Daryna Antoniuk. Pakistan-linked hackers target Indian government, universities in new spying campaign // Recorded Future News (https://therecord.media/pakistan-linked-hacking-group-targets-indian-orgs). 02.01.2026).***

***

«Кампанія Ірану з метою перешкоджання роботі Starlink в країні переросла з простого глушіння в те, що дослідники описують як безпрецедентну електронну війну на державному рівні проти споживчого супутникового інтернету. Всього через кілька годин після повідомлень місцевої групи NasNet про те, що втрата пакетів від перешкод у Тегерані значно покращилася — з приблизно 35% до близько 10% — кіберслідчий Наріман Гаріб опублікував те, що він називає першим задокументованим технічним доказом урядового GPS-спуфінгу, спрямованого проти терміналів Starlink. Телеметрія з пристрою Starlink в Ірані показала, що кілька сфальсифікованих GPS-сигналів перевантажували пристрій і його вбудовані засоби протидії, виводячи з ладу електронне керування. Хоча термінал технічно залишався в мережі, а загальна втрата пакетів становила лише близько 20%, пропускна здатність була різко обмежена, а з'єднання було настільки нестабільним, що його «практично неможливо було використовувати»… Журнали показали, що термінал не зафіксував жодної секунди стабільного з'єднання після 24 хвилин роботи, а його розширений фільтр Калмана, який об'єднує дані датчиків для визначення положення, потребував 198 секунд для збігу, що набагато довше, ніж зазвичай, що вказує на те, що він намагався встановити надійне положення без надійного GPS. Ця атака з підробкою GPS відрізняється від раніше припущеного широкого радіочастотного глушіння і нагадує повідомлення про локальні радіоперешкоди від вантажівок, поставлених Росією, з акцентом на погіршення роботи окремих наземних терміналів, а не космічної або основної інфраструктури Starlink. Результатом є неоднорідність зв'язку по всьому Ірану, оскільки влада зосереджує свої зусилля на обмеженні передачі даних поблизу чутливих або важливих районів, де такі локальні атаки є дуже ефективними… NasNet вже попереджав, що контрзаходи та втручання залишатимуться «постійною грою в кота і мишу», і перехід до GPS-спуфінгу демонструє цю динаміку в режимі реального часу. Навіть якщо повідомлення про те, що Ілон Маск зробив Starlink безкоштовним в Ірані, є точними, цінність цього доступу буде підірвана, якщо Іран зможе продовжувати погіршувати якість послуг таким чином. Як зазначає Гаріб, цей епізод підкреслює як ефективність атак на державному рівні, що серйозно погіршують якість споживчого супутникового інтернету, так і базову стійкість Starlink, яка все ще підтримує слабке базове з'єднання під час тривалих, складних електронних атак…» ***(Zak Doffman. Iran Strikes Musk's Starlink—First 'Electronic Warfare' Attack //***

Forbes Media LLC (https://www.forbes.com/sites/zakdoffman/2026/01/14/iran-strikes-musks-starlink-first-electronic-warfare-attack/). 14.01.2026).

***

«Адміністрація Трампа розглядає можливість кардинальної зміни кіберстратегії США, яка значно розширить роль приватних компаній в наступальних кібероперацiях, за словами колишніх високопосадовців, ознайомлених з проектами майбутньої Національної стратегії кібербезпеки. Хоча уряд вже укладає контракти з фірмами на розробку інструментів і можливостей, новий підхід передбачає більш пряме використання досвіду приватного сектора в кібервійні, що викликає складні юридичні, стратегічні та практичні питання. Чинне законодавство забороняє приватним структурам проводити наступальні онлайн-кампанії, такі як руйнівні хакерські атаки або тривалі операції проти іноземних супротивників, тому будь-які кроки, що дозволяють компаніям «відповідати хакерськими атаками» або вживати прямих заходів, потребуватимуть схвалення Конгресу. Подібні ідеї, зокрема відновлення «каперських листів» часів Громадянської війни для санкціонування приватних кіберрепресій, знову з'явилися в Капітолії, але вони широко критикуються як цифрове піратство, яке може спровокувати хаос і прорахунки в кіберпросторі…

Відставний генерал-лейтенант Чарльз Л. Мур-молодший, колишній заступник командувача Кіберкомандування США, та експерт з кібербезпеки Бретт Голдштейн стверджують, що неконтрольована наступальна роль компаній може спонукати іноземні уряди інтерпретувати приватні хакерські атаки як офіційні дії США, що потенційно може призвести до небезпечної ескалації, включаючи збройний конфлікт. У їхньому звіті, опублікованому Інститутом національної безпеки Університету Вандербільта, рекомендується, щоб будь-яка приватна участь суворо контролювалася під наглядом Кіберкомандування. Вони пропонують юридичні обхідні шляхи, які зберігають розподіл ролей між державним і приватним секторами: наприклад, введення в компанію кібероператора в формі для здійснення атак або залучення приватних фірм до розробки та кодування інструментів, які потім використовує Кіберкомандування. Мур і Голдштейн стверджують, що Міністерство оборони не може впоратися з масштабом і темпами сучасних кіберзагроз лише за допомогою державних службовців, і що використання приватного досвіду є необхідним для побудови постійних, масштабних наступальних кампаній, необхідних для «закидання піску в шестерні» операцій супротивника і підготовки до потенційних надзвичайних ситуацій у воєнний час.

Таке мислення відображає більш широкий поштовх у частинах спільноти національної безпеки до більш частих, проактивних і превентивних наступальних кібератак. Прихильники, такі як Джо Лін, колишній офіцер резерву ВМС, який зараз керує стартапом у сфері кібервійни, стверджують, що Сполучені Штати історично обмежувалися окремими операціями, такими як попередні місії з порушення роботи іноземної інфраструктури або націлені на окремих лідерів, а не тривалими кампаніями, порівнянними з довготривалими операціями, пов'язаними з Китаєм, проти критичної інфраструктури США. Зі зростанням консенсусу щодо

того, що наступальні кібероперації можуть бути менш ескалаційними, ніж раніше побоювалися, прихильники бачать більшу роль венчурних кіберкомпаній та інноваційних стартапів у посиленні можливостей США. Проте будь-який крок, спрямований на те, щоб поставити операторів приватного сектора «пліч-о-пліч» з військовими кібервійськами у проведенні атак, означатиме значне відхилення від давно усталеної практики і, ймовірно, стане центральним пунктом розгляду під час слухань у Конгресі та підтвердження кандидатури наступного керівника Кіберкомандування та Національного агентства безпеки…» ***(Adam Sella. U.S. Weighs Expanding Private Companies' Role in Cyberwarfare // The New York Times Company (https://www.nytimes.com/2026/01/14/us/politics/us-cyberwarfare-private-companies.html). 14.01.2026).***

***

«…На недавніх слуханнях підкомітету Палати представників щодо кіберпотенціалу США голова Енді Оглс та експерти-свідки стверджували, що країна повинна відмовитися від суто оборонної позиції та прийняти «промислову» наступальну стратегію, щоб стримати таких супротивників, як Китай, Росія, Іран та Північна Корея. Посилаючись на такі порушення, як Salt Typhoon та Volt Typhoon, спрямовані проти співробітників Конгресу та критичної інфраструктури, доповідачі наголосили, що нинішні заходи реагування не приносять реальних збитків. Джо Лін з Twenty Technologies закликав автоматизувати роботу операторів, щоб один співробітник міг керувати сотнями цілей, відповідаючи темпам китайських кампаній, а Емілі Хардінг з CSIS зазначила, що американські чиновники часто завмирають під час криз через нечіткі пороги ескалації, і виступила за створення спеціальних кібервійськ…

Також було наголошено на «оперативній співпраці» з приватним сектором, розглядаючи компанії як активних партнерів у сфері оборони, а не пасивних жертв, та обговорила рішення щодо робочої сили, починаючи від автоматизації на основі штучного інтелекту до корпусу «кіберрезерву». Дрю Бейглі з CrowdStrike застеріг від самосуду, але підтримав систематичне руйнування зловмисної інфраструктури. Крім того, було наголошено на вразливості підводних кабелів та висловлено заклики до покращення можливостей спостереження та ремонту. Засідання завершилося консенсусом щодо відмови від принципу «око за око» на користь дипломатичних, економічних або кінетичних інструментів, які дозволяють завдати удару по найболючіших точках супротивника, що свідчить про появу нової цифрової доктрини Монро, згідно з якою порушення мають серйозні наслідки…» ***(Hank Berrien. Beyond Defense: Congress Wants To Industrialize U.S. Cyber Offense // The Daily Wire LLC (https://www.dailywire.com/news/beyond-defense-congress-wants-to-industrialize-u-s-cyber-offense). 14.01.2026).***

***

«Прем'єр-міністр Польщі Дональд Туск заявив, що в грудні 2025 року спецслужби країни запобігли серйозній спробі кібератаки на енергетичну інфраструктуру, яка була спрямована на дві теплоелектростанції та вітроелектростанції і могла залишити до 500 000 споживачів без опалення

взимку. Туск заявив, що критична інфраструктура не була порушена, і віддав належне механізмам раннього виявлення та сильній реакції, зазначивши, що остаточне визначення винних ще не встановлено, але зібрані докази вказують на групи, пов'язані з російськими службами безпеки. Віце-прем'єр-міністр і міністр цифрових справ Кшиштоф Гавковський назвав цей інцидент одним з найсерйозніших за останні роки, попередивши, що Польща була близька до відключення електроенергії, і назвавши сучасні кіберконфлікти «цифровими танками»…

Туск закликав парламент швидко ухвалити нове законодавство про кібербезпеку, щоб посилити захист від іноземного втручання, на тлі поширених в Європі побоювань, що Росія веде «гібридну війну» за допомогою саботажу, кібератак і дезінформації, щоб підірвати підтримку України. Про подібні інциденти з критичною інфраструктурою повідомлялося по всій Європі, і, за даними спецслужб, розслідування російського втручання зараз привертають стільки ж уваги, скільки і боротьба з тероризмом. Європол також наголосив на скоординованих міжнародних зусиллях проти проросійських мереж кіберзлочинців, таких як NoName057(16), пов'язаних з атаками типу «відмова в обслуговуванні» в багатьох європейських країнах. Аналітики підкреслили, що для ефективного захисту потрібні не тільки технології, а й співпраця між державним і приватним секторами, і зазначили, що в цьому випадку захисні системи Польщі спрацювали належним чином, а уряд планує подальші інвестиції, модернізацію та правові реформи, зважаючи на прецеденти, такі як пов'язані з Росією атаки, що спричинили відключення електроенергії в Україні у 2015 році шляхом захоплення контролю над системами SCADA та порушення роботи підстанцій і обслуговування споживачів». ***(Agata Todorow. Poland's PM praises cyber defences after attempted attack on energy infrastructure foiled // euronews (https://www.euronews.com/2026/01/15/polands-pm-praises-cyber-defences-after-attempted-attack-on-energy-infrastructure-foiled). 15.01.2026).***

***

«Національна оборона зараз залежить від кібербезпеки оборонної промислової бази (DIB), де малі та середні підрядники все частіше стають мішенню для супротивників як «бічні двері» до більших систем. Обмежені бюджети та невеликі IT-команди роблять ці підприємства привабливими м'якими мішенями, створюючи критичну вразливість, яку Пентагон вирішує за допомогою обов'язкових стандартів сертифікації зрілості кібербезпеки (CMMC). Однак більшість малих і середніх підприємств не готові до цього, і «розрив у виявленні» збільшується: 35% з них потребують тижня або більше, щоб виявити зловмисника, що в кіберпросторі є вічністю, а 57% оцінюють свої можливості з пошуку загроз як низькі або середні. Незважаючи на те, що 71% розпочали процес забезпечення відповідності, лише 17% готові до рівня 2 CMMC, ризикуючи як контрактами, так і безпекою…

Реальні наслідки є серйозними: 44% малих і середніх підприємств, що працюють у сфері оборони, стикаються з чотирма або більше випадками компрометації кінцевих точок, що дозволяє зловмисникам переміщатися по мережі

та викрадати конфіденційні дані. Яскравим прикладом є злом компанії Stark Aerospace у 2025 році, під час якого було викрадено 4 ТБ проектів ракетних систем та військових документів. Щоб усунути цю прогалину, малі та середні підприємства повинні розглядати CMMC як можливість підвищити стійкість, а не як перелік вимог, що підлягають виконанню, і впроваджувати критично важливі засоби захисту, такі як багатофакторна автентифікація, виявлення та реагування на загрози на кінцевих точках (EDR) корпоративного рівня, постійне навчання з питань фішингу, проактивне виявлення загроз та цілодобовий моніторинг. Зрештою, забезпечення безпеки ланцюга поставок — це не лише питання дотримання вимог, а стратегічна необхідність для захисту національної безпеки…» ***(Chris Petersen. The Hidden Cyber Gap in America's Defense Supply Chain // Cyber Defense Media Group (https://www.cyberdefensemagazine.com/the-hidden-cyber-gap-in-americas-defense-supply-chain/). 17.01.2026).***

***

«Національний центр кібербезпеки Великобританії (NCSC) випустив нове попередження про те, що проросійські хактивісти становлять зростаючу загрозу для місцевих органів влади та критичної національної інфраструктури (CNI), використовуючи прості, але руйнівні атаки типу «відмова в обслуговуванні» (DoS), здатні вивести з ладу важливі веб-сайти та системи і спричинити значні фінансові та виробничі витрати під час відновлення. Хоча ці групи, включаючи NoName057(16), технічно не є складними і часто діють опортуністично, використовуючи незахищене програмне забезпечення або незахищені VNC-з'єднання, вони регулярно атакують вузьке коло організацій протягом декількох днів, виводячи з ладу веб-сайти місцевих рад, а потім перебільшуючи їх вплив в Інтернеті…

Це попередження є продовженням спільного повідомлення, опублікованого минулого місяця, в якому також згадувалися Cyber Army of Russia Reborn, Z-Pentest і Sector16, і відображає більш широке занепокоєння щодо ворожої кіберпозиції Росії, яку високопоставлені представники британської служби безпеки описують як частину неоголошеного конфлікту «сірої зони», що знаходиться трохи нижче порогу війни. NCSC закликає всі організації, а не тільки ті, що входять до CNI та місцевих органів влади, посилити свою оборону, дотримуючись його рекомендацій, використовуючи сторонні послуги з протидії DDoS-атакам, використовуючи мережі доставки контенту та покращуючи базову кібергігієну, попереджаючи, що навіть незначна кібернебезпечна діяльність може серйозно порушити доступ до повсякденних публічних послуг…» ***(Connor Jones. Don't underestimate pro-Russia hacktivists, warns UK's cyber crew // The Register (https://www.theregister.com/2026/01/19/dont_underestimate_prorussia_hacktivists_warns/). 19.01.2026).***

***

«З середини 1990-х років Російська Федерація застосовує проти США витончену «стратегію інформаційного протистояння», використовуючи державні органи, такі як ФСБ, СВР і ГРУ, а також приватні компанії, такі як

Positive Technologies. Росія, яка посідає перше місце в світовому індексі кіберзлочинності за 2024 рік, постійно націлена на США більше, ніж на будь-яку іншу країну, на її частку припадає 20% атак за минулий рік, а її історія включає гучні порушення, такі як зараження шкідливим програмним забезпеченням Міністерства оборони США в 2008 році (що спонукало до створення USCYBERCOM), вторгнення в Білий дім у 2015 році та втручання у вибори 2016 року. Економісти попереджають, що, незважаючи на завдані досі збитки, потенційні «надзвичайно руйнівні» атаки на критичну інфраструктуру, таку як енергомережа Північного Сходу, можуть коштувати до 1 трильйона доларів…

Хоча США відповіли санкціями та наступальними діями, такими як зрив роботи Інтернет-дослідницького агентства у 2018 році, у березні 2025 року відбулася критична зміна політики, коли міністр оборони Піт Хегсет наказав припинити всі наступальні кібероперації проти Росії. Аналітики стверджують, що це додало сміливості супротивникам, посиливши основну стратегічну слабкість: США покладаються на децентралізовану модель оборони, в якій організації самостійно захищають свої мережі, створюючи «слабкі ланки», подібні до вторгнення Moonlight Maze. На відміну від Росії та Китаю, які інтегрують кіберзлочинність, шпигунство та військові дії в єдину доктрину, США як і раніше зосереджуються переважно на боротьбі зі злочинністю. Щоб протидіяти цій зростаючій загрозі, експерти рекомендують відновити наступальні операції для відновлення стримування та впровадити «захист цілей» на всіх рівнях уряду та інфраструктури для усунення вразливостей…» ***(Josef Wolpert. Russian Cyberwarfare Doctrine and America's Counterstrategy // moderndiplomacy.eu (https://moderndiplomacy.eu/2026/01/20/russian-cyberwarfare-doctrine-and-americas-counterstrategy/). 20.01.2026).***

***

«Наприкінці грудня польська електромережа стала об'єктом атаки шкідливого програмного забезпечення типу «wiper», ймовірно організованої російськими державними хакерами з групи Sandworm, з метою перешкодити постачанню електроенергії. Атака, яка збіглася з 10-ю річницею сумнозвісного відключення електроенергії в Україні в 2015 році, організованого Sandworm, мала на меті перервати зв'язок між об'єктами відновлюваної енергетики та операторами розподілу електроенергії, але в кінцевому підсумку зазнала невдачі з невідомих причин…

Компанія ESET, що спеціалізується на питаннях безпеки, ідентифікувала шкідливе програмне забезпечення як «DynoWiper» — руйнівний інструмент, призначений для остаточного видалення даних і паралізування роботи систем. Sandworm, відома тим, що використовує спеціальні програми для видалення даних у кібератаках, зокрема під час інциденту NotPetya у 2017 році та атаки AcidRain на українські супутникові модеми у 2022 році, неодноразово націлювалася на критичну інфраструктуру ворожих країн. Хоча атака DynoWiper не призвела до відключення електроенергії, вона підкреслює постійну загрозу, яку становлять російські кібероперації проти європейських енергетичних систем, та зростаючу важливість надійних кіберзахисних заходів для запобігання таким руйнівним

інцидентам…» ***(Dan Goodin. Poland's energy grid was targeted by never-before-seen wiper malware // Condé Nast (https://arstechnica.com/security/2026/01/wiper-malware-targeted-poland-energy-grid-but-failed-to-knock-out-electricity/). 24.01.2026).***

***

Створення та функціонування кібервійськ

«Високопоставлені американські законодавці попереджають, що Сполучені Штати в даний час ведуть активний і ескалаційний кіберконфлікт, в якому супротивники створюють реальні загрози для критичної інфраструктури та національних систем, які все складніше виявити або відвернути. Голова Комітету Сенату з питань збройних сил Роджер Вікер під час слухань щодо затвердження заявив, що кіберзагроза є «не теоретичною загрозою», а «постійною боротьбою», позиціонуючи Кіберкомандування США як «першу і останню лінію оборони» проти витончених ворожих суб'єктів, які інвестують значні кошти в технології ухилення. Вікер підкреслив, що ця проблема проявляється як на території країни, де критична інфраструктура залишається вразливою, так і в глобальному масштабі, особливо в Індо-Тихоокеанському регіоні.

Під час слухань щодо затвердження на посаді керівника Кіберкомандування США та Національного агентства безпеки генерал-лейтенант Джошуа Радд підтвердив, що кібероперації є невід'ємною частиною сучасної війни і вимагають швидкості, маневреності та постійної інтеграції всіх можливостей. Член комітету Джек Рід висловив занепокоєння тим, що США вступають у «період вразливості», оскільки такі супротивники, як Китай і Росія, інтегрують кіберінструменти зі штучним інтелектом та інформаційною війною, ставлячи під сумнів готовність Кіберкомандування в період структурних змін («Кіберкомандування 2.0») та вакансії керівника. Радд підтвердив, що захист демократичних процесів залишається головним пріоритетом і що Кіберкомандування тісно співпрацює з іншими агентствами для протидії цим загрозам…

Під час слухань також було підкреслено розбіжності щодо позиції США у кіберпросторі. Сенатор Ден Салліван стверджував, що для стримування необхідні більш явні наступальні можливості, і запитав: «Хіба напад не є хорошою обороною?». Рудд відповів, що хоча Кіберкомандування повинно володіти як оборонними, так і наступальними можливостями, рішення про застосування наступальних кіберзасобів остаточно залишається за цивільним керівництвом. Крім того, сенатори наполягали на тому, щоб Радд гарантував, що кібер- та розвідувальні інструменти ніколи не будуть використовуватися проти американських громадян, які не мають зв'язків із закордоном, підкреслюючи необхідність суворих конституційних гарантій при застосуванні цих потужних засобів». ***(US says cyber war has already begun // Sambad English (https://sambadenglish.com/national-international-news/world/us-says-cyber-war-has-already-begun-11015723). 20.01.2026).***

***

«Кібератаки на критичну інфраструктуру США посилюються, а національні угруповання все частіше націлюються на сектор водопостачання та водовідведення (WWS). Застаріле обладнання, понад 150 000 переважно невеликих комунальних підприємств та відсутність обов'язкових правил кібербезпеки роблять водопровідні системи привабливою здобиччю. Нещодавні повідомлення від Агентства з кібербезпеки та безпеки інфраструктури (CISA), Агентства з охорони навколишнього середовища (EPA) та міжнародних партнерів попереджають, що зловмисники тепер виходять за межі псування веб-сайтів, використовуючи незахищені інтерфейси «людина-машина» та інші операційні технології (OT) для порушення роботи або забруднення систем водопостачання…

Відставання в регулюванні: на відміну від регуляторів енергетики, EPA не має чітких законодавчих повноважень відповідно до Закону про безпечну питну воду для введення базових заходів кіберконтролю. Її спроба в 2023 році включити кіберперевірки до санітарних інспекцій була скасована в суді, залишивши лише добровільні рекомендації. Інспекції в 2024 році виявили, що майже 70% комунальних підприємств не дотримуються базових практик, таких як зміна стандартних паролів…

Доки не будуть прийняті федеральні правила, комунальні підприємства повинні діяти самостійно. Рекомендовані найкращі практики включають: надійні паролі, багатофакторну автентифікацію (MFA) та навчання співробітників; своєчасне встановлення виправлень та створення списків дозволених IP-адрес; щорічне тестування планів реагування на інциденти, забезпечення безперервності роботи та відновлення після аварій; сегментацію мереж OT–IT, постійний моніторинг OT та перевірку доступу третіх сторін; а також регулярну оцінку прогалин та вразливостей, яка в ідеалі повинна здійснюватися під наглядом зовнішнього консультанта для збереження привілеїв.

Ради директорів повинні розглядати кіберзрілість та стійкість як стратегічні імперативи, оскільки очікування на введення обов'язкових вимог може призвести до серйозних перебоїв у наданні послуг, криз у сфері охорони здоров'я та втрати довіри, оскільки противники національних держав продовжують досліджувати інфраструктуру водопостачання США». ***(Arjun P. Ramadevanahalli. Understanding the Cybersecurity Risks Flooding the Water and Wastewater Systems Sector // Morgan, Lewis & Bockius LLP. (https://www.morganlewis.com/pubs/2026/01/understanding-the-cybersecurity-risks-flooding-the-water-and-wastewater-systems-sector). 05.01.2026).***

***

«…Інцидент з викраденням даних Colonial Pipeline у 2021 році ілюструє основну проблему кіберінцидентів у нафтогазовій галузі: перевірку фізичного процесу. Хоча атака торкнулася лише систем білінгу Colonial і не було підтверджено порушення операційних технологій, компанія не могла швидко і

впевнено перевірити, чи є нормальними потоки, тиск і умови безпеки в трубопроводі. В результаті вона зупинила роботу трубопроводів у всій своїй мережі, поки персонал не був відправлений на термінали та об'єкти для підтвердження умов на місці. Зупинка тривала кілька днів не тому, що фізичне обладнання було пошкоджене, а тому, що безпеку не можна було підтвердити лише на основі даних системи…

Ця проблема перевірки стає все складнішою у міру зміни структури операцій. Багато об'єктів, які раніше мали постійний персонал на місці, тепер управляються з централізованих диспетчерських. Компресорні, насосні та запірні станції часто працюють без нагляду, а персонал на місцях охоплює великі території. Коли виникає невизначеність, пов'язана з кібербезпекою, фізичні перевірки, які раніше виконувалися за лічені хвилини, тепер займають години через необхідність переїзду, доступу та процедур безпеки. Водночас більша автоматизація зменшила неформальне усвідомлення процесів: з меншою кількістю людей, які фізично присутні на місці, розбіжності між тим, що відображають системи управління, і тим, що насправді робить обладнання, менш імовірно будуть помічені, якщо тільки команди не будуть спеціально відправлені для розслідування. Ручна перевірка залишається остаточною гарантією, коли даним не можна довіряти, але вона стала повільнішою, менш доступною і дуже заважає саме тоді, коли швидка перевірка є найбільш критичною.

У цьому контексті розмежування між даними системи управління та даними рівня процесу (рівень 0) набуває стратегічного значення. Значення SCADA, PLC та HMI представляють оброблений, залежний від мережі огляд заводу. На відміну від цього, дані рівня 0 — це необроблені електричні та фізичні сигнали, що генеруються самим процесом — тиск, струм, потік, положення клапанів — які існують до того, як програмне забезпечення їх інтерпретує і до того, як зловмисники можуть сфальсифікувати відображення або логіку. Постійний моніторинг сигналів рівня 0 не замінює системи управління або безпеки, але забезпечує фізично обґрунтоване джерело достовірної інформації. Він дозволяє операторам підтвердити, чи дійсно відбулася задана дія (наприклад, чи споживав насос струм, коли йому було наказано запуститися), виявити розбіжності між тим, що повідомляє система, і тим, що робить процес, раніше визначити, чи обмежується вторгнення мережею або має фізичні наслідки, та зменшити залежність від відправлення людей на місце події під час або після кіберінциденту…

Регулюючі органи все частіше кодують ці очікування. Після інциденту з Colonial Адміністрація транспортної безпеки США видала директиви щодо безпеки трубопроводів, які вимагають сегментації, постійного моніторингу, оперативного повідомлення CISA та перевірки впливу на роботу. Закон про повідомлення про кіберінциденти для критичної інфраструктури (CIRCIA) вимагає повідомляти про суттєві кіберінциденти протягом 72 годин. В Європі Директива NIS2 поширює зобов'язання на системи OT і вимагає доказів готовності до безперебійної роботи. У всіх цих рамках вимальовується спільна тема: оператори повинні бути в змозі довести, що фізичний процес залишається в безпечному, відомому стані під час і

після кіберінциденту, і що така впевненість в кінцевому рахунку залежить від перевірених, фізично обґрунтованих даних про процес.

З цієї точки зору, головне питання в кіберінцидентах у нафтогазовій галузі полягає не тільки в тому, чи були порушені мережі або контролери, але й у тому, чи фізичний процес все ще працює як передбачалося. Коли це неможливо підтвердити, оператори з обережності сповільнюють або зупиняють потік, що створює операційний, комерційний та безпековий тиск навіть за відсутності пошкоджень. Зі зменшенням кількості людей на об'єкті та зростанням автоматизації покладатися виключно на екрани SCADA вже недостатньо. Тому моніторинг на рівні процесів став критично важливим — не лише як технічне вдосконалення, але й як оперативна, нормативна та управлінська вимога для збереження контролю, безпеки та довіри до сучасних цифрових систем передачі…» ***(Amir Samoiloff. The hidden risk in oil and gas cybersecurity: Verifying the physical process // Palladian Publications Ltd. (https://www.oilfieldtechnology.com/special-reports/19012026/the-hidden-risk-in-oil-and-gas-cybersecurity-verifying-the-physical-process/). 19.01.2026).***

***

«MITRE запустила Embedded Systems Threat Matrix™ (ESTM) — спеціальну систему кібербезпеки для вбудованих систем, що лежать в основі критичної інфраструктури та оборонних технологій. Розроблена спільно з Управлінням кіберстійкості озброєних систем (CROWS) ВПС США, ESTM покликана допомогти дослідникам, постачальникам і фахівцям з безпеки розуміти, класифікувати та захищатися від кіберзагроз, спрямованих на вбудовані платформи в таких секторах, як транспорт, енергетика, охорона здоров'я, промислове управління та робототехніка. Спираючись на підхід MITRE ATT&CK® та узгоджуючись з моделлю загроз EMB3D™, ESTM систематизує тактики та методи, характерні для вбудованих систем, усуваючи як існуючі, так і нові вразливості, щоб її можна було інтегрувати в існуючі програми безпеки та використовувати для розробки безпечних систем. Підкреслюючи місію MITRE, що ставить на перше місце інтереси суспільства, старший віце-президент Кеокі Джексон описав ESTM як засіб, що заповнює ключову прогалину, надаючи чіткі, практичні рекомендації щодо захисту базових систем…» ***(MITRE Launches Embedded Systems Threat Matrix to Strengthen Cyber Defense for Critical Infrastructure and Defense Systems // MITRE (https://www.mitre.org/news-insights/news-release/mitre-launches-embedded-systems-threat-matrix-strengthen-cyber-defense). 20.01.2026).***

***

Кіберзахист виробничих об’єктів

«Зближення операційних технологій (OT) та інформаційних технологій (IT) у виробництві, зумовлене глобальними ланцюгами постачання та цифровими лініями, зробило безпеку та захист нерозривними поняттями. Скомпрометовані облікові дані або вразливість постачальника зараз становлять

таку ж загрозу, як і механічна несправність, що може призвести до зупинки виробництва, втрати якості та небезпеки для співробітників, про що свідчить 65% частка атак програм-вимагачів, спрямованих на цей сектор у другому кварталі 2025 року. Випадок порушення безпеки бразильської компанії C&M Software продемонстрував, що компрометації одного стороннього постачальника достатньо, щоб порушити роботу декількох установ — цей урок можна безпосередньо застосувати до виробництва, де команди дистанційного обслуговування, інтегратори та виробники оригінального обладнання часто мають доступ до конфіденційних виробничих систем…

Недавні інциденти у виробника медичного обладнання Masimo та сталевого гіганта Nucor підтверджують цю закономірність: кібервтручання використовували доступ для порушення роботи, що вплинуло на фізичну виробничу дільницю. Це розмиття меж означає, що традиційні фізичні заходи безпеки (блокування) та IT-безпека (брандмауери) тепер повинні управлятися як взаємопов'язані рівні…

Ідентифікація стала важливою складовою безпеки обладнання. Прості загрози, такі як неактивовані облікові записи, постійні VPN або спільні паролі адміністратора, можуть дозволити зловмиснику змінити логіку процесу або вимкнути функції безпеки. Тому обов'язковими є такі заходи безпеки ідентифікації, як Zero Trust, доступ «just-in-time» (JIT) та постійний аудит. Управління віддаленим доступом повинно замінити традиційні VPN сучасними системами, які надають облікові дані тільки для конкретних, обмежених у часі завдань і контролюють сеанси за допомогою поведінкового аналізу на основі штучного інтелекту. Ця зміна підкріплюється розвитком стандартів, таких як ISA/IEC 62443 та ISO 13849-1, які вимагають інтегрованої «безпеки за дизайном» та «безпеки за конструкцією» протягом усього життєвого циклу обладнання». ***(Marcelo Pinto. Manufacturing's Cybersecurity Crisis: Third-Party Access May Be Your Biggest Safety Risk // Automation World (https://www.automationworld.com/cybersecurity/article/55341939/isa-manufacturings-cybersecurity-crisis-third-party-access-may-be-your-biggest-safety-risk). 15.01.2026).***

***

«Промислова кібербезпека перебуває на переломному етапі, оскільки традиційні засоби захисту периметра вже не є достатніми для захисту все більш взаємопов'язаних заводів, мереж та виробничих середовищ. Інтеграція IT- та OT-систем розширила площу атаки, що зробило перебої у виробництві, ризики для безпеки та втрати надійності більш імовірними та серйознішими. Як результат, понад третина виробників зараз надають пріоритет підвищенню безпеки IT/OT, а майже половина використовує аналітику в режимі реального часу та штучний інтелект не тільки для виявлення порушень, але й для перевірки часу безвідмовної роботи та якості…

Незаплановані простої в середовищах OT можуть бути надзвичайно дорогими, і зараз зрілі програми кібербезпеки оцінюються за такими операційними показниками, як час безвідмовної роботи, безпека та пропускна здатність, а не лише за технічними показниками. Нормативні вимоги, такі як EU NIS2, змушують

організації демонструвати не лише відповідність вимогам, а й стійкість, тоді як кіберстрахування все більше впливає на управління ризиками та інвестиції в безпеку.

Експерти сходяться на думці, що вимоги щодо дотримання нормативних вимог привернули увагу до безпеки операційних технологій та сприяли інвестиціям у цю сферу, але для досягнення справжньої стійкості організаціям необхідно вийти за межі дотримання нормативних вимог та інтегрувати кібербезпеку в бізнес-процеси. Це означає переосмислення кіберризиків з операційної точки зору — зосередившись на тому, як кіберінциденти впливають на доступність, безпеку та відновлення, — а не розглядати їх як суто технічну проблему. Співпраця між підрозділами кібербезпеки, інженерії, експлуатації та безпеки є надзвичайно важливою, як і впровадження архітектур на основі ідентифікації, що постійно контролюються…

Технологічні зміни, такі як хмарні операційні технології, безпечний віддалений доступ та виявлення аномалій на основі штучного інтелекту, дозволяють кібербезпеці підтримувати роботу підприємств, а не перешкоджати їй. Однак більшість організацій все ще недостатньо підготовлені, не мають базових засобів контролю та зрілих планів відновлення після аварій. Найбільш прогресивні організації використовують кібербезпеку як систему раннього попередження про оперативну нестабільність, покращуючи передбачуваність та стійкість.

Нормативні акти підвищили базові вимоги до кібербезпеки ОТ, але часто підсилюють формальне дотримання вимог, а не справжню стійкість. Найефективнішими є ті рамки, які наголошують на постійному вдосконаленні та реальних операційних результатах. Кіберстрахування також сприяє покращенню практик безпеки, стимулюючи створення захищених архітектур та надійних систем реагування на інциденти, хоча власники активів повинні збалансувати вимоги страховиків з оперативними реаліями…

Зрештою, промислова кібербезпека повинна еволюціонувати від фокусу на захисті периметра та дотриманні вимог до цілісного, орієнтованого на ефективність підходу, який надає пріоритет операційній стійкості, безпеці та безперервності бізнесу. Ця зміна вимагає дисциплінованої інтеграції технологій, процесів та людей, з кібербезпекою, вбудованою як основний фактор надійної та ефективної промислової діяльності». ***(Anna Ribeiro. Aligning OT cybersecurity with uptime, safety, and throughput as digital transformation reshapes industrial risk // Industrial Cyber (https://industrialcyber.co/features/aligning-ot-cybersecurity-with-uptime-safety-and-throughput-as-digital-transformation-reshapes-industrial-risk/). 18.01.2026).***

***

«Інтелектуальна метрологія, в якій мережеві автоматизовані вимірювальні системи безпосередньо підключені до замкнутого циклу управління процесами, цифрових двійників, аналітичних платформ і корпоративних систем, перетворила метрологію на основний рушій сучасної виробничої ефективності, але також створила нову лінію фронту кібербезпеки. Оскільки результати вимірювань у реальному часі тепер впливають на налаштування обладнання, забезпечують якість та відповідність нормативним

вимогам, а також навчають аналітичні та ШІ-моделі, будь-яке порушення безпеки цих даних через маніпуляції, втрату або несанкціонований доступ може призвести до неправильних рішень про прийняття/відхилення, невиявлених дефектів, спотворених тенденцій процесів, недосконалої оптимізації ШІ, порушення нормативних вимог та шкоди репутації…

Поверхня атаки розширилася від ізольованих інструментів до взаємопов'язаного середовища, що охоплює виробництво, якість та корпоративні ІТ, із загальними векторами загроз, включаючи мережеві атаки на погано сегментовані або слабо аутентифіковані посилання, вразливості у вбудованих операційних системах та прошивці на кінцевих точках метрології, неправильно налаштовані хмарні платформи, що містять довгострокові записи про якість, та незахищені компоненти програмного забезпечення сторонніх виробників у ланцюжку постачання. Недавній кіберзлом Jaguar Land Rover, який змусив зупинити роботу та виробництво на декількох об'єктах, ілюструє, наскільки тісно пов'язаними стали цифрові заводи: хоча інцидент не був пов'язаний безпосередньо з метрологією, він показав, що злом в одній області може порушити виробництво, якість, логістику та роботу партнерів, які покладаються на спільні дані… Для інтелектуальної метрології урок полягає в тому, що збої в кібербезпеці швидко перетворюються на збої в якості. Тому захист вимірювальних систем повинен розглядатися з такою ж суворістю, як і захист критично важливої для безпеки автоматизації, вбудовуючи кібербезпеку в управління якістю, а не розглядаючи її як окрему проблему ІТ. Узгодження з промисловими системами безпеки, такими як IEC 62443 для промислової автоматизації та ISO/IEC 27001 для інформаційної безпеки, допомагає визначити послідовний контроль доступу, безпечну обробку даних та процеси, що підлягають аудиту, протягом усього життєвого циклу вимірювання, одночасно уточнюючи відповідальність за безпеку метрологічних даних у функціях ІТ, ОТ та якості. У міру того, як метрологія еволюціонує в повністю підключену, керовану даними дисципліну, багаторівнева кібербезпека та управління стають важливими компонентами цілісності вимірювань, забезпечуючи виробникам не тільки захист їх систем, але й збереження довіри до кожного вимірювання, яке визначає їх діяльність». ***(Cybersecurity in Smart Metrology – Safeguarding Data Integrity in Connected Systems // E-Zine Media (https://metrology.news/cybersecurity-in-smart-metrology-safeguarding-data-integrity-in-connected-systems/). 20.01.2026).***

***

«У 2026 році злиття інформаційних технологій (ІТ) та операційних технологій (ОТ) кардинально змінило ландшафт кібербезпеки. Колись окремі ІТ-системи, що управляли даними, та ОТ-системи, що контролювали фізичні операції, тепер тісно взаємопов'язані, що розмиває традиційні межі безпеки та наражає застарілі ОТ-пристрої, багато з яких не мають вбудованих засобів захисту, на нові ризики. Така інтеграція вимагає єдиних стратегій, що забезпечують захист, прозорість та управління ризиками в обох сферах…

Середовище загроз стало більш складним, оскільки зловмисники все частіше націлюються на системи ОТ, використовуючи застарілі вразливості та

застосовуючи автоматизовані сканування та атаки на основі штучного інтелекту для швидкого виявлення та компрометації критично важливих активів. Зараз порушення безпеки часто впливають як на IT, так і на OT, ставлячи під загрозу дані, промислові об'єкти та громадську безпеку.

У відповідь на це для OT стало необхідним впровадження безпеки за принципом «нульової довіри» — «ніколи не довіряй, завжди перевіряй», що передбачає сегментацію, суворий контроль доступу та постійну автентифікацію для запобігання поширенню загроз. Однак впровадження «нульової довіри» в OT вимагає ретельного планування, щоб уникнути порушення критично важливих операцій…

Основною проблемою залишається недостатня прозорість в OT-середовищах, де застаріле обладнання та пропрієтарне програмне забезпечення перешкоджають моніторингу в режимі реального часу та виявленню загроз. Провідні організації інвестують в уніфікований моніторинг, аналітику на основі штучного інтелекту та комплексні інвентаризації активів, щоб усунути ці прогалини та підвищити операційну стійкість.

Ефективна кібербезпека OT також залежить від співпраці, культури та талантів. Подолання традиційного розриву між командами IT та OT вимагає міждисциплінарної співпраці, спільної мови та скоординованого керівництва. Інвестиції керівництва в розвиток персоналу та структурну інтеграцію мають вирішальне значення, особливо з огляду на нестачу фахівців, які володіють навичками як у сфері кібербезпеки, так і в операціях OT…

Нарешті, набирає обертів рух за посилення стандартів і нормативних вимог, а такі рамки, як ISO/IEC 62443 і NERC CIP, спонукають постачальників і операторів до вдосконалення дизайну, надійної аутентифікації та управління життєвим циклом. Дотримання нормативних вимог еволюціонує від формальної процедури до рушійної сили зрілості безпеки.

Зрештою, об'єднання IT та OT розширює площу атаки, але також змушує організації застосовувати цілісні стратегії кібербезпеки, що поєднують технології, управління та культуру, засновані на міждисциплінарній співпраці, повній прозорості та принципах нульової довіри, для захисту як фізичної, так і цифрової інфраструктури в умовах постійно мінливого середовища загроз». ***(Chuck Brooks. OT–IT Cybersecurity: Navigating The New Frontier Of Risk // Forbes Media LLC. (https://www.forbes.com/sites/chuckbrooks/2026/01/27/otit-cybersecurity-navigating-the-new-frontier-of-risk/). 27.01.2026).***

***

Кіберзахист закладів охорони здоров'я

«Атака програм-вимагачів на приватний портал для пацієнтів Manage My Health (MMH) призвела до витоку медичних даних понад 120 000 новозеландців. MMH вже визначив лікарів загальної практики, пацієнти яких постраждали, але ще не встановив чіткий графік повідомлення про це окремих осіб; Health NZ очікує, що графік буде оголошено до вівторка…

Health NZ активувала команду з управління інцидентами та координує свої дії з Національним центром кібербезпеки та підрозділом поліції з боротьби з кіберзлочинністю. Хоча власні системи Health NZ та інші портали для пацієнтів не були скомпрометовані, чиновники наполягають, щоб MMH – та всі постачальники медичних даних – продемонстрували більш надійну безпеку та поділилися отриманим досвідом, щоб запобігти повторенню подібних інцидентів…

General Practice New Zealand співпрацює з мережами первинної медичної допомоги, щоб підтримувати клініки та обробляти запити пацієнтів, а MMH планує регулярно публікувати оновлення, додавати інформацію до свого додатку та відкрити гарячу лінію 0800. Health NZ також підтримує юридичні заходи MMH, спрямовані на запобігання подальшому зловживанню викраденими даними. Усі загальнопрактичні клініки залишаються відкритими, і пацієнти можуть продовжувати звертатися за медичною допомогою, як зазвичай». ***(Manage My Health cybersecurity hack: GPs whose patients' data was stolen identified // Radio New Zealand (https://www.rnz.co.nz/news/national/583156/manage-my-health-cybersecurity-hack-gps-whose-patients-data-was-stolen-identified). 04.01.2026).***

***

«Кіберінциденти в медичних пристроях виходять далеко за межі традиційних проблем IT-безпеки і охоплюють збої в системах управління, які можуть становити загрозу для життя, проте багато таких інцидентів залишаються невизначеними як пов'язані з кібербезпекою, оскільки організації з кібербезпеки та виробництва не можуть налагодити належну комунікацію. Керівництво FDA (Федеральне управління з контролю за лікарськими засобами) з кібербезпеки медичних пристроїв від вересня 2023 року зосереджується на IT — конфіденційності, цілісності та доступності — і наголошує на безпечній мережевій комунікації, але не розглядає безпосередньо режими відмов систем управління, що виникають через проблеми з апаратним забезпеченням, логікою програмного забезпечення, синхронізацією, чергою команд, надійністю датчиків або непередбаченими взаємодіями між взаємопов'язаними компонентами. Аналіз IEEE Spectrum 56 000 випадків відкликання медичних виробів FDA з 2002 року показав, що 15% з них були пов'язані з помилками управління процесами, багато з яких насправді є кіберінцидентами в системах управління; проблеми з програмним забезпеченням були розділені на шість основних причин, проте кібербезпека згадувалася лише стосовно «середовища використання» пристрою (додатки для смартфонів та допоміжне програмне забезпечення)…

Знакові випадки ілюструють небезпеку. Апарат для променевої терапії Therac-25 (1982) застосовував дози опромінення, що в сотні разів перевищували норму, через одночасні помилки в програмуванні, що призвело до щонайменше шести нещасних випадків у період з 1985 по 1987 рік із летальними наслідками та серйозними травмами — зараз це стандартний приклад для вивчення. Глюкозні датчики компанії Abbott надавали неправильні показники низького рівня глюкози, що призводило до неправильних рішень щодо лікування і, станом на листопад 2025 року, до 736 випадків серйозних травм і семи смертей. Інсулінові помпи Control-IQ компанії Tandem Diabetes Care зазнавали збоїв у роботі додатку iOS, що

спричиняло надмірну активність Bluetooth, яка розряджала батареї помпи, викликаючи несподіване вимкнення та припинення подачі інсуліну; станом на квітень 2024 року це призвело до 224 випадків травм. Компанія Abbott також відкликала пристрій для підтримки лівого шлуночка, в якому помилки в черзі команд призвели до несподіваного зупинення або запуску насоса без сигналу тривоги — було зареєстровано два випадки травм. Компанія Globus Medical відкликала пристрій для фіксації хребта під час хірургічного втручання через помилку в алгоритмі калібрування, що вплинула на точність розміщення імплантату; це призвело до восьми випадків травм…

Ці кіберінциденти в системах управління виявляють критичні прогалини: вимоги FDA до кібербезпеки є недостатніми для систем управління, а відповідне навчання для виробників і кінцевих користувачів недоступне. Для безпеки пацієнтів ці прогалини в кібербезпеці систем управління необхідно терміново усунути». ***(Joe Weiss. Medical device control system cyber incidents have injured and killed people // Endeavor Business Media (https://www.controlglobal.com/blogs/unfettered/blog/55342771/how-to-avoid-injuries-caused-by-medical-device-control-system-cyber-incidents). 12.01.2026).***

***

«…Таємний аудит, проведений Аудиторською службою штату Новий Південний Уельс, оприлюднений незадовго до Різдва, виявив, що Департамент охорони здоров'я штату Новий Південний Уельс не в змозі управляти ризиками кібербезпеки клінічних систем, що робить лікарні та дані пацієнтів вкрай вразливими до кібератак. Аудит виявив системне недотримання вимог уряду штату щодо кібербезпеки в 15 місцевих округах охорони здоров'я (LHD), жоден з яких не мав відповідних планів реагування на інциденти. З 2019 року всі LHD не відповідали мінімальним вимогам кібербезпеки, що свідчить про недостатню підготовленість та стійкість до кіберзагроз, які можуть порушити надання медичних послуг та поставити під загрозу конфіденційну інформацію про пацієнтів…

У звіті також було виявлено «нормалізацію недотримання вимог» серед клінічного персоналу, що випливає з «відчутної напруги» між терміновістю надання медичних послуг та протоколами безпеки. Незважаючи на спостереження поширеного недотримання вимог, перевірені LHD не оцінили ефективність існуючих засобів контролю та не інвестували в альтернативні IT-рішення, які могли б збалансувати клінічні потреби та безпеку. Крім того, було встановлено, що ролі та обов'язки eHealth NSW та LHD щодо кібербезпеки є нечіткими…

Аудиторська служба рекомендувала Міністерству охорони здоров'я штату перевірити відповідність вимогам, уточнити ролі в галузі кібербезпеки, а також розробити конкретні рекомендації щодо балансу між клінічними потребами та вимогами безпеки. З моменту отримання звіту в липні 2025 року Міністерство охорони здоров'я штату Новий Південний Уельс створило робочу групу і почало вживати заходів відповідно до цих рекомендацій…» ***(Denham Sadler. NSW hospitals exposed to cyber attacks // Australian Computer Society***

(https://ia.acs.org.au/article/2026/nsw-hospitals-exposed-to-cyber-attacks.html). 06.01.2026).

***

Захист персональних даних та соціальні мережі

«…Захист даних та кібербезпека часто розглядаються разом, проте вони стосуються різних проблем. Захист даних є регуляторним та базується на правах: він регулює, чому та як організація збирає, використовує, передає та зберігає особисту інформацію, а також зобов'язує підприємства дотримуватися таких принципів, як законність, мінімізація даних, обмеження мети, прозорість та права суб'єктів даних відповідно до таких законів, як GDPR. Натомість кібербезпека є технічною та оборонною: вона захищає системи, мережі та дані від несанкціонованого доступу, програм-вимагачів, зловживань з боку інсайдерів або перебоїв у роботі послуг за допомогою таких засобів контролю, як брандмауери, шифрування, управління ідентифікацією та доступом, а також інструменти реагування на інциденти…

Оскільки ці дві сфери є взаємодоповнюючими, їх окреме розглядання призводить до серйозних прогалин. Навіть ідеально захищена мережа може порушувати вимоги GDPR, якщо особисті дані збираються без згоди або зберігаються довше, ніж це необхідно; і навпаки, зразкові політики конфіденційності не мають сенсу, якщо слабкий контроль доступу дозволяє зловмисникам викрасти дані. Регулюючі органи визнають цю взаємозалежність: GDPR вимагає від організацій вживати «відповідних технічних та організаційних заходів», чітко пов'язуючи зобов'язання щодо конфіденційності з ефективними практиками безпеки…

Сучасні засоби безпеки забезпечують дотримання вимог конфіденційності шляхом шифрування даних під час зберігання та передачі, впровадження принципу мінімальних привілеїв доступу, виявлення порушень для дотримання 72-годинного терміну повідомлення та запобігання втраті або пошкодженню збереженої інформації. Проте багато компаній стикаються з труднощами: юридичні відділи можуть не мати достатнього уявлення про технічні засоби захисту, відділи безпеки можуть зосереджуватися на інфраструктурі, а не на потоках персональних даних, а плани реагування на порушення часто стосуються відновлення, але ігнорують обов'язкові вимоги щодо розкриття інформації.

Для усунення цієї прогалини необхідна міжфункціональна співпраця. Організації повинні визначити, де зберігаються персональні дані, включити перевірки конфіденційності в оцінку ризиків, проводити спільні навчання з реагування на інциденти та використовувати централізовані платформи, які відстежують обробку даних та контролюють безпеку. Такі рішення, як Data Privacy Essentials від Sovy, у поєднанні з навчанням персоналу з питань кібербезпеки, допомагають малим підприємствам управляти документацією, згодою та записами

про потік даних, а їхні системи безпеки забезпечують шифрування, моніторинг та контроль доступу…

Таке узгодження конфіденційності та кібербезпеки перетворює дотримання вимог з додаткової функції на основний елемент стійкості, зберігаючи довіру клієнтів та зменшуючи фінансові збитки та шкоду репутації від неминучих кіберінцидентів…» ***(Data Privacy vs Cybersecurity Solutions: Key Differences // Techstrong Group Inc. (https://securityboulevard.com/2026/01/data-privacy-vs-cybersecurity-solutions-key-differences/). 03.01.2026).***

***

«…Крадіжка особистих даних та шахрайство залишаються постійною загрозою в США, але новий аналіз WalletHub показує, що деякі штати є більш вразливими, ніж інші. У рейтингу, складеному на основі кількості скарг, загальних фінансових втрат та рівня захисту на рівні штату, перше місце посіла Флорида, за нею йдуть Каліфорнія, Джорджія, Нью-Джерсі та Вашингтон, округ Колумбія. У цих штатах або фіксується велика кількість інцидентів, або втрачаються великі суми грошей, або і те, і інше. На іншому кінці спектру Мен, Західна Вірджинія, Коннектикут, Монтана та Вермонт були визнані найменш вразливими, що, на думку аналітиків, може свідчити про більшу обізнаність та кращі запобіжні звички серед мешканців. У міру того, як все більше особистих даних переходить в онлайн для покупок, банківських операцій, охорони здоров'я та соціальних мереж, кількість точок входу для шахраїв зростає, що полегшує злочинцям крадіжку логінів, захоплення облікових записів, відкриття нових кредитних ліній або перенаправлення коштів… Експерти підкреслюють, що хоча місцезнаходження може впливати на ризик, індивідуальна поведінка має вирішальне значення в будь-якому випадку: використання довгих, унікальних паролів замість повторного використання одного і того ж, увімкнення двофакторної автентифікації (особливо на основних електронних поштових рахунках), увімкнення сповіщень про входи та зміни в обліковому записі, а також регулярний моніторинг банківських та кредитних рахунків можуть допомогти виявити шахрайство на ранній стадії та ускладнити злодіям отримання контролю. У разі виявлення підозрілої діяльності вони радять негайно звертатися до фінансових установ та правоохоронних органів, а також повідомляти кредитні бюро, щоб вони могли заморозити рахунки та запобігти подальшим збиткам». ***(Caresse Jackman. Analysis ranks states most vulnerable to identity theft, fraud // A Gray Local Media Station (https://www.wbrc.com/2026/01/14/analysis-ranks-states-most-vulnerable-identity-theft-fraud/). 14.01.2026).***

***

Масштабні витоки персональних даних

«Група хакерів Everest, що спеціалізується на викраденні даних, заявила, що викрала близько 186 ГБ даних з Bolttech, страхової інфраструктурної платформи з Сінгапуру, вартість якої оцінюється в 2,1 млрд доларів. На своєму

сайті в даркнеті Everest опублікувала скріншоти, встановила зворотний відлік і висунула вимоги про виплату викупу, попередивши, що опублікує викрадені дані, якщо Bolttech не відповість на її вимоги протягом тижня. Група стверджує, що викрадені дані включають облікові дані співробітників і агентів, особисту інформацію клієнтів, деталі полісів і іпотечних кредитів, фінансові параметри та внутрішні ідентифікатори…

Аналітики Cybernews, після вивчення зразків, стверджують, що витік інформації може призвести до фішингу, крадіжки особистих даних та шахрайських страхових вимог; якщо в наявності є повні адреси, жертви також ризикують стати жертвами доксингу. Запущена в 2020 році, компанія Bolttech об'єднує понад 150 страхових компаній та брокерів і обробляє понад 5 мільярдів доларів щорічних валових страхових премій.

Everest, який, як вважається, має зв'язки з Росією і діє з 2021 року, за останній рік атакував понад 100 організацій, серед яких Petrobras і Under Armour, а раніше хвалився проникненням в AT&T». ***(Gintaras Radauskas. Russia-linked hackers nab highly sensitive Bolttech data, demand ransom // Cybernews (https://cybernews.com/security/everest-hack-bolttech-ransom-data/). 05.01.2026).***

***

«NordVPN категорично заперечив звинувачення у витоку даних, підтвердивши, що всі його системи та внутрішня виробнича інфраструктура залишаються повністю безпечними після того, як зловмисник на незаконному форумі помилково заявив, що отримав доступ до «сервера розробки NordVPN Salesforce». Лаура Тирилите, керівник відділу зв'язків з громадськістю, заявила, що криміналістичний аналіз показав, що витік даних стався не з внутрішнього середовища NordVPN, а з конфігураційних файлів, пов'язаних з короткостроковим пробним обліковим записом на сторонній платформі. Зловмисник, використовуючи новий обліковий запис під назвою «1011», стверджував, що викрав вихідні коди, ключі API та дампи баз даних, отримані шляхом брутфорсу неправильно налаштованого сервера, але надані зразки містили застарілі часові мітки та неправильно відформатовані ключі, а що важливо, не містили жодних особистих даних користувачів…» ***(Ernestas Naprys. Nord Security confirms systems are secure after fake breach allegations // Cybernews (https://cybernews.com/security/nordvpn-confirms-systems-secure-after-breach-allegations/). 05.01.2026).***

***

«Канадська організація з регулювання інвестицій (CIRO) повідомляє, що близько 750 000 канадських інвесторів могли стати жертвами витоку персональних даних, що стався минулого року.

За даними CIRO, витік міг торкнутися таких даних, як номери соціального страхування, номери інвестиційних рахунків, номери телефонів тощо.

CIRO заявляє, що на даний момент немає доказів того, що інформація була використана не за призначенням, але організація продовжуватиме стежити за потенційною зловмисною діяльністю.

За даними CIRO, витік даних став результатом складної фішингової атаки, яка була швидко локалізована.

CIRO заявляє, що зв'язується з постраждалими інвесторами, і з 14 січня їм будуть надіслані листи з повідомленням…» ***(CIRO says about 750K people's data affected by cybersecurity incident // CTV News (https://www.ctvnews.ca/sci-tech/article/ciro-says-about-750k-peoples-data-affected-by-cybersecurity-incident/). 14.01.2026).***

***

«Ingram Micro, великий глобальний дистриб'ютор технологій та постачальник послуг ланцюга поставок, повідомив, що в результаті атаки програм-вимагачів були викрадені особисті дані приблизно 42 000 осіб. Компанія, яка співпрацює з такими постачальниками, як Microsoft, Cisco, HP, Apple та безліччю реселерів і постачальників послуг, виявила інцидент 3 липня 2025 року і відключила деякі внутрішні системи, залучивши експертів з кібербезпеки та повідомивши правоохоронні органи. Внутрішнє розслідування встановило, що між 2 і 3 липня неавторизована третя сторона отримала доступ до певних внутрішніх сховищ і викрала з них файли. Ці файли містили записи про працевлаштування та заявників на роботу, що включали імена, контактну інформацію, дати народження, ідентифікаційні номери, видані урядом (такі як номери соціального страхування, водійських посвідчень та паспортів), а також різні деталі, пов'язані з працевлаштуванням, такі як оцінки роботи, хоча конкретні дані, що стали доступними, різняться залежно від особи. Ingram Micro повідомила, що до 9 липня відновила роботу уражених систем і повністю відновила свою діяльність у всьому світі. Хоча компанія не оприлюднила інформацію про зловмисника, група Safepay ransomware взяла на себе відповідальність на своєму сайті Tor leak, заявивши, що викрала 3,5 ТБ конфіденційних даних і пізніше нібито опублікувала їх, що свідчить про провал переговорів про викуп, хоча посилання для завантаження наразі не працює. У відповідь Ingram Micro пропонує постраждалим особам два роки безкоштовних послуг з моніторингу кредитів та захисту особистих даних». ***(Pierluigi Paganini. Ransomware attack on Ingram Micro impacts 42,000 individuals // securityaffairs (https://securityaffairs.com/187083/data-breach/ransomware-attack-on-ingram-micro-impacts-42000-individuals.html). 19.01.2026).***

***

«Дослідник у галузі кібербезпеки Джеремія Фаулер виявив величезну незахищену базу даних, що містила 149 мільйонів викрадених імен користувачів та паролів, зокрема 48 мільйонів облікових записів Gmail, 17 мільйонів Facebook та 3,4 мільйона Netflix, які були доступні для перегляду та використання кіберзлочинцями. Ці облікові дані, зібрані шкідливим програмним забезпеченням, яке непомітно записує натискання клавіш та збережені паролі з інфікованих комп'ютерів, зберігалися без шифрування та захисту, що робило їх легко доступними для пошуку та використання…

Шкідливе програмне забезпечення Infostealer зробило крадіжку паролів такою ж простою, як підписка на стрімінговий сервіс, адже злочинці можуть

орендувати ці інструменти всього за 200–300 доларів на місяць. Вкрадені облікові дані виходять далеко за межі соціальних мереж, включаючи банківські логіни, криптогаманці та урядові акаунти, що дозволяє зловмисникам здійснювати атаки з використанням вкрадених облікових даних і ставити під загрозу все цифрове життя користувачів, особливо з огляду на те, що багато людей використовують одні й ті ж паролі на різних платформах…

Незважаючи на масштаби порушення, такі великі компанії, як Google, Meta, Apple та Netflix, публічно не коментували цей інцидент. Хоча база даних зрештою була видалена, облікові дані, ймовірно, поширювалися на ринках даркнету, що підкреслює, як наші цифрові ідентичності стали цінним товаром у процвітаючій підпільній економіці. Це порушення підкреслює нагальну потребу в кращих практиках гігієни та безпеки паролів, оскільки паролі зараз є валютою на кримінальному ринку…» ***(149 Million Passwords Exposed as Infostealer Malware Turns Logins Into Black Market Inventory // Gadget Review (https://www.gadgetreview.com/149-million-passwords-exposed-as-infostealer-malware-turns-logins-into-black-market-inventory). 26.01.2026).***

***

Кібербезпека Інтернету речей. Штучний інтелект

«Новий звіт Boston Consulting Group показує, що майже 60% африканських компаній за останній рік зазнали кібератак, пов'язаних із штучним інтелектом, але лише половина з них вважає штучний інтелект пріоритетом для посилення своєї кіберзахисту. Незважаючи на очевидну загрозу, африканські компанії відстають від своїх глобальних колег: лише 3% значно збільшили бюджети на кібербезпеку через штучний інтелект (проти 5% у світі), а 82% повідомляють про серйозні труднощі з наймом фахівців з кібербезпеки в галузі штучного інтелекту (проти 69% у світі). Лише 25% вважають свої засоби захисту на основі штучного інтелекту передовими, що створює все більший розрив, оскільки агентський штучний інтелект прискорює еволюцію загроз…

Штучний інтелект значно розширює можливості зловмисників у сфері програм-вимагачів, фішингу, клонування голосу та шахрайства з використанням глибоких підробок. Приклади з практики підкреслюють реальний вплив: шахрайство на суму 25 мільйонів доларів, спричинене глибокою підробкою відео, в якому фігурував фінансовий директор; штраф у розмірі 1 мільйона доларів, накладений регуляторним органом після того, як автоматизовані дзвінки, згенеровані штучним інтелектом, підробили повідомлення виборців; а також атака програм-вимагачів, яка зашифрувала системи лікарні та затримала проведення операцій. Особливо вразливими визнано сектори охорони здоров'я та державного управління.

Протягом наступних двох років африканські керівники вважають найсерйознішими загрозами фінансове шахрайство з використанням штучного інтелекту (43%), соціальну інженерію на основі штучного інтелекту (39%),

прискорене виявлення вразливостей (28%) та адаптивне шкідливе програмне забезпечення на основі штучного інтелекту (26%). У звіті закликають до подвійної моделі лідерства — генеральні директори повинні підвищити кібербезпеку та штучний інтелект до пріоритетів на рівні ради директорів, а керівники служб інформаційної безпеки повинні швидко впровадити високоефективні засоби захисту на основі штучного інтелекту — і попереджають, що організації повинні зараз «відповідати автономії автономією», інакше вони ризикують бути сформованими кіберпростором на основі штучного інтелекту, а не формувати його самі…» ***(Schalk Burger. 60% of African companies faced AI-enabled attacks; 25% of AI defence tools seen as advanced - BCG report // Martin Creamer (https://www.engineeringnews.co.za/article/60-of-african-companies-faced-ai-enabled-attacks-25-of-AI-defence-tools-seen-as-advanced-bcg-report-2026-01-06). 06.01.2026).***

***

«Штучний інтелект трансформує кожен етап роботи медіа та розважальної індустрії, від автоматизованого редагування відео та рекомендаційних систем до сценаріїв, створених за допомогою ШІ. Однак у міру того, як компанії впроваджують алгоритми у виробництво та дистрибуцію, їхня вразливість до атак різко зростає. Кіберзлочинці — і все частіше державні суб'єкти — тепер націлюються на стрімінгові платформи, студії та рекламні технології з метою вимагання викупу, DDoS-шантажу, крадіжки контенту, наповнення облікових даних, шахрайства з використанням фейкових профілів та компрометації ланцюгів постачання. Штучний інтелект сам по собі створює нові ризики: отруєні навчальні дані, вкрадені моделі та маніпулювання контентом на основі підказок, що може спотворити рекомендаційні системи або зашкодити репутації бренду…

Захисники також використовують штучний інтелект, застосовуючи машинне навчання для аналізу журналів, виявлення аномалій та автоматизації реагування на інциденти, але гонка озброєнь триває. Тому основні засоби захисту залишаються життєво важливими:

• Управління ідентифікацією та доступом на основі моделі «нульової довіри» з використанням багатофакторної аутентифікації (MFA) та адаптивних засобів контролю.

• Сегментація мережі та дизайн з мінімальними привілеями, що ізолюють виробничі, пост-виробничі та дистрибуційні середовища.

• Постійне оновлення хмарних та сторонніх інтеграцій, що складають сучасні контент-пайплайни.

• Аналітика безпеки/SIEM, налаштована на сповіщення, специфічні для штучного інтелекту (зсув моделі, незвичайні виклики API, автоматичне сканування).

• Навчання персоналу для протидії все більш переконливим фішинговим та соціально-інженерним кампаніям, що використовують штучний інтелект.

• Сувора гігієна конвеєра штучного інтелекту: перевірка навчальних даних, тестування на наявність ворожих вхідних даних, моніторинг поведінки моделі у виробництві…

На це накладаються зобов'язання США: заходи FTC щодо боротьби з оманливими заявами про безпеку, закони штатів про конфіденційність, такі як CCPA/CPRA, COPPA щодо даних про дітей, обов'язки щодо безпечної гавані DMCA та майбутні правила CIRCIA щодо повідомлення про інциденти. Більшість компаній приводять свої заходи контролю у відповідність до Рамки кібербезпеки NIST, інтегруючи при цьому нові рекомендації NIST щодо ризиків штучного інтелекту…

Плани реагування на інциденти повинні поєднувати технічні заходи з оцінкою репутаційних ризиків: для боротьби з програмним забезпеченням-вимагачем, яке зупиняє пряму трансляцію спортивних подій, або з фейковими відео, що імітують виступи відомих акторів, необхідні скоординовані дії з боку юридичних служб, PR-відділів та керівництва. Регулярні навчальні тренування, що охоплюють такі сценарії, як пошкодження моделей або відключення CDN, підвищують готовність до реагування.

Кіберстрахування все ще доступне, але страховики тепер вимагають доказів «розумної безпеки»: задокументованої дисципліни IAM, сегментованої архітектури, перевірених планів реагування та чітких заходів захисту для моделей штучного інтелекту…

Аналіз ризиків на основі обов'язку дбайливості (DoCRA) надає обґрунтований спосіб продемонструвати, що заходи контролю є пропорційними до шкоди. Наприклад, потоковий сервіс може використовувати DoCRA, щоб обґрунтувати інвестиції в виявлення аномалій на основі штучного інтелекту для пікових подій; студія може продемонструвати, чому попередні версії відеоматеріалів піддаються сильному шифруванню, а рекламні ролики — ні.

Штучний інтелект надає медіакомпаніям безпрецедентну творчу та комерційну силу, але також дає зловмисникам нові автоматизовані засоби для атак. Застосовуючи підхід, заснований на ризиках та обов'язку дбати про безпеку, — реєструючи кожну нову функцію штучного інтелекту з урахуванням можливого зловживання нею — студії, стрімінгові сервіси та видавці можуть монетизувати інновації, зберігаючи при цьому стійку безпеку, що відповідає вимогам регуляторних органів». ***(What's New in the Media and Entertainment Industry with AI and Cybersecurity Risk? // Halock Security Labs (https://www.halock.com/whats-new-in-the-media-and-entertainment-industry-with-ai-and-cybersecurity-risk/). 01.01.2026).***

***

«Агентний штучний інтелект (ШІ) — це автономні системи, які можуть досягати конкретних цілей з обмеженим контролем з боку людини. Це «агенти» ШІ, які сприймають своє оточення, приймають рішення та діють у режимі реального часу. На відміну від традиційних, обмежених правилами інструментів ШІ, які вимагають постійного керівництва з боку людини, агентний ШІ демонструє автономність, цілеспрямовану поведінку та адаптивність, імітуючи аспекти прийняття рішень людиною. Ці можливості викликають зростаючий інтерес з боку американських військових і Конгресу, хоча, як зазначає Центр аналізу інформації з кібербезпеки та інформаційних систем Міністерства оборони (DOD), на даний

момент не існує офіційної політики уряду США, яка б конкретно регулювала агентний ШІ…

У сфері оборони передові військові сили розглядають агентний ШІ як спосіб автоматизації складних завдань зі швидкістю та масштабом, властивими машинам. Потенційні сфери застосування включають ШІ-агенти, які самостійно аналізують розвіддані, пропонують тактичні та стратегічні варіанти, виконують завдання на полі бою та ініціюють або проводять кібероперації, включаючи організовані ШІ кібератаки, які можуть бути спрямовані як на дружні, так і на ворожі ШІ-системи. Декілька підрозділів Міністерства оборони США вже експериментують з такими можливостями. Програма DARPA AI Cyber Challenge (AIxCC) продемонструвала системи штучного інтелекту, які в деяких випадках можуть самостійно виявляти, використовувати та виправляти реальні вразливості програмного забезпечення швидше, ніж люди, з метою зміцнення критичної інфраструктури. Програма Artificial Intelligence Reinforcements (AIR) має на меті навчити автономних «роботизованих крилатих» для повітряних боїв за межами зони видимості в високоточних симуляціях, тоді як Thunderforge прагне інтегрувати ШІ в оперативне планування та планування на рівні театру військових дій, об'єднуючи потоки даних і сенсорів в інструменти підтримки прийняття рішень для командирів. Паралельно з цим, центри аналізу оборонної інформації, такі як DSIAC та CSIAC, збирають та синтезують технічну інформацію про нові технології штучного інтелекту, а у звіті CSIAC за червень 2025 року «Агентний штучний інтелект: стратегічне впровадження в Міністерстві оборони США» викладено приклади використання в Міністерстві оборони та проблеми кібербезпеки…

Водночас агентна ШІ створює нові кіберризики. Оскільки автономні агенти можуть самостійно аналізувати цільові системи, генерувати експлойт-код і просівати великі обсяги викрадених даних, вони можуть дати змогу як досвідченим державним суб’єктам, так і відносно недосвідченим злочинним угрупованням проводити масштабні шпигунські та деструктивні атаки ефективніше, ніж людські команди. Дослідники попереджають, що агентний ШІ може допомогти зловмисникам виявляти та експлуатувати «задні двері» в мережах, імплантувати стійкий шкідливий код та діяти таємно з мінімальним людським наглядом. Яскравий приклад з'явився у вересні 2025 року, коли американська компанія Anthropic повідомила про виявлення «високорозвиненої операції кібершпигунства» з боку китайської групи, спонсорованої державою, яку вона назвала GTG-1002. За даними Anthropic, зловмисники використовували інструменти штучного інтелекту Claude, розроблені самою компанією, для автоматизації приблизно 80–90% глобальної шпигунської кампанії проти близько 30 організацій, в основному шляхом соціальної інженерії, переконавши Claude, що він є авторизованим тестувальником безпеки. Як повідомляється, оператори-люди зосередилися на стратегії, виборі цілей і рішеннях щодо витоку інформації, тоді як ШІ виконував більшу частину оперативної роботи — це стало першим задокументованим випадком кібератаки, організованої ШІ, як назвала його компанія Anthropic. Деякі експерти ставлять під сумнів ступінь автономності, але цей інцидент ілюструє, як швидко зловмисники адаптуються до використання передових технологій ШІ…

З точки зору оборони, агентна ШІ також може посилити кібербезпеку. Автономні агенти, навчені на даних про кіберзагрози, можуть забезпечувати швидке, адаптивне виявлення та реагування в режимі реального часу, усуваючи вразливості та застосовуючи контрзаходи таким чином, як це не можуть зробити традиційні системи, що базуються на правилах. Захист «AI-on-AI» може допомогти впоратися з автоматизованими атаками, виявляючи аномалії, створюючи звіти про інциденти та вживаючи негайних коригувальних заходів, не чекаючи на людських аналітиків. Визнаючи як перспективи, так і ризики таких систем, Конгрес у розділі 1535 Закону про національну оборону на 2026 фінансовий рік доручив міністру оборони створити до 1 квітня 2026 року Керівний комітет з питань майбутнього штучного інтелекту. Цей орган має завдання сформулювати проактивну політику для оцінки, впровадження, регулювання та зменшення ризиків від передових систем ШІ, які є більш потужними, ніж ті, що використовуються зараз, а також проаналізувати траєкторію розвитку передових і нових технологій ШІ, включаючи агентний ШІ та потенційні шляхи до штучного загального інтелекту. Комітет повинен оцінювати розвиток противника, пропонувати стратегії протидії ШІ, оцінювати операційні ефекти інтеграції передових систем ШІ в мережі Міністерства оборони та розробляти стратегію впровадження та нагляду з урахуванням ризиків, а також доповідати про свої висновки Конгресу до 31 січня 2027 року…

Ці події піднімають кілька політичних питань для Конгресу. Законодавці, можливо, повинні будуть розглянути, як агентний ШІ може створити нові вектори атак у кіберпросторі та чи має Міністерство оборони повноваження, ресурси та можливості для виявлення таких загроз і реагування на них. Вони також можуть розглянути, чи слід розширити або зробити обов'язковими для комерційних агентних систем ШІ добровільні партнерства з тестування перед розгортанням, такі як ті, що деякі фірми укладають з Центром стандартів та інновацій у галузі ШІ Міністерства торгівлі, а також які стандарти або обмеження могли б зменшити ризик використання їх противником. Крім того, оскільки Конгрес розглядає питання про поновлення та потенційне розширення Закону про обмін інформацією з питань кібербезпеки після його закінчення в січні 2026 року, він може розглянути, як включити обмін інформацією про загрози, вразливості та найкращі практики, пов'язані з агентною ШІ, між урядом, промисловістю та іншими зацікавленими сторонами». ***(Catherine A. Theohary and Kelley M. Sayler. Agentic Artificial Intelligence And Cyberattacks – Analysis // Eurasia Review (https://www.eurasiareview.com/15012026-agentic-artificial-intelligence-and-cyberattacks-analysis/). 15.01.2026).***

***

«…У звіті «Глобальний прогноз у сфері кібербезпеки на 2026 рік» Всесвітнього економічного форуму зазначається, що штучний інтелект став головним чинником кіберризиків: 94% керівників назвали його найважливішою силою в цій галузі. У 2025 році вразливість, пов'язана зі штучним інтелектом, зростала швидше, ніж будь-яка інша категорія: 87% респондентів повідомили про її зростання, понад третина зазнали витоку даних,

пов'язаного з генеративним штучним інтелектом, а 29% назвали зловмисників, що використовують штучний інтелект, своїм головним страхом. Паоло Дал Чін з Accenture зазначає, що використання штучного інтелекту як зброї, поряд з геополітичними конфліктами, вимагає переходу від традиційного захисту до захисту за допомогою «агентного штучного інтелекту»…

Тим часом вразливість ланцюгів постачання залишається гострою проблемою. Серед великих компаній 65% вказують на ризики, пов'язані з третіми сторонами, як на головну проблему в забезпеченні стійкості (у порівнянні з 54% минулого року), що посилюється концентрацією постачальників у великих хмарних і сервісних провайдерів, де одна-єдина несправність може спричинити ланцюгову реакцію збою. Роб Демейн з e2e-assure попереджає, що навіть безпечні організації наражаються на ризики через своїх партнерів, що є особливою проблемою для складної інфраструктури Великої Британії. У звіті визначено «ризик успадкування» — неможливість перевірити цілісність третіх сторін — як головну небезпеку для ланцюга поставок, проте значущі заходи захисту відстають: лише близько третини компаній комплексно картографують свої екосистеми, а лише 27% проводять спільні навчання з відновлення. Експерти з безпеки закликають ставитися до стійкості ланцюга поставок не як до переліку вимог, а як до динамічного виклику для екосистеми, що вимагає постійної спільної видимості». ***(Emma Woollacott. Supply chain and AI security in the spotlight for cyber leaders in 2026 // Future US, Inc. (https://www.itpro.com/security/supply-chain-and-ai-security-in-the-spotlight-for-cyber-leaders-in-2026). 12.01.2026).***

***

«…У міру поширення штучного інтелекту в різних галузях промисловості кібербезпека стає однією з найпривабливіших довгострокових інвестиційних можливостей, оскільки кожне нове впровадження ШІ створює більше цифрових активів і точок входу, які необхідно захищати. У міру того як компанії вкладають все більше коштів у ШІ — від моделей, що обробляють великі обсяги даних, до фізичних систем, таких як гуманоїдні роботи та автономні транспортні засоби — кожне пристрій, додаток і потік даних стає потенційною мішенню для хакерів. Це значно підвищує стратегічну важливість постачальників послуг кібербезпеки, чиї моделі на основі регулярних доходів та передплати дозволяють їм стягувати більшу плату в міру розширення площі атаки та обсягів даних клієнтів… Водночас кіберзлочинці також використовують ШІ, щоб зробити свої атаки більш витонченими та масштабованими, змушуючи компанії, що займаються безпекою, постійно оновлювати свої інструменти та виправдовуючи вищі ціни на передові засоби захисту. Ця гонка озброєнь може призвести до того, що окремі користувачі та підприємства стануть все більш залежними від спеціалізованих послуг з кібербезпеки. З часом, у міру поширення фізичних продуктів та послуг на основі штучного інтелекту і збільшення обсягу конфіденційних даних, багато організацій, ймовірно, перейдуть на більш високий рівень безпеки, щоб охопити більше кінцевих точок і активів, підвищивши як довічну цінність клієнтів, так і загальний попит на рішення в галузі кібербезпеки…» ***(Marc Guberti. Cybersecurity Can Be The Next Mega Trend Thanks***

To AI // 24/7 Wall St. (https://247wallst.com/investing/2026/01/13/cybersecurity-can-be-the-next-mega-trend-thanks-to-ai/). 13.01.2026).

***

«Швидке поширення Інтернету речей (IoT) змушує кардинально переосмислити кібербезпеку, оскільки конвергенція IT та операційних технологій (OT) робить традиційні моделі безпеки застарілими. Згідно з доповіддю IoT Analytics «2026 OT Cybersecurity Insights Report», у міру того як промислові системи стають підключеними до Інтернету, стандартом стають гібридні архітектури безпеки, що поєднують централізовані та розподілені моделі. Це передбачає створення демілітаризованих зон (DMZ) між IT- та OT-середовищами та прийняття базового принципу «нульової довіри», за яким кожне пристрій та з'єднання постійно перевіряються. Штучний інтелект (ШІ) зараз відіграє центральну роль у цій зміні, перевершуючи системи на основі правил у виявленні аномалій, хоча самі моделі ШІ стали новою поверхнею для атак. У звіті підкреслюється, що майбутній успіх IoT залежить від вбудовування безпеки в дизайн системи з самого початку, а не від її розгляду як додаткової функції…

Прикладом такої інтеграції ШІ та промисловості є лондонська компанія Aibuild, яка розробляє програмне забезпечення на основі ШІ для автономного виробництва. Нещодавно вона отримала стратегічне фінансування від IQ Capital, до якого приєдналися турецька компанія 212 NexT та Driventure від Ford Otosan. Ця інвестиція поєднує глобальний венчурний капітал із турецькою екосистемою глибоких технологій, прискорюючи реалізацію концепції «фізичного ШІ» від Aibuild для 3D-друку та промислової автоматизації. Однак дослідження Mercer, в якому взяли участь майже 12 000 керівників, підкреслює, що однієї технології недостатньо; справжня цінність полягає в перепроектуванні робочих процесів для співпраці людини та штучного інтелекту, а не простому впровадженні штучного інтелекту в існуючі процеси. Хоча 72% інвесторів вважають, що інтеграція людини та штучного інтелекту забезпечує конкурентну перевагу, існує значна розбіжність з керівниками відділів кадрів, а страх співробітників перед втратою роботи зростає, що вимагає прозорої комунікації та перепідготовки…

Тим часом у телекомунікаційному секторі Туреччини компанія Türk Telekom піднялася на друге місце на ринку мобільного зв'язку за кількістю абонентів, використовуючи свою розгалужену оптоволоконну інфраструктуру — понад 535 000 км по всій країні — для підтримки свого зростання в секторі мобільного зв'язку. Компанія, яка досягла найвищих чистих прибутків у сфері перенесення номерів, має на меті забезпечити покриття 5G по всій країні до квітня і використовує штучний інтелект для поліпшення управління клієнтським досвідом». ***(Timur Sırt. IoT expansion forcing rethink of cybersecurity architecture // Turkuvaz Haberleşme ve Yayıncılık (https://www.dailysabah.com/business/tech/iot-expansion-forcing-rethink-of-cybersecurity-architecture). 23.01.2026).***

***

«Влітку 2025 року Мадху Готтумуккала, виконуючий обов'язки директора Агентства з кібербезпеки та безпеки інфраструктури США (CISA),

завантажив конфіденційні, але несекретні контрактні документи з позначкою «тільки для службового користування» у публічну версію ChatGPT. Ця дія викликала кілька автоматичних попереджень безпеки, призначених для запобігання несанкціонованому розголошенню урядових матеріалів. Хоча Готтумуккала отримав спеціальний дозвіл на використання ChatGPT — тоді як для інших співробітників Міністерства внутрішньої безпеки (DHS) доступ до нього залишався заблокованим — його завантаження були помічені сенсорами кібербезпеки CISA, що спричинило проведення внутрішньої перевірки для оцінки потенційної шкоди…

Хоча ці документи не були засекречені, вони містили конфіденційну інформацію, і їх оприлюднення на публічній платформі OpenAI означало, що вони потенційно могли бути використані для відповідей на запити інших користувачів, що викликало занепокоєння з приводу конфіденційності даних та безпеки уряду. Директор з питань громадських відносин CISA заявив, що використання ChatGPT Готтумуккалою було короткочасним, обмеженим і санкціонованим, і підкреслив прихильність агентства до використання штучного інтелекту для модернізації уряду відповідно до виконавчого розпорядження Трампа…

Цей інцидент є особливо примітним, враховуючи місію CISA щодо захисту федеральних мереж від складних кіберзагроз та очікування, що всі федеральні чиновники проходять навчання з питань поводження з конфіденційною інформацією. У перевірці DHS брали участь високопосадовці, зокрема виконуючий обов'язки генерального юрисконсульта та головний інформаційний директор, щоб визначити, чи є підстави для адміністративних або дисциплінарних заходів.

Цей епізод додається до низки суперечок, що відбулися під час перебування Готтумуккали на посаді, включаючи невдалий тест на поліграфі контррозвідки та внутрішні суперечки щодо керівництва. Цей інцидент підкреслює ризики використання публічних інструментів штучного інтелекту для виконання конфіденційної урядової роботи та необхідність суворого дотримання протоколів безпеки навіть на найвищих рівнях керівництва кіберзахисту…» ***(John Sakellariadis. Trump's acting cyber chief uploaded sensitive files into a public version of ChatGPT // POLITICO LLC (https://www.politico.com/news/2026/01/27/cisa-madhu-gottumukkala-chatgpt-00749361). 27.01.2026).***

***

Штучний інтелект, як інструмент боротьби із кіберзлочинністю

«…Національні лабораторії США, які довгий час були центром високозасекречених досліджень у сфері кібербезпеки, починають розкривати прориви в області кіберзахисту на основі штучного інтелекту, що свідчить про те, що уряд, можливо, досяг більшого прогресу в боротьбі з ворожим штучним інтелектом, ніж це публічно демонструється. У Тихоокеанській північно-західній національній лабораторії (PNNL) вчені розробили Aloha, генеративну систему на основі штучного інтелекту, яка дозволяє захисникам швидко моделювати та відтворювати кібератаки на власні мережі. Створена на базі Claude від Anthropic та відкритого фреймворку Caldera від MITRE, Aloha дозволяє аналітикам з безпеки

описувати реальні або гіпотетичні атаки простою мовою; Claude перетворює цей опис на детальну покрокову послідовність атак, яку Caldera потім виконує в контрольованому тестовому середовищі. Aloha спостерігає за моделюванням у реальному часі, перевіряє, чи кожен крок є успішним, автоматично коригує дії, коли атака зупиняється, і дозволяє захисникам неодноразово налаштовувати умови мережі та засоби контролю безпеки, поки вони не знайдуть ефективну оборонну позицію. Це стискає те, що традиційно займало тижні експертного скриптування та аналізу, до значною мірою автоматизованого процесу «натисни та йди», знижуючи бар'єр для організацій, які не мають глибокої внутрішньої експертизи або ресурсів для виконання розширеного моделювання атак…

Aloha з'являється в той час, коли як нападники, так і захисники швидко впроваджують штучний інтелект. Нещодавно компанія Anthropic повідомила, що китайська група, спонсорована державою, використовувала її модель Claude для автоматизації масштабної кампанії кібершпигунства, оператори програм-вимагачів поступово автоматизують свої ланцюги знищення, а команди на минулорічній конференції DEF CON широко використовували штучний інтелект у конкурсах Capture the Flag. За лаштунками національні лабораторні кіберкоманди, включаючи ті, що пов'язані з ядерною програмою США, вже роками використовують моделі OpenAI, тоді як OpenAI співпрацює з Лос-Аламоською національною лабораторією для дослідження безпеки мультимодального штучного інтелекту, а Anthropic працює з Національною адміністрацією ядерної безпеки для розрізнення законного використання в дослідницьких цілях від спроб видобути ядерні секрети. Спираючись на нещодавню роботу DARPA на DEF CON, команда PNNL тепер прагне розширити Aloha, щоб вона могла автоматично тестувати нововиявлені вразливості в системі, перетворювати висновки про вразливість на повні експлойти для перевірки концепції, а потім допомагати розробляти та перевіряти засоби захисту. У сукупності ці зусилля свідчать про зростаючу, обумовлену штучним інтелектом зміну в кіберзахисті, при цьому національні лабораторії тихо розширюють межі автоматизованих адаптивних інструментів, щоб не відставати від дедалі більш активних загроз, пов'язаних зі штучним інтелектом…» ***(Sam Sabin. National labs are quietly making breakthroughs in AI-powered cyber defense // Axios Media Inc. (https://www.axios.com/2026/01/13/pacific-northwest-national-lab-ai-cyber-defense). 13.01.2026).***

***

«У сучасному гіперпідключеному світі традиційні заходи кібербезпеки виявляються недостатніми для протидії все більш витонченим загрозам, таким як фішинг, програми-вимагачі, шкідливе програмне забезпечення та DDoS-атаки. Таке середовище вимагає трансформаційного підходу, який забезпечується інтеграцією прогнозного штучного інтелекту. Прогнозний штучний інтелект використовує алгоритми машинного навчання та аналіз даних, щоб перевести кібербезпеку з реактивної моделі на проактивну, передбачаючи та ідентифікуючи потенційні загрози, перш ніж вони можуть проявитися у вигляді реальних атак…

Переваги впровадження прогнозного штучного інтелекту в кіберзахисті є багатогранними: він дозволяє виявляти загрози на ранній стадії, розпізнаючи аномалії та закономірності у величезних масивах даних у режимі реального часу; він забезпечує автоматизовані реакції, запускаючи протоколи захисту, такі як ізоляція системи або блокування IP-адрес, швидше, ніж можуть зреагувати оператори-люди; він підтримує безперервне навчання, вдосконалюючи моделі за допомогою нових даних для адаптації до нових загроз; він підвищує ефективність використання ресурсів шляхом автоматизації рутинних завдань, дозволяючи IT-командам зосередитися на складних стратегічних питаннях…

Успішне впровадження прогнозного ШІ вимагає ретельного виконання, починаючи з комплексного збору даних з мережевого трафіку, кінцевих точок та зовнішніх джерел загроз. Потім організації повинні вибрати відповідні інструменти безпеки на основі ШІ, навчити свої моделі за допомогою історичних даних та створити структуру для автоматизованих протоколів, які відповідають політикам безпеки та відповідності. Постійний моніторинг та коригування є життєво важливими для підтримання точності. Однак існують певні виклики, зокрема захист конфіденційності даних через необхідність використання великих наборів даних, управління помилковими спрацьовуваннями, які можуть перевантажити команди безпеки, та подолання обмежень ресурсів, необхідних для значних інвестицій у технології та таланти.

У майбутньому роль прогнозного штучного інтелекту розшириться і включатиме вдосконалене прогнозування загроз, глибшу інтеграцію з Інтернетом речей (IoT) для захисту підключених мереж та більш тісну міжгалузеву співпрацю з метою обміну інформацією про загрози. Застосовуючи рішення на основі штучного інтелекту, організації можуть отримати конкурентну перевагу, рухаючись до більш безпечного та стійкого цифрового майбутнього…» ***(Enhancing Cybersecurity with Predictive AI for Automated Attack Defense // QUE.com (https://que.com/enhancing-cybersecurity-with-predictive-ai-for-automated-attack-defense/). 17.01.2026).***

***

«Штучний інтелект у кібербезпеці використовується для більш раннього виявлення загроз, швидшого реагування та підвищення операційної спроможності без збільшення чисельності персоналу шляхом перетворення різноманітних телеметричних даних на події, пріоритетні з точки зору ризику, автоматизації повторюваних дій та задіяння аналітиків для прийняття рішень, що вимагають людського судження. При правильному впровадженні це істотно зміцнює оборонну позицію організації. Моделі штучного інтелекту та машинного навчання чудово справляються з переглядом величезних обсягів журналів та мережевих даних, виявляючи закономірності та аномалії, які можуть бути непомітні для людини. Це дозволяє виявляти вторгнення, шкідливе програмне забезпечення та ненормальну поведінку майже в режимі реального часу, замість того, щоб чекати години або дні, поки будуть помічені незначні відхилення. Крім виявлення, штучний інтелект може координувати та автоматизувати більшу частину робочого процесу реагування — ізолювати кінцеві точки, запускати заходи

з локалізації або передавати людям тільки найскладніші випадки — тим самим скорочуючи час від виявлення до реагування...

Дізнавшись, що є «нормальним» для певного середовища, ШІ може оцінювати та пріоритезувати загрози на основі контексту (хто що зробив, коли, звідки та з якими наслідками), перетворюючи шумні сповіщення на ранжований список, пов'язаний з критичністю бізнесу, щоб системи та дані, які є найціннішими, отримували увагу в першу чергу. Він також підтримує проактивне управління вразливостями та поверхнею атаки шляхом постійного відображення потоків даних, поведінки користувачів та сторонніх скриптів, щоб виявити слабкі місця до того, як ними скористаються, а також шляхом перешкоджання зловмисникам на різних етапах кібернетичного ланцюга вбивств, особливо під час розвідки та озброєння. Оскільки глибоке навчання дозволяє виявляти складні нелінійні закономірності, добре підтримувані моделі здатні адаптуватися до нових і прихованих загроз, за умови, що вони регулярно навчаються, налаштовуються та перевіряються з урахуванням відгуків від команд безпеки для управління помилковими спрацьовуваннями та зміщенням моделі… Водночас штучний інтелект не є панацеєю: супротивники також використовують штучний інтелект для обходу засобів захисту, і необхідно вирішувати практичні питання, такі як якість даних, упередженість, пояснюваність та інтеграція зі старими системами. Справжня цінність проявляється, коли штучний інтелект розглядається як стратегічна здатність, вбудована в надійне управління, надійну гігієну даних, чіткі інструкції та захисні механізми, а також операційну модель «людина в циклі», яка поєднує швидкість машини з людським наглядом та судженням». ***(Meeba Gracy. Real-World Examples of AI in Cybersecurity // Group-IB (https://www.group-ib.com/blog/examples-of-ai-in-cybersecurity/). 20.01.2026).***

***

«Керівники служб інформаційної безпеки швидко впроваджують інструменти безпеки на основі штучного інтелекту для посилення кіберзахисту. 73% осіб, які приймають рішення, зараз схильні обирати рішення на основі штучного інтелекту, що на 59% більше, ніж у минулому році. Дослідження Foundry Security Priorities Study та останні дані PwC показують, що штучний інтелект очолює списки інвестицій у виявлення шкідливого програмного забезпечення, виявлення аномалій, прогнозування ризиків у реальному часі та автоматизовану реакцію, що має на меті зменшити навантаження на аналітиків та прискорити локалізацію загроз…

Однак експерти застерігають, що важливо не піддаватися ажіотажу. Хоча ШІ чудово справляється з обробкою величезних обсягів даних для виявлення аномалій у поведінці та загроз ідентичності на ранній стадії (які часто передують викраденню даних з метою вимагання викупу), багато «ШІ»-продуктів є лише перейменованими застарілими інструментами. Керівники служб інформаційної безпеки повинні ретельно перевіряти досвід постачальників і уникати накладання розрізнених функцій ШІ, які створюють невідповідності в даних…

Успішна реалізація залежить від управління даними: моделі аутентифікації та виявлення на основі штучного інтелекту є ефективними лише за умови належного

контролю ідентичності та якості зразків. Замість того, щоб купувати окремі інструменти, керівники повинні інвестувати в архітектури даних, які розглядають телеметрію безпеки як керований продукт. Надмірна залежність залишається небезпечною — ШІ не може замінити такі основи, як виправлення, сегментація та управління ідентифікацією, а погано навчені моделі можуть створювати «сліпі зони». Зрештою, ШІ приносить користь лише тоді, коли він покращує процес прийняття рішень і зменшує шум, дозволяючи командам запобігати кризам, а не просто швидше на них реагувати…» ***(73% of CISOs more likely to consider AI-enabled security solution // FoundryCo, Inc. (https://www.csoonline.com/article/4120218/73-of-cisos-more-likely-to-consider-ai-enabled-security-solution.html). 22.01.2026).***

***

Штучний інтелект, як зброя кіберзлочинців

«Кіберзлочинці все частіше використовують браузери на базі штучного інтелекту для атак типу «prompt injection» — методу, при якому шкідливі інструкції ховаються у веб-сторінках, документах або електронних листах, щоб змусити агентів штучного інтелекту виконувати шкідливі дії. OpenAI відкрито визнала, що ці атаки є довгостроковим ризиком, властивим дозволу агентам штучного інтелекту вільно пересуватися у відкритій мережі, порівнюючи цю проблему з шахрайством у сфері соціальної інженерії, яке можна пом'якшити, але ніколи повністю усунути. Вразливість є структурною: браузери на базі штучного інтелекту, такі як ChatGPT Atlas від OpenAI, а також конкуренти, такі як Comet від Perplexity, поєднують автономність з доступом до конфіденційних даних користувачів, що означає, що одна прихована підказка може вплинути на дії штучного інтелекту без відома користувача…

Цей ризик посилюється «режимом агента», який розширює площу атаки, дозволяючи ШІ читати електронні листи та виконувати дії від імені користувача. Хоча OpenAI використовує більш швидкі цикли виправлення, безперервне тестування і навіть «автоматизованого зловмисника на основі LLM» для моделювання та виявлення слабких місць, Національний центр кібербезпеки Великобританії попереджає, що ці атаки, можливо, ніколи не будуть повністю усунені. Отже, користувачам рекомендується обмежувати дозволи ШІ, вимагати підтвердження від людини для таких чутливих дій, як покупки або електронні листи, використовувати унікальні паролі за допомогою менеджера паролів та підтримувати надійне антивірусне програмне забезпечення. Оскільки технологія, що лежить в основі браузерів ШІ від великих технологічних компаній, все ще розвивається, рекомендується бути обережними, щоб не стати жертвою цих загроз, що постійно еволюціонують…» ***(Kurt Knutsson. OpenAI admits AI browsers face unsolvable prompt attacks // Yahoo (https://www.aol.com/openai-admits-ai-browsers-face-171026394.html). 04.01.2026).***

***

«Масове поширення штучного інтелекту створило нову еру небезпеки, в якій кібератаки стають все більш витонченими та масштабними, що робить застарілі засоби захисту від кіберзагроз неефективними. Щоб відповісти на виклики сьогодення, організації повинні швидко переосмислити свої системи безпеки та перейти від реактивної до превентивної стратегії…

На 2026 рік прогнозуються три критичні тенденції:

Еволюція загроз: масове персоналізування кібератак порушить класичну модель ланцюга знищення. Зловмисники використовуватимуть штучний інтелект для створення нового, спеціально розробленого програмного забезпечення для кожного підприємства, що призведе до зростання кількості складних загроз, які не можуть бути виявлені за допомогою сучасних засобів безпеки. Ситуація ускладниться через розвиток автономного шкідливого програмного забезпечення, здатного змінювати свій код і поведінку, щоб уникнути виявлення, а також через значне погіршення якості фейкових відео та кампаній соціального інжинірингу на основі штучного інтелекту, які майже не відрізняються від законних комунікацій, що робить залежність від людських захисників неприйнятною…

Розширення площі атаки: пристрої IoT та IT, особливо індивідуальні та застарілі мережеві інфраструктури, стануть основними цілями, оскільки штучний інтелект спрощує створення та здійснення атак на різні операційні системи. Крім того, штучний інтелект сам по собі зараз є основною ціллю, і оскільки він широко інтегрується в корпоративне програмне забезпечення, його автономний характер буде використано для створення загрози, подібної до внутрішньої загрози з боку людини, що призведе до масштабних витоків даних та порушення діяльності підприємств…

Зрілість кіберзлочинності як послуги (CaaS): Підпільна економіка, що базується на штучному інтелекті, змінює ландшафт загроз, надаючи фінансово мотивованим суб'єктам безпрецедентні можливості. Очікується, що у 2026 році CaaS досягне нового рівня складності, що дозволить навіть недосвідченим зловмисникам здійснювати складні багатоетапні кампанії з вражаючою точністю, стираючи межу між опортуністичними та високоорганізованими кіберзлочинними угрупованнями.

Традиційна реактивна модель безпеки не спрацює в світі, де головну роль відіграють зловмисники, що використовують штучний інтелект, а просте додавання штучного інтелекту до застарілих інструментів створить помилкове відчуття безпеки. Підприємствам необхідно терміново перейти до превентивної стратегії, щоб передбачити та уникнути майбутніх атак». ***(Scott Harrell. 3 defining trends for cybersecurity in 2026 // Mansueto Ventures, LLC (https://www.fastcompany.com/91464687/3-defining-trends-for-cybersecurity-in-2026). 02.01.2026).***

***

«Кіберзлочинці підривають довіру до штучного інтелекту, заповнюючи результати пошуку Google сфабрикованими сторінками «розмов» у стилі ChatGPT і Grok, які надають покрокові поради з обслуговування Mac. Відповіді виглядають досконалими і походять з посилань, розміщених на

авторитетних доменах, які часто просуваються за допомогою реклами або SEO. Жертвам, які шукають такі фрази, як «очистити дисковий простір на macOS», пропонують вставити одну команду терміналу. Ця команда непомітно декодує шкідливий скрипт bash і встановлює Atomic macOS Stealer (AMOS), який збирає облікові дані, розширює привілеї і зберігається, не викликаючи звичайних попереджень Apple про завантаження…

Слідчі відстежили десятки таких отруйних діалогів, всі вони були адаптовані до типових запитів про допомогу, що вказує на навмисну кампанію, спрямовану проти користувачів Mac. Схема поєднує два потужні сигнали довіри — рейтинг Google та авторитетний тон штучного інтелекту — приховуючи при цьому підказки зловмисника та розміщуючи корисне навантаження на легальній хмарній інфраструктурі. Оскільки все виконується заздалегідь упакованим у командному рядку, звичайні діалоги інсталятора та перевірки дозволів користувача обходять.

Щоб уникнути зараження, експерти з безпеки радять дотримуватися восьми запобіжних заходів: ніколи не вставляйте команди терміналу з результатів пошуку або штучного інтелекту; розглядайте результати штучного інтелекту як рекомендації та перевіряйте їх за допомогою документації Apple; використовуйте менеджер паролів та інструменти моніторингу порушень; регулярно оновлюйте macOS та браузери; використовуйте антивірус на основі поведінки; ретельно перевіряйте спонсоровані посилання в пошуку; уникайте інструкцій з «очищення/встановлення» з невідомих сайтів; та зупиняйтеся, коли інструкції здаються занадто ідеальними, щоб у них сумніватися. Цей епізод показує, як зловживання штучним інтелектом переносить фішинг з електронної пошти на пошук, і підкреслює, що автентичність, а не якість контенту, повинна стати першим критерієм довіри до онлайн-порад…» ***(Kurt Knutsson. Fake AI chat results are spreading dangerous Mac malware // FOX News Network, LLC. (https://www.foxnews.com/tech/fake-ai-chat-results-spreading-dangerous-mac-malware). 02.01.2026).***

***

«2026 рік стане переломним моментом у сфері кібербезпеки, коли штучний інтелект перетвориться з експериментального інструменту на основний двигун кіберзлочинності, що дозволить здійснювати автономну розвідку, гіперперсоналізовану соціальну інженерію та майже не відрізнити від оригіналу фейкові відео, які зруйнують традиційні методи верифікації. Поряд із цією загрозою, пов'язаною з штучним інтелектом, програмне забезпечення для вимагання викупу перетворилося на багаторівневу економіку вимагання, що поєднує крадіжку даних із підривом репутації, а ідентичність витіснила інфраструктуру як основний вектор атак. Одночасно конвергенція IT та операційних технологій (OT) наражає критичну інфраструктуру на фізичні ризики безпеки, а атаки на ланцюги постачання стали індустріалізованими. Зіткнувшись із посиленням регулювання, таким як правило SEC про розкриття інформації протягом чотирьох днів, NIS2 та DORA, керівники повинні відмовитися від поступового контролю на користь інженерної стійкості за допомогою Zero Trust,

що ставить ідентичність на перше місце, виявлення на основі штучного інтелекту та квантової готовності…

Щоб протидіяти цим загрозам, організації повинні вирішити десять критичних ризиків. Для захисту від шкідливого програмного забезпечення на базі штучного інтелекту та автономних наборів експлойтів необхідні поведінковий аналіз та мови, безпечні для пам'яті. Для боротьби з шахрайством за допомогою глибоких підробок (BEC 2.0) організації повинні застосовувати позасмугове криптографічне підтвердження та відмовитися від багатофакторної автентифікації на основі SMS. Модель багаторазового вимагання викупу вимагає мікросегментації та незмінних резервних копій, а промисловий ланцюжок постачання програмного забезпечення вимагає підписаних артефактів (SLSA/Sigstore) та підтвердження SBOM. Оскільки зловмисники тепер «входять» в систему, а не «зламують» її, використовуючи слабку MFA, впровадження ключів доступу FIDO2/WebAuthn є надзвичайно важливим. OT-середовища вимагають усунення впливу Інтернету та постійного виявлення аномалій, оскільки кіберінциденти тепер становлять фізичну небезпеку. Крім того, керівники повинні забезпечити готовність до виконання вимог SEC, NIS2 та DORA, розпочати перехід на постквантову криптографію для протидії атакам типу «зібрати зараз, розшифрувати пізніше» та управляти суверенітетом даних у гібридних середовищах. Нарешті, щоб подолати обмеження в кадрах, команди повинні автоматизувати рутинні заходи контролю та зосередити внутрішню експертизу на стратегічному моделюванні загроз…

90-денний план дій для керівників включає в себе обов'язкову аутентифікацію, стійку до фішингу, проведення спринту з управління штучним інтелектом для контролю над тіньовим штучним інтелектом, очищення від OT-вразливостей, зміцнення ланцюжка поставок за допомогою підписаних артефактів та впровадження робочих процесів з розкриття інформації відповідно до нормативних вимог. В кінцевому підсумку, кібербезпека в 2026 році вимагає рішучого лідерства, де ідентичність є площиною контролю, штучний інтелект суворо регулюється, а стійкість будується за допомогою цілеспрямованих дій, а не сподівань». ***(Ojo Emmanuel Ademola. Top cybersecurity risks of 2026: Issues, thought processes, and strategic solutions // Businessday Media Limited (https://businessday.ng/life/article/top-cybersecurity-risks-of-2026-issues-thought-processes-and-strategic-solutions/). 11.01.2026).***

***

Кіберзлочинність та кібертероризм

«Європейське космічне агентство (ESA) повідомило про порушення кібербезпеки, яке торкнулося «дуже невеликої» групи зовнішніх серверів, що використовуються для спільних інженерних проектів, підкресливши, що його внутрішня корпоративна мережа та секретні системи не були зачеплені. Інцидент став відомим після того, як хакер, який називає себе «888», оголосив на BreachForums і DarkForums, що 18 грудня 2025 року він проник в інфраструктуру ESA, викравши понад 200 ГБ матеріалів — приватні репозиторії Bitbucket,

вихідний код, CI/CD-пайплайни, API та токени доступу, файли Terraform і SQL, а також інші конфіденційні документи — і зараз пропонує цю скарбницю на продаж виключно в Monero…

ESA повідомляє, що розпочала криміналістичне розслідування, вжила заходів щодо локалізації загрози та повідомила зацікавлені сторони, але ще не перевірила заяви зловмисника та не вказала, які саме сервери були скомпрометовані. Заява агентства нагадує інцидент 2024 року, коли його публічний інтернет-магазин був атакований шкідливим програмним забезпеченням для зчитування даних з карток, що підкреслює постійні ризики, пов'язані з системами третіх сторін та зовнішніми системами. З огляду на ключову роль ESA в європейських космічних дослідженнях та супутникових операціях, слідчі зосередяться на підтвердженні того, які дані були фактично викрадені та чи могли будь-які облікові дані або токени розробників бути використані для глибшого проникнення в середовище агентства. Подальші оновлення будуть опубліковані в міру продовження розслідування». ***(Samiksha Jain. European Space Agency Confirms Cybersecurity Breach on External Servers // The Cyber Express LLC (https://thecyberexpress.com/european-space-agency-confirms-cyber-incident/). 05.01.2026).***

***

«…Кібер-шантаж швидко набирає обертів: з жовтня 2024 року по вересень 2025 року кількість жертв зросла на 45% через поширення кіберзлочинності як послуги (CaaS), що призвело до потроєння кількості окремих злочинних угруповань з 2020 року. Таке поширення дозволяє організованій злочинності легко купувати технічні послуги, роблячи фішинг і вимагання доступними навіть без глибоких технічних знань. Ці атаки посилюються новими техніками соціальної інженерії, включаючи багатоканальні атаки, депфейки та п'ятикратне зростання кількості експлойтів ClickFix, коли користувачів маніпулюють, змушуючи їх виконувати шкідливі команди…

Важливо, що ШІ трансформує фішинг, забезпечуючи високу переконливість персоналізації, бездоганний переклад та масштабовану автоматизовану розвідку. Електронні листи, створені за допомогою ШІ, зараз майже досконалі, що збільшує швидкість і масштаб кампаній, а шахрайство із синтетичною ідентичністю з використанням дипфейків і клонування голосу сприяє шахрайству з боку генеральних директорів/фінансових директорів та проникненню іноземних агентів. Експерти попереджають, що в 2026 році ШІ також буде використовуватися для автоматизації робочих процесів, виявлення вразливостей та створення ШІ-агентів для підготовчих і складних завдань з атак…

Окрім соціальної інженерії, зростають технічні загрози: очікується збільшення кількості зловживань OAuth, які використовують дозволи додатків для збереження постійного доступу до додатків Microsoft 365 та SaaS. Крім того, зловмисники обходять обережність користувачів щодо посилань, поширюючи шкідливі дані через QR-коди та використовуючи файли календаря .ics…

Для керівників служб інформаційної безпеки стратегія повинна виходити за межі інформування користувачів, що є недостатнім для боротьби з депфейками та досконалим фішинговим контентом. Експерти рекомендують впроваджувати

позасмугове підтвердження в робочі процеси з високим рівнем ризику, посилювати процеси багатофакторної автентифікації для протидії фішингу «супротивник посередині» та зосередитися на зміцненні мереж для запобігання поперечному переміщенню та підробці ідентичності, одночасно підтримуючи базову кібергігієну для захисту від постійних низькотехнологічних загроз». ***(Stephen Pritchard. Inside the Cyber Extortion Boom: Phishing Gangs and Crime-as-a-Service Trends // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news-features/inside-the-cyber-extortion-boom/). 02.01.2026).***

***

«Компанія Securonix виявила триваючу кібершпигунську операцію під назвою «PHALT#BLYX», яка спрямована проти європейських готельних компаній і поєднує переконливу соціальну інженерію з інструментами Windows типу «living-off-the-land». Кампанія починається з фішингових електронних листів, які маскуються під повідомлення про скасування бронювання на сайті Booking.com і викликають паніку, повідомляючи про великі штрафи. Жертви, які натискають на вбудоване посилання, потрапляють на переконливий підроблений сайт Booking.com, де бачать фальшиву помилку браузера, а потім підроблений «синій екран смерті» Windows. Потім сайт пропонує їм «виправити» проблему, вставивши заздалегідь завантажений рядок з буфера обміну в поле «Виконати» Windows — це метод «ClickFix», який використовується користувачами і дозволяє обійти багато автоматизованих засобів захисту…

Виконання рядка запускає багатоетапний ланцюжок інфікування: PowerShell запускає легітимний файл MSBuild.exe від Microsoft для компіляції та запуску прихованого проекту, вимикає Windows Defender, встановлює стійкість і, зрештою, запускає налаштовану версію трояна віддаленого доступу DCRat. RAT забезпечує повне віддалене керування, реєстрацію натискань клавіш, виконання команд і подальше поширення шкідливого програмного забезпечення, а процес порожнистості приховує шкідливий код усередині надійних виконуваних файлів Windows. Кириличні рядки налагодження та перекриття інфраструктури вказують на російськомовного зловмисника.

Хоча зараз атаки зосереджені на готельному бізнесі в пікові періоди подорожей, Securonix попереджає, що така ж тактика може бути застосована і в інших секторах. Компанія закликає організації вийти за межі захисту на основі сигнатур і стежити за поведінковими аномаліями та походженням процесів, щоб виявляти такі атаки типу «життя за рахунок землі». ***(Duncan Riley. Securonix warns of malware campaign targeting hospitality sector // SiliconANGLE Media Inc (https://siliconangle.com/2026/01/05/securonix-warns-phaltblyx-malware-campaign-targeting-hospitality-sector/). 05.01.2026).***

***

«Атаки типу «розподілена відмова в обслуговуванні» (DDoS) оточені небезпечними міфами, які можуть зробити організації вразливими. На відміну від поширеної думки, що такі атаки трапляються рідко і спрямовані лише проти великих корпорацій, DDoS-атаки є надзвичайно поширеними: у 2024 році було

зафіксовано понад 15 мільйонів таких атак, які зачіпали підприємства будь-якого розміру та критичну інфраструктуру. Крім того, зловмисники не завжди є досвідченими хакерами; багато хто з них користується недорогими послугами «DDoS-for-hire» (DDoS-атаки на замовлення)…

Іншою помилковою думкою є те, що DDoS-атаки полягають виключно у затопленні мереж величезними обсягами трафіку. Насправді, у 2024 році кількість невеликих, точкових атак на рівні додатків (націлених на DNS і HTTP) зросла на 43%, часто обходячи захист інтернет-провайдерів, призначений лише для великих обсягів трафіку. Аналогічно, атаки на вичерпання стану TCP спеціально націлені на пристрої з підтримкою стану, такі як брандмауери, що спростовує міф про те, що лише брандмауери нового покоління (NGFW) можуть зупинити DDoS-атаки; насправді, їхня підтримка стану робить їх вразливими без бездержавного захисту перед ними…

Покладатися виключно на хмарний захист також недостатньо, оскільки дрібні атаки можуть проникнути крізь нього. Для протидії сучасним багатовекторним атакам необхідна гібридна система захисту, що поєднує хмарні та локальні рішення. Нарешті, штучний інтелект і машинне навчання (AI/ML) зараз є необхідними для захисту, оскільки зловмисники використовують ці технології для підвищення рівня складності атак. Захист на основі AI/ML є критично важливим для виявлення аномалій у трафіку в режимі реального часу та автоматичного коригування контрзаходів для підтримки безперебійної роботи мережі». ***(Brad Christian. 5 myths about DDoS attacks and protection // FoundryCo, Inc. (https://www.csoonline.com/article/4110714/5-myths-about-ddos-attacks-and-protection.html). 05.01.2026).***

***

«Електронна пошта залишається основним вектором кіберзагроз, причому з року в рік кількість загроз стрімко зростає: кількість шкідливого програмного забезпечення в електронній пошті зросла на понад 130%, кількість шахрайських повідомлень — на 30%, а кількість фішингових повідомлень — на 20%. За останні 12 місяців 78% організацій зазнали порушення безпеки електронної пошти, головним чином через фішинг, підробку особи та захоплення облікових записів, які часто перетинаються, сприяючи поширенню програм-вимагачів та втраті даних…

Кіберзлочинці все частіше націлюються на конкретні сектори, причому виробництво вже шостий квартал поспіль зазнає найбільшої кількості атак (26%), за ним йдуть роздрібна торгівля (20%) та охорона здоров'я (19%). В охороні здоров'я застарілі системи та обхідні шляхи користувачів посилюють ризики для даних пацієнтів. Кількість атак типу Vendor Email Compromise (VEC) також різко зросла: зловмисники намагаються викрасти понад 300 мільйонів доларів за один рік. Тривожним є той факт, що 7% співробітників, які стали жертвами однієї атаки, потрапили в пастку і наступної атаки, що підкреслює складність розрізнення законних повідомлень від постачальників…

Тактика атак еволюціонує в бік «низькотехнологічних» методів: кількість спроб фішингових атак із зворотним дзвінком зросла до 16%, тоді як використання

традиційних шкідливих посилань зменшилося. Примітно, що хоча засоби захисту до доставки ефективно блокують шкідливе програмне забезпечення (лише 1% шкідливих електронних листів, що надходять до поштових скриньок, містять його), вони не можуть впоратися з 99% загроз, що базуються на соціальному інжинірингу або фішингу. Ситуацію ускладнює той факт, що дев'ять із десяти електронних листів зараз класифікуються як спам, який все частіше створюється з точністю штучного інтелекту, щоб його було неможливо відрізнити від законних повідомлень». ***(Anamarija Pogorelec. What security teams miss in email attacks // Help Net Security (https://www.helpnetsecurity.com/2026/01/06/rising-email-breach-risks/). 06.01.2026).***

***

«Зловмисник, відомий під псевдонімом «Zestix» (також використовує псевдонім «Sentap»), непомітно зламав облікові записи хмарних сховищ приблизно 50 організацій, використовуючи для цього лише повторно використані імена користувачів та паролі, викрадені за допомогою поширеного шкідливого програмного забезпечення для викрадення інформації. Співробітники цільових організацій в авіаційній, оборонній, медичній, фінансовій та урядовій сферах несвідомо завантажили троянські файли, які запускали RedLine, Lumma або Vidar; зловмисники викрали збережені в браузері облікові дані та надіслали їх до дампів журналів у даркнеті. Zestix прочісував ці дампи в пошуках URL-адрес ShareFile, Nextcloud та OwnCloud, входив у систему та викрадав терабайти даних, оскільки мережі жертв не застосовували багатофакторну автентифікацію…

Серед порушень: компанія Pickett & Associates втратила 139 ГБ карт LiDAR для комунальних підприємств США; Intecro Robotics виточила 11,5 ГБ креслень авіаційних компонентів, що контролюються ITAR; Iberia Airlines оприлюднила 77 ГБ документів з технічного обслуговування та безпеки польотів; а бразильський військово-поліцейський портал Maida Health виточив 2,3 ТБ медичних записів. Багато з викрадених облікових даних циркулювали роками…

Послідовність атаки проста: фішинг або несанкціоноване завантаження → інфостілер виконується в пам'яті та збирає паролі, файли cookie, токени → журнали продаються або поширюються на підпільних ринках → брокер продає доступ до корпоративного хмарового сховища за криптовалюту. За відсутності багатофакторної автентифікації (MFA) Zestix «заходить через парадні двері», а потім перепродає цей початковий доступ іншим злочинцям.

Лікування є настільки ж простим: обов'язково впроваджуйте MFA у кожній хмарній та бізнес-програмі, постійно стежте за ринками інфокрадіїв-логів на предмет витоку корпоративних облікових даних та посилюйте контроль кінцевих точок, щоб блокувати завантаження, що містять шкідливе програмне забезпечення…» ***(Tushar Subhra Dutta. Threat Actors Hacked Global Companies via Leaked Cloud Credentials from Infostealer Infections // Cyber Security News (https://cybersecuritynews.com/threat-actors-hacked-global-companies-via-leaked-cloud-credentials/#google_vignette). 06.01.2026).***

***

«Слідчі Hudson Rock попереджають, що корпоративні портали хмарного зберігання даних масово грабуються злочинцем під псевдонімом «Zestix» (він же «Sentap»). Замість того, щоб використовувати уразливості нульового дня, зловмисник переглядає старі журнали шкідливого програмного забезпечення для викрадення інформації (RedLine, Lumma, Vidar тощо) у пошуках паролів до облікових записів ShareFile, OwnCloud і Nextcloud, які все ще не мають багатофакторної автентифікації. Коли дійсні облікові дані працюють, терабайти даних викачуються і виставляються на аукціон на російськомовних форумах… Близько 50 підприємств в галузі авіації, оборонної робототехніки, охорони здоров'я, комунальних послуг, фінансів та урядової інфраструктури вже втратили від десятків до сотень гігабайтів даних, наприклад, Pickett & Associates (139 ГБ карт електромереж LiDAR), Intecro Robotics (11 ГБ креслень безпілотних літальних апаратів, що контролюються ITAR), Iberia Airlines (77 ГБ даних про технічне обслуговування) та Maida Health (2,3 ТБ військових медичних записів). Багато з викрадених облікових даних роками зберігалися в журналах порушень, що ілюструє, як екосистема інфокрадіїв та відсутність багатофакторної автентифікації (MFA) замінили хакерство методом грубої сили як основний механізм компрометації хмарних сервісів. Zestix, пов'язаний з іранськими та Funksec-колами викрадачів викупу, продає доступ за біткойни або монеро, підкреслюючи необхідність для організацій універсально впровадити MFA та моніторити дампи інфокрадіїв у даркнеті на предмет викрадених облікових даних». ***(Ernestas Naprys. Stolen passwords and no MFA led to 50 major recent breaches // Cybernews (https://cybernews.com/security/fifty-firms-breached-using-stolen-cloud-storage-passwords/). 07.01.2026).***

***

«…Масштабна кібератака на компанію Jaguar Land Rover (JLR) у 2025 році змусила зупинити роботу ключових глобальних систем, від програмного забезпечення для проектування автомобілів і виробництва до постачання запчастин і продажів, що призвело до зупинки виробництва на заводах у Великій Британії, Китаї, Словаччині, Індії та Бразилії на кілька тижнів. У вересні у Великій Британії не було вироблено жодного автомобіля, і хоча в жовтні у Вулвергемптоні було відновлено обмежене виробництво, повне відновлення очікується не раніше початку 2026 року. Ця перерва у роботі викрила вразливість ланцюгів постачання «точно в строк», оскільки роздрібні продавці JLR та постачальники другого і третього рівня зіткнулися з раптовою зупинкою замовлень, а багато хто з них не мав резервів, щоб поглинути цей удар… Понад 200 000 працівників опинилися під загрозою безробіття, багатьом працівникам JLR було наказано залишатися вдома з 1 вересня без чіткої дати повернення, а такі постачальники, як Autins Group і Brose, вдалися до виплати працівникам «накопичених» годин, які будуть відпрацьовані пізніше. Робочі місця залишаються під загрозою в таких компаніях, як Dana, Lear Corporation і Webasto, і профспілки закликали уряд запровадити програму тимчасового звільнення, щоб запобігти масовим звільненням і банкрутствам у всьому ланцюжку поставок.

Ця атака, відповідальність за яку взяла на себе хакерська група Scattered Spider, підкреслює, що кіберінциденти можуть швидко перерости в системні бізнес-кризи. Щоб підвищити готовність, організації повинні посилити виявлення загроз у режимі реального часу, підвищити кіберсвідомість, впровадити структуровані механізми реагування на інциденти та цільові посібники для атак з високим рівнем ризику, забезпечити чітку та скоординовану комунікацію, виконувати нормативні та юридичні зобов'язання, включити стійкість до трудових договорів та політики щодо персоналу, а також посилити загальний рівень безпеки за допомогою додаткових засобів захисту…» ***(Emily Rickard. Jaguar Land Rover cyber-attack — protecting your workforce during digital disruption // Brabners (https://www.brabners.com/insights/data-protection/jaguar-land-rover-cyber-attack-protecting-your-workforce-during-digital-disruption). 13.01.2026).***

***

«Веб-сайт, створений для публікації особистої інформації про співробітників Імміграційної та митної служби США (ICE) та прикордонників, зазнав тривалої кібератаки, яка, на думку його засновника, могла бути здійснена з Росії. Домінік Скіннер, імміграційний активіст з Нідерландів, який управляє веб-сайтом «ICE List», повідомив The Daily Beast, що у вівторок ввечері сайт зазнав масштабної DDoS-атаки (Distributed Denial of Service) незабаром після того, як видання повідомило про його плани опублікувати надані інформатором дані про тисячі співробітників імміграційної служби. Атака супроводжувалася величезним обсягом трафіку з численних IP-адрес, багато з яких, судячи з усього, були російськими, хоча Скіннер зазначив, що використання проксі-серверів робить справжнє джерело фактично не відстежуваним… Він описав операцію як «складну» через її інтенсивність і тривалість. За словами Скіннера, час проведення операції збігся з підготовкою до оприлюднення більшості з приблизно 4500 імен у базі даних, яка, як повідомляється, містить імена офіцерів, адреси електронної пошти, номери телефонів, посади та іншу довідкову інформацію. Він сказав, що мав намір виключити деяких осіб, таких як ті, хто працює в сфері догляду за дітьми або медсестри, з публічного оприлюднення. Дані нібито були надані інформатором Міністерства внутрішньої безпеки після вбивства поліцією 37-річної Рене Гуд у Міннеаполісі. Міністерство внутрішньої безпеки засудило проект ICE List, а його речник назвав його «огидним доксингом», що ставить під загрозу офіцерів та їхні сім'ї, посилаючись на 1300-відсоткове зростання кількості нападів та 8000-відсоткове зростання кількості погроз смерті проти правоохоронців… Держбезпека попередила, що будь-хто, хто оприлюднить особисті дані співробітників, буде притягнутий до відповідальності «в повному обсязі закону», хоча голландський хостинг ICE List знаходиться поза межами прямої юрисдикції уряду США. Скіннер, який заявляє, що його команда має захист від DDoS-атак, але визнає складність повного запобігання таким атакам, вважає, що ці атаки явно спрямовані на блокування доступу до сайту. Він стверджує, що це не тільки не відлякує його, а й зміцнює його рішучість, оскільки ці атаки показують, що є люди, які не хочуть, щоб особистість співробітників ICE та прикордонної служби була оприлюднена, що, на його думку, пов'язано з посиленням критики

їхньої діяльності з боку громадськості». ***(Ariana Baio. Website that leaked thousands of ICE agents' personal information is down after huge 'Russian cyberattack,' founder says // The Independent (https://www.independent.co.uk/news/world/americas/us-politics/ice-information-leak-website-down-russia-cyberattack-b2900713.html). 15.01.2026).***

***

«Betterment, автоматизована інвестиційна служба, нещодавно зазнала атаки соціального інжинірингу, в ході якої неавторизована особа видала себе за довіреного співробітника, отримала доступ до корпоративних поштових систем і надіслала шахрайські повідомлення, пов'язані з криптовалютою, невідомій кількості клієнтів. Хоча Betterment підтвердила, що її технічна інфраструктура та клієнтські рахунки залишилися в безпеці, а паролі та облікові дані не були скомпрометовані, зловмисник отримав доступ до особистих даних клієнтів, включаючи імена, адреси електронної пошти, фізичні адреси, номери телефонів та дати народження. Цей інцидент підкреслює більш широку реальність у сфері кібербезпеки: у міру того, як фінансові компанії розширюють свої технологічні можливості на хмарні сторонні платформи, що підтримують маркетинг та операції, вони стикаються з посиленням загроз, які часто обходять технічні засоби захисту через людську вразливість…

Експерти підкреслюють, що атаки соціального інжинірингу зараз становлять основну загрозу. Максвелл Аллес, засновник компанії Alles Technology, що надає послуги з управління IT та кібербезпекою, зазначає, що «у 21 столітті ми маємо в своєму розпорядженні відповідні інструменти, щоб запобігти більшості технічних порушень; саме шахрайством повинні найбільше перейматися консалтингові компанії». Великі компанії можуть впровадити моніторинг входу в електронну пошту та політику умовного доступу, що обмежує вхід на захищені компанією пристрої — заходи, які могли б запобігти порушенню безпеки Betterment. Менші консалтингові компанії можуть дозволити собі модульні послуги з управління безпекою для аутсорсингового моніторингу. Однак однієї лише технології недостатньо. Пол Остерберг, генеральний директор Security Basecamp, підкреслює, що «без належного управління ризиками, пов'язаними з третіми сторонами, без належного навчання з питань безпеки та обізнаності, що враховує людський фактор, ми завжди будемо мати проблеми з кібербезпекою». Посилення захисту з точки зору соціальної інженерії вимагає всебічного навчання, інструкцій для конкретних ролей, моделювання атак, обізнаності щодо розпізнавання особи та захисних заходів щодо комунікації з клієнтами. «Необхідно створити людський брандмауер», — сказав Остерберг, маючи на увазі щорічну оцінку ризиків, постійний моніторинг та постійне зміцнення змін у поведінці…» ***(Davis Janowski. In Betterment's Recent Social Engineering Incident, a Reminder To Be Cyber Prepared // The Wealth Management Group (https://www.wealthmanagement.com/financial-cybersecurity/betterment-warns-clients-after-cybersecurity-breach-exposes-personal-data). 15.01.2026).***

***

«За останнє десятиліття кількість кіберзлочинів подвоїлася, що робить інтегровану галузь кіберкриміналістики та інформаційної безпеки критично важливою для боротьби з такими сучасними загрозами, як програми-вимагачі та фішинг. Інформаційна безпека (InfoSec) зосереджується на захисті інформаційних систем та забезпеченні конфіденційності, цілісності та доступності, тоді як кіберкриміналістика виступає компонентом розслідування після інциденту. Це структурований процес ідентифікації, збору, аналізу, збереження та представлення цифрових доказів після порушення безпеки з метою визначення того, що сталося, хто несе відповідальність та які дані були скомпрометовані…

Кіберкриміналістика включає такі спеціалізовані галузі, як мережева криміналістика (аналіз журналів трафіку), криміналістика шкідливого програмного забезпечення (розуміння поведінки шкідливого програмного забезпечення) та мобільна криміналістика (витяг даних з пристроїв). Фахівці використовують такі сучасні інструменти, як EnCase, FTK та Wireshark, для проведення розслідувань, дотримуючись суворого процесу ідентифікації, збереження, аналізу, документування та презентації, щоб забезпечити надійність та прийнятність доказів…

Майбутнє цієї галузі швидко розвивається під впливом нових технологій: штучний інтелект і машинне навчання автоматизують складний аналіз даних; хмарна криміналістика адаптує методи розслідування до мінливих хмарних середовищ з багатокористувацьким доступом; криміналістика Інтернету речей зосереджується на взаємопов'язаних пристроях; а криміналістика блокчейну має вирішальне значення для відстеження криптовалюти у випадках шахрайства та вимагання викупу. Випускники цієї галузі мають широкі кар'єрні можливості в уряді, правоохоронних органах, BFSI, IT та охороні здоров'я в якості криміналістичних аналітиків, реагувальників на інциденти та аналітиків шкідливого програмного забезпечення, які відіграють важливу роль у забезпеченні безпеки цифрового світу…» ***(Cyber Forensics and Information Security: A Complete Guide for 2026 // JAIN (Deemed-to-be University) (https://www.jainuniversity.ac.in/blogs/cyber-forensics-and-information-security). 09.01.2026).***

***

«Казино є надзвичайно привабливою мішенню для кіберзлочинців через великі обсяги готівки, великий масив даних про споживачів та складність їх інтегрованих IT/OT-середовищ, які часто є менш захищеними, ніж фінансові мережі. Гучна атака на MGM Resorts, яка спричинила збитки на суму 100 мільйонів доларів після 10-денного припинення діяльності, підкреслила серйозні наслідки таких порушень…

Сучасний ландшафт загроз є надзвичайно широким і охоплює гібридні майданчики, онлайн-платформи та тисячі підключених пристроїв Інтернету речей, від інтелектуальних ігрових автоматів до систем відеоспостереження. Зловмисники використовують різні вектори: програми-вимагачі, DDoS-атаки (значне джерело онлайн-інцидентів), крадіжку даних (особисті дані, дані KYC) та шахрайство (захоплення облікових записів, зловживання бонусами) за допомогою ботів та

викрадених облікових даних. Важливо, що інструменти віддаленого управління сторонніх постачальників постійно визнаються найпоширенішою точкою входу, що дозволяє зловмисникам одночасно компрометувати кілька казино…

Для боротьби з цим необхідна проактивна стратегія кібербезпеки на рівні правління. Найкращі практики включають:

Нульова довіра та сегментація: впровадження системи управління ідентифікацією та доступом (IAM) з обов'язковою багатофакторною автентифікацією (MFA) для всіх співробітників і постачальників, а також мікросегментація мереж (ізоляція слотів, PMS і платіжних систем) для запобігання поперечному переміщенню.

Боротьба із соціальним інжинірингом: визнаючи, що основна загроза пов'язана з людьми, казино повинні проводити постійне навчання співробітників на основі сценаріїв, щоб протистояти індивідуальному фішингу та глибокому фейкуванню, що стало можливим завдяки штучному інтелекту…

Управління штучним інтелектом: встановлення суворого контролю над моделями штучного інтелекту, що використовуються для оцінки ризиків та персоналізації, забезпечення захисту каналів передачі даних від отруєння та зловживання.

Видимість та моніторинг: підтримання видимості в режимі реального часу на величезній поверхні атаки та розробка інструкцій для конкретних гібридних фізичних/онлайн-інцидентів порушення безпеки…

Поза межами 2026 року галузь вступає в «гонку озброєнь у сфері штучного інтелекту», де автономні системи будуть керувати шахрайством та цілісністю, а імерсивні VR/AR-досвід буде покладатися на щільні IoT- та периферійні пристрої, що ще більше розширить поверхню атаки. Зрештою, кібербезпека буде стимулювати довіру ринку і може незабаром стати обов'язковою вимогою для отримання ліцензії». ***(Neil C. Hughes. Casino Cybersecurity 2026: Top Threats & Best Practices // Techopedia (https://www.techopedia.com/casino-cybersecurity). 13.01.2026).***

***

«Рада Інверклайда підтвердила, що нещодавній кіберінцидент, який вплинув на її освітні системи, було локалізовано і що зараз триває поетапне відновлення. У своєму повідомленні рада зазначила, що почала поступово відновлювати облікові записи Microsoft для дорослих, пов'язані з освітою, та відновлювати цифрові освітні послуги, вживаючи «рішучих і рішучих заходів» для безпечного управління ситуацією та оцінки її впливу. Рада, яка співпрацює з відповідними органами, заявила, що не вважає цей інцидент атакою програм-вимагачів, але наголосила, що залишається пильною до постійних кіберзагроз і ставиться до безпеки своїх даних «надзвичайно серйозно». Для забезпечення стабільності та безпеки протягом декількох днів проводиться поетапне ввімкнення облікових записів, а також посилено моніторинг у міру повернення користувачів до систем. Рада продовжуватиме співпрацювати з органами влади та партнерами і зобов'язалася зв'язатися з усіма, хто безпосередньо постраждав від інциденту. Вона принесла вибачення за перебої в роботі та подякувала батькам, опікунам, вчителям

і учням за терпіння під час відновлення роботи служб…» ***(Graham Turner. Inverclyde Council Begins Recovery Following Cyber Incident // DIGIT (https://www.digit.fyi/inverclyde-council-begins-recovery-following-cyber-incident/). 22.01.2026).***

***

«Компанія Nike розпочала розслідування після того, як кіберзлочинна група заявила про крадіжку даних з її систем.

Гігант спортивного взуття та одягу був внесений до списку жертв на веб-сайті витоків інформації на базі Tor, яким керує угруповання WorldLeaks, 22 січня, а таймер показує, що викрадені дані будуть оприлюднені 24 січня, якщо не буде сплачено викуп.

Кіберзлочинці не уточнили, скільки або які саме дані вони нібито вкрали у Nike…» ***(Eduard Kovacs. Nike Probing Potential Security Incident as Hackers Threaten to Leak Data // SecurityWeek (https://www.securityweek.com/nike-probing-potential-security-incident-as-hackers-threaten-to-leak-data/). 24.01.2026).***

***

«Великі спортивні події стали головними цілями для кібератак, і Зимові Олімпійські ігри, які відбудуться наступного місяця в Мілані та Кортіна-д'Ампеццо, не є винятком. За даними Unit 42 компанії Palo Alto Networks, Ігри поєднують у собі все, що шукають зловмисники: щільну критичну інфраструктуру, цінні цілі, такі як спортсмени та офіційні особи, а також підвищену геополітичну напруженість. Минулі інциденти ілюструють ризик. Кампанія «Olympic Destroyer» 2018 року в Пхьончхані, яку приписують російській ГРУ, була спрямована виключно на зрив, а не на фінансову вигоду чи крадіжку даних. Вона на короткий час паралізувала системи продажу квитків, Wi-Fi та публічних дисплеїв під час церемонії відкриття, продемонструвавши, як навіть короткочасні атаки можуть спричинити глобальне збентеження та операційний хаос. Нещодавно відкладені Ігри 2020 року в Токіо та 2024 року в Парижі зазнали хвилі спроб саботажу та DDoS-атак, що підкреслює, що Олімпійські ігри зараз є постійним полем кібербоїв…

Unit 42 бачить кілька загроз для Мілана-Кортіни. Державні групи, особливо з Росії, яка залишається забороненою для участі в Олімпійських іграх, можуть намагатися створити геополітичну нестабільність і нашкодити репутації, потенційно використовуючи позиції, закріплені за кілька місяців або років до цього. Групи хакерів, що використовують програми-вимагачі, ймовірно, розглядатимуть цю подію як вигідну можливість: якщо їм вдасться зламати критично важливі IT-системи в умовах жорстких термінів проведення заходу, жертви можуть бути готові заплатити великі суми, щоб швидко відновити роботу. Складне, федеративне IT-середовище, в якому сотні національних спортивних федерацій підключають свої інфраструктури до центральних олімпійських систем, розширює площу атаки та створює схованки для зловмисників. Хактивісти становлять третю значну категорію, мотивовану не стільки грошима, скільки політичними або ідеологічними цілями; вони можуть націлюватися на конкретних

спортсменів, команди або комітети та виточувати конфіденційні документи, щоб спричинити збій у роботі.

Незважаючи на гучний контекст, основні тактики залишаються звичними. Фішинг через електронну пошту, підроблені сайти з продажу квитків, шкідливі QR-коди, шахрайські додатки, крадіжка облікових даних, використання вразливостей програмного забезпечення та DDoS-атаки — все це очікується, а тепер до цього додаються ще й дипфейки, високо персоналізовані приманки та SEO-отруєння. Unit 42 характеризує Ігри як типовий приклад події, яку надзвичайно важко захистити, але зазначає, що ті самі методи загрожують і звичайним організаціям. Різниця полягає в тому, що більшість підприємств, якщо вони інвестують у зрілі програми безпеки, можуть вжити передбачуваних, проактивних заходів: автоматизація на основі штучного інтелекту для скорочення часу реагування, добре налагоджені SOC, що зменшують кількість помилкових тривог, та постійна оцінка стану безпеки додатків, хмарних активів та середовищ розробки. З наближенням Зимових Олімпійських ігор «цифрова битва» за лаштунками буде вестися за звичними схемами — тільки в масштабах та з інтенсивністю, які роблять будь-яку слабкість, хай навіть найменшу, потенційно глобальною новиною…» ***(Erik van Klinken. What are the cyber threats to the Winter Olympics? // Dolphin Publications B.V. (https://www.techzine.eu/blogs/security/138139/what-are-the-cyber-threats-to-the-winter-olympics/). 21.01.2026).***

***

«Кілька веб-сайтів уряду Люксембургу були тимчасово виведені з ладу у вівторок вранці після того, як державний сектор зазнав кібератаки, підтвердив Державний центр інформаційних технологій (CTIE). Домен «public.lu», на якому розміщені ключові сервіси, включаючи Guichet.lu та медичну страхову компанію CNS, став об'єктом розподіленої атаки типу «відмова в обслуговуванні» (DDoS) між 07:58 та 08:39, що тимчасово порушило доступ до нього. Влада заявила, що проблема була швидко вирішена, і підкреслила, що доступ до конфіденційних даних не був отриманий і вони не були викрадені. З міркувань безпеки CTIE не розкрив масштаби та джерело атаки…

Інцидент стався на тлі різкого зростання кіберактивності проти люксембурзьких установ. У липні 2025 року Post Luxembourg зазнала мережевої атаки, в результаті якої тисячі людей протягом декількох годин залишилися без інтернету та телефонного зв'язку, а раніше того ж року також була атакована веб-сайт Fondation Cancer. Постачальник послуг з кібербезпеки повідомив про 76% зростання кількості кібератак у Люксембурзі в першому кварталі 2025 року порівняно з аналогічним періодом 2024 року. Ця тенденція відображає загальні європейські тенденції, зокрема вересневу атаку на європейського постачальника послуг аеропорту, яка спричинила затримки рейсів у багатьох країнах, серпневу атаку на веб-сайт німецького міста Трір, яка порушила роботу послуг на кілька днів, та великий витік даних у французькій мережі супермаркетів Auchan, який зачепив сотні тисяч клієнтів». ***(Sebastian Offner. Luxembourg state websites briefly disrupted by cyber attack // The Luxembourg Times***

(https://www.luxtimes.lu/luxembourg/luxembourg-state-websites-briefly-disrupted-by-cyber-attack/125330565.html). 21.01.2026).

***

«Урядові керівники з інформаційної безпеки (CISO) та інші високопосадовці закликаються перенести акцент у сфері кібербезпеки з технічної термінології та традиційних загроз на зростаючі ризики фінансового шахрайства, шахрайства з використанням штучного інтелекту, довіри громадян та цілісності даних. У той час як державні та місцеві органи влади стикаються з скороченням бюджетів, нестачею кадрів та зменшенням ресурсів, кіберзлочинці активізують схеми онлайн-шахрайства, які використовують недоліки в управлінні ідентифікаційними даними, викрадені облікові дані та слабкий нагляд. Штучний інтелект погіршує ці проблеми, дозволяючи здійснювати більш складні та масштабні шахрайські схеми, спрямовані як на окремих осіб, так і на державні програми…

Останні дані підкреслюють масштаб проблеми: понад 300 мільярдів доларів шахрайських виплат на боротьбу з пандемією, 25% річне зростання збитків від шахрайства у сфері споживання та глобальний сплеск кібершахрайства. У відповідь на це федеральний уряд започаткував нові ініціативи, такі як створення Відділу з боротьби з національним шахрайством при Міністерстві юстиції, а також двопартійні заклики до посилення запобігання шахрайству в урядових програмах…

Керівникам служб безпеки рекомендується брати участь у заходах щодо запобігання шахрайству, співпрацювати з аудиторами та використовувати аналітику ідентичності та засоби контролю цілісності кінцевих точок. Рекомендації включають обов'язкову позасмугову перевірку платежів, впровадження аналітики поведінки користувачів та організацій (UEBA) для виявлення аномалій, а також забезпечення захисту від мобільних загроз для захисту від крадіжки облікових даних. Акцент робиться на створенні засобів контролю, які передбачають порушення рівня довіри, та на пріоритетності рішень, що враховують реальні бізнес-ризики…

Зрештою, керівники служб інформаційної безпеки повинні очолити боротьбу з шахрайством, пов'язаним із штучним інтелектом, і переконатися, що їхні команди беруть участь у вирішенні проблеми, а не чекають, поки інші почнуть діяти. Послання чітке: боротьба з фінансовим шахрайством в Інтернеті тепер є основним завданням урядової кібербезпеки, що вимагає проактивної взаємодії, міжфункціональної співпраці та зосередження уваги на захисті довіри громадян і репутації уряду». ***(Dan Lohrmann. Cybersecurity's New Business Case: Fraud // e.Republic LLC (https://www.govtech.com/blogs/lohrmann-on-cybersecurity/cybersecuritys-new-business-case-fraud). 25.01.2026).***

***

«Прямі атаки, такі як вішинг (шахрайські телефонні дзвінки) та смішинг (шахрайські текстові повідомлення), використовують терміновість і страх, щоб змусити жертв розкрити конфіденційні дані. На робочому місці Business Email Compromise (BEC) та whaling націлені на співробітників і

керівників, видаючи себе за авторитетних осіб. Інші ризики, такі як підробка бренду та атаки типу «водопій», використовують довіру до відомих організацій або заражають часто відвідувані веб-сайти. Перелік облікових даних та фізичні загрози, такі як підглядання через плече, також становлять значний ризик…

Постійні загрози, такі як шкідливе програмне забезпечення, шпигунське програмне забезпечення та рекламне програмне забезпечення, продовжують завдавати шкоди системам і наражати користувачів на подальші ризики. Хоча кіберзагрози постійно еволюціонують, багатьох з них можна запобігти за допомогою надійних паролів, двофакторної автентифікації, регулярних оновлень програмного забезпечення та обережної поведінки в Інтернеті. Розуміння та усунення цих сучасних кіберризиків є надзвичайно важливим для захисту як особистого, так і професійного цифрового життя…» ***(Samuel Bemi. Understanding modern cyber threats // Vanguard Media Limited (https://www.vanguardngr.com/2026/01/understanding-modern-cyber-threats/). 25.01.2026).***

***

«Складна кібератака серйозно порушила операції з нерухомістю в двох найбагатших районах Лондона, Вестмінстері та Кенсінгтоні і Челсі, паралізувавши їхню здатність обробляти запити місцевих органів влади — важливий етап у процесі купівлі житла. З листопада обидві ради не можуть надавати ці запити, які необхідні для затвердження іпотеки та обережності покупців, що платять готівкою, через що тисячі продажів житла опинилися в підвішеному стані без чіткого терміну вирішення…

Ця атака змусила ради активувати плани дій у надзвичайних ситуаціях і ретельно відновлювати системи під керівництвом експертів з кібербезпеки та правоохоронних органів. Ця перешкода з'явилася на тлі загального спаду на лондонському ринку нерухомості, який посилився через підвищення гербового збору та майбутнє введення податку на нерухомість, що призвело до зниження обсягу продажів дорогої нерухомості на 18% у порівнянні з минулим роком…

Ці два райони, які мають спільну технологічну інфраструктуру, зазвичай обробляють близько 350 операцій з нерухомістю на місяць і отримують значні доходи від гербового збору. Очікується, що затримка, спричинена кібератакою, призведе до затримки продажів нерухомості та зменшення доходів району навіть після відновлення систем. Цей інцидент підкреслює зростаючу загрозу кібератак на критично важливі державні служби у Великій Британії, які, за оцінками урядових досліджень, коштують країні 14,7 млрд фунтів стерлінгів на рік…» ***(Damian Shepherd. London Cyberattack Threatens to Hold Up Thousands of Home Sales // Wells Media Group, Inc. (https://www.insurancejournal.com/news/international/2026/01/27/855827.htm). 27.01.2026).***

***

«Кіберзлочинці розробили складну атаку, спрямовану на розробників, використовуючи платформу GitHub. Кампанія, яка проводилася переважно в

Європі та ЄЕЗ у вересні-жовтні 2025 року, полягала у створенні підроблених версій інсталятора GitHub Desktop, які виглядали як справжні. Зловмисники створили одноразові облікові записи GitHub, скопіювали офіційне сховище GitHub Desktop і змінили посилання для завантаження README, щоб вони вказували на шкідливі інсталятори. Потім вони просували ці заражені файли за допомогою спонсорованих оголошень, націлених на пошукові запити «GitHub Desktop»…

Ключова техніка, відома як «репо-сквотинг», дозволяла зловмисним комітам із видалених форкованих репозиторіїв залишатися видимими в просторі імен офіційного репозиторію, що ускладнювало GitHub виявлення та усунення загроз. Шкідливе програмне забезпечення, замасковане під стандартний інсталятор інструментів розробки, було багатоступеневим завантажувачем і також було виявлено під виглядом інсталяторів для Chrome, Notion, 1Password та Bitwarden.

Технічно, шкідливий інсталятор був додатком .NET, прихованим у виконуваному файлі, схожому на C++, з корисним навантаженням, прихованим у розділі накладення файлу, щоб уникнути базового сканування. Шкідливе програмне забезпечення використовувало API на основі GPU (OpenCL) для запобігання аналізу в стандартних середовищах пісочниці, тактику, яку назвали «GPUGate», що змусило дослідників використовувати фізичні машини з реальним графічним обладнанням для аналізу. Додаткове відволікання уваги коду ще більше ускладнило статичний аналіз і відновлення ключа дешифрування. Ця еволюційна загроза підкреслює необхідність для розробників бути пильними під час завантаження інструментів, а для платформ — посилювати захист від таких оманливих атак…» ***(Tushar Subhra Dutta. Attackers Hijacking Official GitHub Desktop Repository to Distribute Malware as Official Installer // Cyber Security News (https://cybersecuritynews.com/attackers-hijacking-official-github-desktop-repository/). 27.01.2026).***

***

Діяльність хакерів та хакерські угруповування

«Відома кіберзлочинна група Scattered LAPSUS$ Hunters зазнала публічного приниження після того, як в Telegram похвалилася проникненням в системи компанії з кібербезпеки Resecurity, але виявила, що її заманили в пастку. Спочатку група заявила, що отримала повний доступ до внутрішніх чатів Resecurity, даних співробітників і списків клієнтів, висміюючи компанію за те, що вона не змогла захистити себе. Однак Resecurity повідомила, що у відповідь на виявлену в листопаді розвідувальну діяльність вони створили «медовий» обліковий запис з обмеженими правами…

Це змусило зловмисника увійти в емульовану програму, наповнену синтетичними даними, а саме понад 28 000 синтетичних записів про споживачів і 190 000 записів про платіжні операції, які імітували реальну конфіденційну інформацію, але були практично марними. Дослідники Resecurity терпляче стежили за групою, яка 12 грудня відновила свою діяльність, зробивши понад 188 000 запитів на вивантаження та зчитування підроблених даних. Під час цього процесу

зловмисники припустилися критичних помилок, ненавмисно розкривши свої реальні IP-адреси, незважаючи на використання проксі-серверів, що дозволило Resecurity ідентифікувати їхні сервери. Resecurity підтвердила, що ця група є перейменованою версією ShinyHunters з перетинами з Lapsus$ і Scattered Spider, і з того часу передала зібрану інформацію правоохоронним органам». ***(Emma Woollacott. Cyber crime group claims successful attack on security firm, crows about it on Telegram – but it was all an elaborate honeypot // Future US, Inc. (https://www.itpro.com/security/cyber-crime-group-claims-successful-attack-on-security-firm-crows-about-it-on-telegram-but-it-was-all-an-elaborate-honeypot). 05.01.2025).***

***

«…Неформальна мережа хакерів, вимагачів та молодих хижаків, відома як «The Com», діє поза увагою влади, не має керівництва та правил і складається переважно з членів віком від 16 до 25 років, а деякі з них мають лише 11 років. Ця хаотична та жорстока спільнота займається діяльністю, що варіюється від хакерських атак на ігри до серйозних кіберзлочинів, включаючи відключення систем та вимагання, які іноді переростають у реальне насильство. Кіберрозслідувачі та правоохоронні органи намагаються зрозуміти та протистояти The Com, що характеризується поєднанням ігрової культури та хижацького поведінки…

На відміну від традиційних злочинних організацій, The Com не має чіткої структури, що ускладнює боротьбу з нею. Її діяльність варіюється від виведення з ладу систем великих роздрібних мереж і погроз школам до маніпулювання вразливою молоддю з метою спонукання її до самоушкодження та інших злочинних дій. Одна з найвідоміших гілок організації, ShinyHunters, порушила конфіденційність, отримавши доступ до даних користувачів PornHub, що ще раз підкреслило агресивну тактику спільноти…

The Com також застосовує тактику вербування, схожу на тактику сект, де старші члени готують молодших геймерів до вчинення все більш серйозних цифрових злочинів. Використовуючи для спілкування такі платформи, як Discord і Telegram, вони обмінюються незаконним контентом, хваляться успішними хакерськими атаками та сприяють злочинній діяльності. Правоохоронні органи відреагували на зростаючу загрозу: ФБР опублікувало попередження про The Com, щодо діяльності якого різко зросла кількість повідомлень…

Ейден Синотт із Sophos відзначає мінливість між підгрупами, які можна класифікувати як Hacker Com — зосереджені на цифровому шкоді, IRL Com — займаються насильством у реальному житті, та Extortion Com — націлені на неповнолітніх із жорстокими психологічними маніпуляціями. Останні відомі тим, що примушують дітей до таких дій, як самоушкодження, роблячи їх вразливими до подальшої експлуатації. Загроза The Com є динамічною і постійно еволюціонує, представляючи нове покоління кіберзлочинців, які не піддаються традиційній класифікації і становлять серйозну небезпеку для суспільства». ***(Raphael Kahan. From gamers to predators: Inside the internet's most dangerous cybercriminal network***

// ynet Global (https://www.ynetnews.com/tech-and-digital/article/r1rxklwv11g). 04.01.2026).

***

Вірусне та інше шкідливе програмне забезпечення

«…Компанія Koi Security, що спеціалізується на питаннях безпеки, відстежила три великомасштабні кампанії з розповсюдження шкідливих розширень для браузерів — ShadyPanda, GhostPoster і нещодавно виявлену Zoom Stealer — до одного добре фінансованого китайського суб'єкта, який отримав назву «DarkSpectre». Загалом ці кампанії заразили приблизно 8 мільйонів інсталяцій розширень для Chrome, Edge і Firefox…

• Zoom Stealer (18 підроблених додатків, що імітують Google Meet, Zoom, GoTo Webinar тощо) заразив 2,2 мільйона користувачів. Хоча ці розширення надають легітимні функції відеоконференцій, вони непомітно викрадають інформацію про корпоративні зустрічі — URL-адреси з вбудованими паролями, ідентифікаторами, списками учасників, даними про організаторів та деталями планування — через WebSocket на сервери C2, що розміщені в Alibaba-Cloud…

• ShadyPanda, виявлена на початку грудня, вразила 5,6 мільйона користувачів, викравши дані, перехопивши пошукові запити та здійснивши афілійовані шахрайські схеми.

• GhostPoster приховує шкідливий JavaScript у файлах логотипів розширення Firefox, надаючи зловмисникам повний контроль над браузером після його встановлення…

Серед підказів щодо авторства є коментарі до коду китайською мовою, реєстрація ICP, що вказує на Хубей, інфраструктура Alibaba Cloud та шахрайська діяльність, спрямована на внутрішні сайти електронної комерції JD.com і Taobao. Дослідники Koi попереджають, що, на відміну від рекламного ПЗ, орієнтованого на споживачів, інструменти DarkSpectre становлять «інфраструктуру корпоративного шпигунства», збираючи конфіденційні дані про зустрічі від підприємств, які довірилися, на перший погляд, нешкідливим доповненням». ***(Gintaras Radauskas. 2.2M Chrome, Firefox, Edge users impacted by meeting-stealing malware // Cybernews (https://cybernews.com/security/darkspectre-malicious-browser-extension-campaign/). 02.01.2026).***

***

«…Складний ботнет RondoDoX посилив свою дев'ятимісячну кампанію (березень–грудень 2025 р.) проти інфраструктури підприємств, продемонструвавши безжальний багатоетапний підхід до компрометації. Згідно з даними, отриманими з відкритих журналів команд і контролю, кампанія розпочалася з ручного тестування вразливостей, у квітні переросла в автоматичне щоденне сканування, а з липня 2025 р. посилилася до щогодинних спроб розгортання…

Шкідливе програмне забезпечення працює шляхом сканування вразливих систем, розгортання бінарних файлів ELF та встановлення стійкості за допомогою завдань cron, одночасно агресивно припиняючи роботу конкуруючого шкідливого програмного забезпечення, щоб монополізувати ресурси для криптомайнінгу та роботи ботнету. Ботнет RondoDoX підтримує кілька архітектур процесорів і використовує кілька резервних механізмів завантаження, щоб забезпечити доставку корисного навантаження в гетерогенних середовищах…

Найбільш тривожна подія сталася в грудні 2025 року, коли зловмисники швидко використали критичну вразливість Next.js для розгортання React2Shell, продемонструвавши здатність групи швидко адаптуватися до нових вразливостей. Організації, що використовують маршрутизатори, камери та додатки Next.js, підключені до Інтернету, наражаються на безпосередній ризик. Основні заходи захисту включають сегментацію мережі, негайне виправлення вразливих додатків, розгортання брандмауерів веб-додатків та блокування виявленої інфраструктури управління та контролю на периферійних брандмауерах». ***(Tushar Subhra Dutta. RondoDoX Botnet Weaponizing a Critical React2Shell Vulnerability to Deploy Malware // Cyber Security News (https://cybersecuritynews.com/rondodox-botnet-weaponizing-a-critical-react2shell/). 02.01.2026).***

***

«Шкідливе програмне забезпечення Stealc — це прихована та вдосконалена загроза, що викрадає інформацію та поширюється за моделлю «шкідливе програмне забезпечення як послуга» (MaaS), що робить його легко доступним для кіберзлочинців. Поширюючись переважно через фішингові електронні листи, підроблені інсталятори програмного забезпечення та оманливі веб-сайти, Stealc тихо працює у фоновому режимі, використовуючи техніки заплутування, щоб уникнути виявлення. Його основною метою є вилучення конфіденційних даних з веб-браузерів, включаючи збережені паролі, файли cookie, дані автозаповнення та інформацію про сеанси, а також дані про гаманці з криптовалютою та системні файли. Ці викрадені дані потім виводяться на сервери, контрольовані зловмисниками, для використання в шахрайстві, захопленні облікових записів або перепродажу…

Шкідливе програмне забезпечення становить серйозну довгострокову загрозу, оскільки воно здатне обходити традиційні системи входу в систему шляхом крадіжки сеансів, що призводить до фінансових втрат і потенційного ризику для бізнесу. Розповсюдження цього програмного забезпечення значною мірою базується на зловживанні довірою користувачів за допомогою термінових тактик соціальної інженерії та підроблених брендів. Захист від Stealc вимагає багаторівневого підходу: забезпечення кінцевих точок за допомогою розширеного захисту, оновлення систем, уникнення ненадійних завантажень, увімкнення багатофакторної автентифікації (MFA) та посилення безпеки електронної пошти. Такі рішення, як StrongBox IT, забезпечують необхідний захист, пропонуючи моніторинг загроз у реальному часі, виявлення схем збору облікових даних та блокування шкідливих виконуваних файлів, перш ніж вони отримають доступ до конфіденційних даних…» ***(Charles Paul. What is Stealc Malware? // Techstrong***

Group Inc. (https://securityboulevard.com/2026/01/what-is-stealc-malware/). 05.01.2026).

***

«Дослідники в галузі кібербезпеки виявили надзвичайно складну кампанію з розповсюдження шкідливого програмного забезпечення, спрямовану проти виробничих і урядових організацій в Італії, Фінляндії та Саудівській Аравії, в якій використовується завантажувач, спільний для декількох груп зловмисників. В операції застосовуються різноманітні вектори зараження — збройові документи Office, що використовують CVE-2017-11882, шкідливі файли SVG та ZIP-архіви з ярликами LNK — всі вони замасковані під законні повідомлення про замовлення на поставку, щоб доставити багатошаровий корисний вантаж…

Ланцюжок атак демонструє передові техніки ухилення: фішингові електронні листи призводять до заплутаного JavaScript, який запускає приховані процеси PowerShell, завантажує зображення PNG з Archive.org, що містять вбудовані стеганографічні корисні дані, і використовує витяг регулярних виразів для завантаження збірки .NET у пам'ять для безфайлового виконання. На третьому етапі використовується троянізована бібліотека TaskScheduler з відкритим кодом з GitHub, перекомпільована зі шкідливими функціями, для виконання порожнистості процесів за допомогою RegAsm.exe. Кінцевим корисним навантаженням є PureLog Stealer, розшифрований і розпакований для викрадення промислових даних та адміністративних облікових даних…

Послідовне використання в цій кампанії стеганографії, маніпулювання рядками та введення процесів через декілька векторів вказує на наявність стандартизованої, спільної інфраструктури атак, що дозволяє різним зловмисникам здійснювати складні атаки з низьким рівнем виявлення та мінімальними слідами для криміналістичного розслідування». ***(Tushar Subhra Dutta. Threat Actors Leverage Commodity Loader to Attack Organizations in Targeted Email Campaigns // Cyber Security News (https://cybersecuritynews.com/threat-actors-leverage-commodity-loader/). 06.01.2026).***

***

«Нещодавно виявлена кампанія з поширення шкідливого програмного забезпечення для macOS використовує підроблену версію чат-бота Grok AI Ілона Маска для зараження комп'ютерів Apple і таємного видобутку криптовалюти. Компанія Mosyle, що займається безпекою пристроїв Apple, виявила операцію «SimpleStealth», в рамках якої зловмисники зареєстрували схожий домен (xaill.com) і розмістили підроблений інсталятор Grok.dmg поза межами Mac App Store. Після інсталяції шкідливе програмне забезпечення виглядає як легальне і уникає виявлення антивірусом, виконуючи приховані фонові процеси. Незвично, що його код має явні ознаки того, що він принаймні частково згенерований великою мовною моделлю, змішуючи англійську та бразильську португальську мови з безладними поясненнями та повторюваною логікою — це свідчить про те, що генеративний штучний інтелект вже використовується для

прискорення розробки шкідливого програмного забезпечення… Корисне навантаження — це прихований криптомайнер Monero, який активується лише тоді, коли Mac перебуває в режимі очікування протягом приблизно хвилини, і зупиняється, як тільки користувач відновлює активність, що допомагає уникнути підозр. Експерти з безпеки застерігають користувачів від завантаження програмного забезпечення з сторонніх сайтів або невідомих URL-адрес і рекомендують користуватися лише Mac App Store або послугами перевірених постачальників, перевіряючи веб-адреси та уникаючи непотрібних форм. Хоча цей конкретний штам спочатку проник повз антивірусні інструменти, використання надійного програмного забезпечення для безпеки Mac разом із вбудованим XProtect від Apple, а також дотримання правил «кібергігієни» та обізнаність про нові загрози залишаються критично важливими для зменшення ризику зараження та компрометації даних». ***(Scott Younker. Fake Grok app built using generative AI discovered spreading malware on macOS devices // Future US, Inc. (https://www.tomsguide.com/ai/grok/fake-grok-app-built-using-generative-ai-discovered-spreading-malware-on-macos-devices). 12.01.2026).***

***

«Нещодавно виявлена платформа шкідливого програмного забезпечення VoidLink є важливою віхою в розвитку кіберзагроз, оскільки вважається першою просунутою платформою шкідливого програмного забезпечення, яка в основному створена за допомогою штучного інтелекту. За даними Check Point Research, VoidLink — це складна платформа шкідливого програмного забезпечення для Linux, що містить спеціальні завантажувачі, імпланти, модулі руткітів та десятки плагінів для розширення функціональних можливостей. Аналіз показав, що VoidLink, ймовірно, був розроблений одним китайським розробником з високими навичками програмування, який використовував AI-асистент, вбудований в TRAE IDE, для швидкого створення шкідливого програмного забезпечення…

Порушення операційної безпеки з боку розробника призвели до витоку вихідного коду, документації та планів спринтів, що дало дослідникам можливість безпосередньо ознайомитися з процесом розробки на основі штучного інтелекту. Розробник використовував Spec-Driven Development (SDD) для визначення цілей та обмежень проекту, що дозволило ШІ створити комплексний план розробки для декількох команд та значну частину кодової бази. Незважаючи на те, що план передбачав термін реалізації від 16 до 30 тижнів, VoidLink досяг функціонального стану з 88 000 рядків коду всього за один тиждень.

Дослідники Check Point підтвердили, що документація, створена штучним інтелектом, і фактичний вихідний код майже повністю збігалися, і їм вдалося відтворити робочий процес, продемонструвавши, що агент штучного інтелекту може генерувати складний код шкідливого програмного забезпечення, що раніше було під силу лише великим командам з великими ресурсами. VoidLink знаменує початок нової ери, в якій окремі зловмисники, озброєні штучним інтелектом, можуть розробляти сучасне шкідливе програмне забезпечення з безпрецедентною швидкістю та в безпрецедентних масштабах…» ***(Bill Toulas. VoidLink cloud malware shows clear signs of being AI-generated // Bleeping Computer® LLC***

(https://www.bleepingcomputer.com/news/security/voidlink-cloud-malware-shows-clear-signs-of-being-ai-generated/). 20.01.2026).

***

«Північнокорейські зловмисники, які стоять за тривалою кампанією Contagious Interview, вдосконалили свою тактику і тепер використовують шкідливі проекти Microsoft Visual Studio Code (VS Code) для доставки бекдорів на цільові кінцеві точки. Дослідники в галузі безпеки повідомляють, що ці зловмисники заманюють інженерів-програмістів, особливо тих, хто працює в галузі криптовалют, блокчейну та фінтеху, даючи їм вказівку клонувати репозиторій GitHub, GitLab або Bitbucket і відкрити його в VS Code в рамках нібито оцінки роботи. Атака використовує файли конфігурації завдань VS Code, які налаштовані на автоматичне виконання шкідливих програм при відкритті папки проекту…

Ланцюг інфікування включає зашифрований JavaScript, який зв'язується з віддаленими серверами, завантажує додаткові корисні дані та встановлює постійний доступ через «задні двері» для віддаленого виконання коду, зчитування відбитків системи та викрадення даних. Шкідливе програмне забезпечення, включаючи такі варіанти, як BeaverTail та InvisibleFerret, здатне здійснювати кейлоггінг, захоплення знімків екрана, викрадення даних з буфера обміну, крадіжку облікових даних та майнінг криптовалюти. Зловмисники використовують резервні механізми, такі як маскування шкідливого програмного забезпечення під словники перевірки орфографії або шкідливі залежності npm, щоб забезпечити успішне зараження…

Дослідники помітили, що шкідливе програмне забезпечення швидко розвивається, з ознаками генерації коду за допомогою штучного інтелекту, і що зловмисники експериментують з різними методами доставки, щоб досягти максимального успіху. Ця кампанія підкреслює зростаючу витонченість і адаптивність кібершпигунських груп, пов'язаних з КНДР, які використовують легальні робочі процеси та інструменти розробників для компрометації цілей. Розробникам рекомендується бути обережними з репозиторіями сторонніх розробників, перевіряти вихідний код перед відкриттям у VS Code та встановлювати тільки перевірені пакети npm, щоб зменшити ці загрози…» ***(Ravie Lakshmanan. North Korea-Linked Hackers Target Developers via Malicious VS Code Projects // The Hacker News (https://thehackernews.com/2026/01/north-korea-linked-hackers-target.html). 20.01.2026).***

***

«Північнокорейська хакерська група Konni (також відома як Opal Sleet або TA406), яка діє з 2014 року і пов'язана з APT37 та Kimsuky, зараз використовує шкідливе програмне забезпечення PowerShell, створене за допомогою штучного інтелекту, для атак на розробників та інженерів блокчейну в Азіатсько-Тихоокеанському регіоні. Дослідники Check Point проаналізували зразки з Японії, Австралії та Індії і виявили, що атака починається з

посилання, розміщеного на Discord, яке доставляє ZIP-файл, що містить PDF-приманку і шкідливий ярлик LNK…

При натисканні LNK запускає завантажувач PowerShell, який витягує DOCX-приманку та CAB-файл, що приховує бекдор, пакетні скрипти та інструмент для обходу UAC. Приманка-документ націлена на середовища розробки з метою викрадення API-ключів, облікових даних гаманців та криптоактивів. Потім заплановане завдання встановлює стійкість під виглядом процесу OneDrive, запускаючи з пам'яті скрипт PowerShell, зашифрований за допомогою XOR.

Примітно, що код бекдору має явні ознаки використання штучного інтелекту: чітка модульна структура, надзвичайно детальні коментарі та характерний рядок-заповнювач — «# <– ваш постійний UUID проекту» — типовий для результатів роботи великих мовних моделей. Шкідливе програмне забезпечення виконує антианалітичні перевірки, генерує унікальний ідентифікатор хоста та запитує сервер управління та контролю щодо подальших інструкцій. Check Point приписує цю кампанію Konni на основі форматів запускаючих програм та збігів інфраструктури, а також опублікував індикатори компрометації, щоб допомогти захисникам блокувати загрозу…» ***(Bill Toulas. Konni hackers target blockchain engineers with AI-built malware // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/konni-hackers-target-blockchain-engineers-with-ai-built-malware/). 24.01.2026).***

***

«Нова багатоетапна кампанія атакує російських користувачів за допомогою Amnesia RAT і викрадача даних, похідного від Hakuna Matata, використовуючи соціальну інженерію, а не експлойти нульового дня для повного компрометації системи. Fortinet повідомляє, що атака починається із ZIP-архівів, які містять файли LNK з подвійним розширенням (наприклад, «Задание_для_бухгалтера_02отдела.txt.lnk»), які при відкритті запускають завантажувач PowerShell, розміщений на GitHub, одночасно відображаючи фальшивий документ, щоб відволікти увагу жертви…

Завантажувач приховує вікно консолі, сповіщає зловмисника через Telegram і через 444 секунди завантажує сильно зашифрований скрипт Visual Basic. Цей скрипт збирає наступний корисний вантаж у пам'яті, примусово підвищує рівень UAC і нейтралізує засоби захисту: виключає ключові папки зі сканування, вимикає адміністративні інструменти Windows і використовує інструмент «defendnot», щоб змусити Microsoft Defender вимкнути себе, зареєструвавши підроблений антивірусний продукт…

Після зниження рівня безпеки шкідливе програмне забезпечення встановлює модуль для створення знімків екрана та два основних корисних навантаження з Dropbox. Amnesia RAT («svchost.scr») викрадає облікові дані з браузерів, гаманців, Discord і Steam, записує аудіо/відео та забезпечує повне дистанційне керування. Програма-вимагач шифрує файли користувача, припиняє роботу процесів, що заважають, та захоплює буфер обміну криптовалютою. Нарешті, компонент WinLocker заморожує екран, даючи жертвам вказівку зв'язатися з зловмисником…

Ця операція аналогічна іншим недавнім кампаніям проти російських корпоративних цілей, таким як «Операція DupeHike» UNG0902 (доставка AdaptixC2 за допомогою приманок на тему бонусів) та створені штучним інтелектом приманки Paper Werewolf, що встановлюють бекдор EchoGather. Захисникам рекомендується увімкнути захист від несанкціонованого втручання та контролювати виклики API, щоб блокувати такі інструменти, як defendnot». ***(Ravie Lakshmanan. Multi-Stage Phishing Campaign Targets Russia with Amnesia RAT and Ransomware // The Hacker News (https://thehackernews.com/2026/01/multi-stage-phishing-campaign-targets.html). 24.01.2025).***

***

«Атаки на браузери стають дедалі більш витонченими та небезпечними, про що свідчить поява в січні 2026 року набору інструментів Stanley для створення шкідливого програмного забезпечення як послуги. Вартість Stanley становить від 2000 до 6000 доларів. Цей інструмент дозволяє зловмисникам показувати користувачам підроблені веб-сайти, тоді як в адресному рядку браузера продовжує відображатися справжній URL-адресу, що робить крадіжку облікових даних та фінансових даних дуже переконливою…

Виявлений на російськомовних форумах, присвячених кіберзлочинності, Stanley продається з гарантією публікації в Chrome Web Store, що дозволяє завантажувати шкідливе розширення, замасковане під легальний додаток для нотаток і закладок під назвою «Notely», безпосередньо з офіційного магазину Google. Після встановлення розширення надає зловмисникам майже повний контроль над діяльністю жертви в Інтернеті. За допомогою веб-панелі управління зловмисники вибирають цілі, налаштовують правила перехоплення та накладають повноекранні фішингові сторінки поверх справжніх веб-сайтів, при цьому легальний домен залишається видимим в адресному рядку.

Stanley використовує IP-адресу жертви як унікальний ідентифікатор, що дозволяє здійснювати точне таргетування та відстеження між пристроями. Розширення кожні десять секунд зв'язується зі своїм сервером управління та контролю для отримання оновлених інструкцій і використовує ротацію резервних доменів для збереження стійкості навіть у разі виведення з ладу основних серверів. Тисячі користувачів вже стали жертвами атаки…

Щоб зменшити такі загрози, підприємства повинні застосовувати суворі правила щодо дозволених розширень, а користувачі повинні мінімізувати кількість встановлених розширень і ретельно перевіряти запити на дозвіл. Більш загальною проблемою є те, що магазини розширень для браузерів часто схвалюють розширення один раз, дозволяючи зловмисним оновленням проникати пізніше, що підкреслює необхідність постійної пильності та поліпшення безпеки магазинів». ***(Tushar Subhra Dutta. New Malware Toolkit Sends Users to Malicious Websites While the URL Stays the Same // Cyber Security News (https://cybersecuritynews.com/new-malware-toolkit-sends-users/). 26.01.2026).***

***

«Програми-вимагачі перетворилися з ІТ-неприємності на критичний стратегічний ризик, про що свідчать нещодавні кампанії таких груп, як Scattered Spider (UNC3944), які обходять традиційні технічні засоби захисту за допомогою витончених методів соціальної інженерії та зловживання ідентифікаційними даними. Атаки перенесли фокус на компрометацію людських процесів, таких як використання голосового фішингу для обману служб технічної підтримки з метою скидання облікових даних, тим самим отримуючи легітимний доступ до корпоративних систем і підриваючи багатофакторну автентифікацію. У міру того, як організації проходять цифрову трансформацію, зловмисники використовують сучасну ІТ-інфраструктуру та системи єдиного входу для переходу між локальними та хмарними середовищами, перетворюючи обмежені вторгнення на повномасштабні компрометації…

Отже, ідентичність стала новим периметром безпеки, що вимагає від рад директорів підвищити її захист до стратегічного пріоритету, рівного традиційним засобам контролю. Ради директорів повинні стимулювати інвестиції в аутентифікацію, стійку до фішингу, узгодити витрати на безпеку з реальними даними про загрози та забезпечити, щоб нагляд за кіберризиками був інтегрований у зусилля з цифрової трансформації з самого початку. Виходячи за межі реактивної оборони та інтегруючи кіберризики в управління, ради директорів можуть захистити стійкість, інновації та довіру від ескалації загроз від програм-вимагачів». ***(Jamie Collier. Identity: the new perimeter of ransomware defence // TechTarget, Inc. (https://www.computerweekly.com/opinion/Identity-the-new-perimeter-of-ransomware-defence). 05.01.2026).***

***

«…У 2025 році програмне забезпечення для вимагання викупу зупинило виробництво Jaguar Land Rover у Великобританії на місяць, що коштувало 260 мільйонів доларів на відновлення та 650 мільйонів доларів на подальші збитки — це приклад того, як цифровізація без безпеки залишає виробництво вразливим. Автоматизація, хмарні технології та штучний інтелект набувають все більшого поширення: за даними Deloitte, 57% великих американських виробників зараз використовують хмарні технології, а 29% — штучний інтелект/машинне навчання на рівні заводів або мереж; Північна Америка вже займає половину світового ринку хмарних технологій у виробництві. Однак застарілі операційні технології (OT) ніколи не були розроблені для підключення до мережі. Звіт IBM X-Force за 2025 рік показує, що виробництво є найбільш уразливою галуззю вже четвертий рік поспіль…

Ризики:

• Старі PLCs та HMI, з'єднані з хмарними/ШІ-платформами, розширюють площу атаки.

• Взаємопов'язані постачальники та інтегратори ланцюга поставок створюють численні слабкі місця.

• Хмара централізує конфіденційні проекти та рецептури; один зламаний обліковий запис може спричинити ланцюгову реакцію на всіх заводах.

• Набори даних ШІ, завантажені до сторонніх інструментів, можуть бути розкриті або використані для навчання зовнішніх моделей.

Основні заходи щодо зменшення ризиків:

Класифікуйте дані та шифруйте особисту інформацію та власні розробки під час зберігання та передачі.

Впровадьте сегментацію між IT, хмарою та OT, щоб порушення безпеки не поширювалися на виробничі лінії.

Ставтеся до наборів даних ШІ як до цінних активів; перевіряйте компоненти моделей постачальників та політику зберігання даних.

Контролюйте використання сторонніх та неформальних інструментів, щоб усунути «тіньову штучну інтелігенцію».

Використовуйте MFA, часто встановлюйте оновлення та застосовуйте надійне управління ключами; «додані» засоби безпеки більше не є ефективними.

Розрахуйте ймовірні збитки, щоб обґрунтувати інвестиції в безпеку; більші витрати не завжди означають більшу безпеку…

Виробники повинні привести архітектуру безпеки у відповідність до складності своїх цифрових заводів, а не сповільнювати інновації, гарантуючи, що підключений завод майбутнього буде побудований на відповідній моделі безпеки». ***(Sakshi Udavant. Cyber risks grow as manufacturers turn to AI and cloud systems // TechTarget, Inc. (https://www.ciodive.com/news/cyber-risks-grow-as-manufacturers-turn-to-ai-and-cloud-systems/808776/). 05.01.2026).***

***

«У 2025 році активність програм-вимагачів знову зросла — компанія Recorded Future зафіксувала приблизно 7200 публічно розкритих інцидентів, що на 47% більше, ніж у 2024 році, — проте загальний дохід і середній розмір викупу зменшилися. Щоб компенсувати скорочення прибутку, оператори змінюють тактику трьома помітними способами…

Комплексні пропозиції DDoS-for-hire в RaaS. Зменшивши розмір комісійних, решта команд ransomware-as-a-service тепер покращують пакети для партнерів, додаючи можливості розподіленого відмови в обслуговуванні, як це вже робить нова група Chaos. Захисники повинні очікувати, що загрози шифрування або крадіжки даних будуть поєднуватися з атаками на пропускну здатність, і забезпечити, щоб плани запобігання DDoS охоплювали такий сценарій.

Агресивний набір співробітників зсередини. Все частіше наймають посередників, для яких англійська є рідною мовою, щоб вони налагоджували контакти з працівниками — одна група навіть обрала своєю мішенню журналіста BBC — з метою отримання облікових даних або встановлення шкідливого програмного забезпечення. Звільнення можуть збільшити цей ризик у 2026 році. Організаціям потрібні більш потужні програми захисту від внутрішніх загроз, моніторинг аномалій та навчання персоналу, що акцентує увагу на спробах зовнішнього набору співробітників…

Використання платформ для фрілансерів. Коли віддалений доступ не працює, деякі злочинні угруповання зараз наймають нічого не підозрюючих фрілансерів-технічних підрядників, щоб ті заходили в офіси і виконували завдання на місці, як зазначено в рекомендаціях ФБР. Тому процедури фізичної безпеки та перевірки відвідувачів повинні з обережністю ставитися до «законних» викликів сервісних служб…

З огляду на майбутнє, Recorded Future прогнозує, що 2026 рік стане першим роком, коли кількість нових учасників ринку програм-вимагачів за межами Росії перевищить їхню кількість всередині країни, що підкреслює швидку глобалізацію цієї моделі злочинності, а не зниження активності російських учасників.

Висновок: слід посилити захист від DDoS-атак, посилити внутрішній та фізичний контроль і припустити, що тактика програм-вимагачів буде продовжувати диверсифікуватися у міру зменшення прибутків». ***(Allan Liska. New ransomware tactics to watch out for in 2026 // Recorded Future (https://www.recordedfuture.com/blog/ransomware-tactics-2026). 05.01.2026).***

***

«Компанія Group-IB, що спеціалізується на кібербезпеці, забила на сполох щодо нової родини програм-вимагачів під назвою DeadLock, яка відрізняється тим, що зловживає смарт-контрактами блокчейну Polygon для управління шкідливою інфраструктурою. Смарт-контракти — це самовиконуючі програми на блокчейні, які автоматично застосовують заздалегідь визначені правила без посередників; у цьому випадку оператори DeadLock використовують їх як недостатньо задокументований механізм для зберігання та ротації адрес проксі-серверів. Вбудовуючи інформацію про проксі-сервери в контракти Polygon, зловмисники можуть генерувати практично нескінченні варіанти своєї інфраструктури, що ускладнює її відстеження та блокування захисниками і дозволяє їм використовувати децентралізовані блокчейни по всьому світу для обходу традиційних засобів захисту. Вперше помічений у липні 2025 року, DeadLock є незвичайним тим, що він не пов'язаний з жодною відомою партнерською програмою програм-вимагачів і не має сайту для витоку даних, а відносно невелика кількість повідомлень про жертв дозволила йому залишитися практично непоміченим… Group-IB визначила свої основні цілі на даний момент як організації в Італії, Іспанії та Індії. Хоча початковий вектор доступу все ще невідомий, аналіз показує використання AnyDesk для віддаленого моніторингу та контролю, а потім видалення різних служб та тіньових копій для максимізації впливу. Потім шкідливе програмне забезпечення шифрує файли, додаючи розширення «.dlock», змінює піктограми файлів і шпалери жертви, а також інструктує жертв через записку з вимогою викупу, як діяти далі. Хоча на даний момент вплив здається обмеженим, Group-IB попереджає, що DeadLock нещодавно відновив свою діяльність, розгорнувши новий проксі-сервер, а його інноваційне використання смарт-контрактів свідчить про розвиток навичок, які можуть стати набагато небезпечнішими, якщо не вжити заходів на ранній стадії…

Поява DeadLock вписується в більш широку тенденцію кіберзлочинців, які використовують технології блокчейну та смарт-контракти як зброю. Google раніше

попереджав, що північнокорейський зловмисник UNC5342 використовує техніку під назвою «EtherHiding», яка зберігає та отримує шкідливі дані через транзакції на публічних блокчейнах для доставки шкідливого програмного забезпечення та крадіжки криптовалюти — підхід, який є дуже стійким до традиційних заходів з видалення та блокування. Приблизно в той же час дослідники ReversingLabs виявили два пакети шкідливого програмного забезпечення з відкритим кодом у репозиторії npm, які використовували смарт-контракти Ethereum для завантаження шкідливого програмного забезпечення на скомпрометовані пристрої. У сукупності ці події показують, що смарт-контракти та децентралізовані реєстри стають дедалі привабливішою та стійкішою основою для управління, доставки корисних навантажень та маскування інфраструктури. Таким чином, малопомітне, але технічно досконале зловживання смарт-контрактами Polygon компанією DeadLock є ранньою ознакою того, як можуть розвиватися програми-вимагачі та інші загрози, якщо організації та захисники не пристосують свої стратегії виявлення та реагування до цього нового класу технологій, що базуються на блокчейні». ***(Emma Woollacott. There's a dangerous new ransomware variant on the block – and cyber experts warn it's flying under the radar // Future US, Inc. (https://www.itpro.com/security/ransomware/deadlock-ransomware-polygon-smart-contract-abuse). 14.01.2026).***

***

«Коли відбувається атака програм-вимагачів, для управління кризовою ситуацією мобілізується спеціалізована екосистема страхових компаній, юристів та компаній з реагування на інциденти (IR). Страхові компанії координують загальне реагування, юридичні фірми займаються управлінням кризовими ситуаціями, дотриманням нормативних вимог та переговорами про викуп, а компанії IR та переговорники виступають посередниками у відносинах із зловмисниками, щоб мінімізувати виплати та сприяти відновленню даних…

Однак нещодавно ця система зазнала серйозного удару через грубе порушення довіри. Двоє колишніх співробітників IR-компаній, Раян Кліффорд Голдберг (раніше працював у Sygnia) та Кевін Тайлер Мартін (раніше був переговірником у DigitalMint), визнали себе винними у змові з групою BlackCat, що займалася вимаганням викупу, з метою викрасти понад 9,5 мільйонів доларів у американських компаній у період з 2023 по 2025 рік. Американські чиновники засудили зраду, зазначивши, що обвинувачені використовували свої знання в галузі кібербезпеки для вчинення тих самих злочинів, яким вони повинні були запобігати…

Цей інцидент висвітлює структурний конфлікт інтересів: багато компаній, що займаються реабілітацією, надають як послуги з ведення переговорів (з метою мінімізації виплат), так і послуги з обробки платежів (які можуть приносити вищі комісії залежно від складності та розміру викупу). Критики стверджують, що це створює невідповідні стимули, особливо для компаній, які не стягують фіксованих комісій, оскільки більші викупи можуть опосередковано збільшити доходи компаній, що займаються реабілітацією.

Coveware, компанія з реагування на інциденти, придбана Veeam, відрізняється тим, що працює за фіксованою платою за кожен інцидент і відмовляє клієнтам, яких направляють зловмисники, прагнучи розірвати «зв'язки» між перемовниками та злочинцями. Генеральний директор Coveware Білл Сігель виступив перед Конгресом із заявою про необхідність обов'язкового повідомлення та запропонував галузі кібервимагання взяти за приклад усталену модель фіксованої плати, яка використовується у сфері викрадення та викупу (K&R). Цілісність усієї галузі реагування на інциденти зараз перебуває під пильною увагою, а справа DigitalMint є суворим нагадуванням про те, що загроза для бізнесу може походити зсередини самої команди реагування…» ***(James Baratta. Ransomware Recovery Firms Share in the Hacking Spoils // The American Prospect, Inc. (https://prospect.org/2026/01/08/ransomware-recovery-firms-share-hacking-spoils/). 08.01.2026).***

***

«…У листопаді 2025 року нещодавно виявлена родина програм-вимагачів під назвою Osiris атакувала велику компанію з надання послуг харчування в Південно-Східній Азії, що ознаменувало появу нової складної загрози, відмінної від варіанту 2016 року з такою ж назвою. Аналітики Symantec пов'язали цю атаку з групою програм-вимагачів «Inc» через технічні збіги, зокрема використання Rclone для викрадення даних у хмарне сховище Wasabi та конкретної версії Mimikatz («kaz.exe») для вилучення облікових даних. Атака продемонструвала передові тактики, зокрема використання спеціального шкідливого драйвера під назвою «Poortry» (або «Abyssworker») в атаці Bring-Your-Own-Vulnerable-Driver (BYOVD). Замаскований під легальне програмне забезпечення Malwarebytes, цей самостійно розроблений драйвер дозволив зловмисникам вимкнути засоби захисту на рівні ядра — це значне підвищення рівня складності порівняно з використанням існуючих вразливих драйверів. На додаток до цього, зловмисники використовували такі інструменти, як Netexec, Netscan і модифікований Rustdesk (замаскований під WinZip) для збереження доступу. Сам викрадач Osiris використовує гібридне шифрування ECC і AES-128-CTR, припиняє роботу баз даних і служб резервного копіювання, а також видаляє знімки томів, щоб запобігти відновленню, що свідчить про роботу досвідчених операторів…» ***(Tushar Subhra Dutta. New Osiris Ransomware Using Wide Range of Living off the Land and Dual-use Tools in Attacks // Cyber Security News (https://cybersecuritynews.com/new-osiris-ransomware-using-wide-range-of-tools/). 22.01.2026).***

***

Фішингові атаки

«…Дослідники в галузі кібербезпеки виявили складну фішингову кампанію, яка зловживає службою інтеграції додатків Google Cloud для розповсюдження шкідливих електронних листів із законної, надійної адреси

(noreply-application-integration@google.com). Ця техніка дозволяє електронним листам, які імітують звичайні корпоративні повідомлення, такі як сповіщення про голосові повідомлення або запити на спільний доступ до файлів, обходити традиційні фільтри безпеки, використовуючи вбудовану довіру, пов'язану з інфраструктурою Google Cloud…

Кампанія, яка була спрямована на приблизно 3200 клієнтів з різних глобальних секторів протягом 14 днів у грудні 2025 року, використовує завдання «Надіслати електронний лист» в Application Integration для надсилання власних електронних листів на довільні адреси, ефективно обходячи перевірки DMARC і SPF. Ланцюг атак являє собою багатоетапний потік перенаправлення: одержувачі, які натискають на вбудоване посилання, розміщене на надійному сайті storage.cloud.google.com, спочатку потрапляють на підроблену сторінку CAPTCHA, яка блокує автоматичні сканери безпеки, а потім перенаправляються на підроблену сторінку входу в Microsoft для викрадення їхніх облікових даних Microsoft 365…

Check Point зазначила, що кампанія в першу чергу націлена на сектори, які залежать від автоматизованих сповіщень та спільних робочих процесів, такі як виробництво, технології та фінанси. Дослідники також помітили, що кампанія еволюціонувала і тепер включає фішинг з використанням згоди OAuth, а також використовує Amazon Web Services (AWS) S3 для розміщення підроблених сторінок входу, що демонструє стратегію зловмисників, які використовують ланцюжок надійної інфраструктури — Google, Microsoft та AWS — для досягнення максимального успіху. З того часу Google заблокував конкретні фішингові спроби, що зловживали функцією повідомлень електронною поштою». ***(Ravie Lakshmanan. Cybercriminals Abuse Google Cloud Email Feature in Multi-Stage Phishing Campaign // The Hacker News (https://thehackernews.com/2026/01/cybercriminals-abuse-google-cloud-email.html). 02.01.2026).***

***

«Flare, лідер у сфері управління загрозами, опублікував дослідження під назвою «Економіка фішингових комплектів на ринках кіберзлочинності» , яке розкрило, як сучасний фішинг перетворився на зрілу, орієнтовану на послуги тіньову економіку.

Результати дослідження показали, що комбіновані набори, створені для імітації цілих кластерів сервісів в одному розгортанні, є двигуном сучасного фішингу. Flare виявив, що 43,8% учасників використовували ці попередньо упаковані набори інструментів та ресурсів для фішингу для масштабування з одним набором, що означало багато жертв і багато шляхів монетизації.

Ґрунтуючись на аналізі понад 8600 обговорень на підпільних, глибоких та темних веб-платформах, а також на платформах обміну повідомленнями, звіт Flare розкриває, як фішингові комплекти та платформи «Фішинг як послуга» (PhaaS) розроблені для масштабування, швидкості та монетизації, дозволяючи навіть низькокваліфікованим гравцям обходити багатофакторну автентифікацію (MFA), красти сесії та захоплювати облікові записи з тривожною ефективністю.

Звіт показує, що сучасні фішингові операції більше не обмежуються географією, мовою чи технічними знаннями. Комплекти створюються в одному

регіоні, продаються в іншому та розгортаються по всьому світу, часто протягом кількох годин…» ***(Mark Bowen. Flare research reveals nearly half of all cybercriminals use multi-brand combo kits to steal data // A Intelligent Global Media Brand (https://www.intelligentciso.com/2026/01/15/flare-research-reveals-nearly-half-of-all-cybercriminals-use-multi-brand-combo-kits-to-steal-data/). 15.01.2026).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Міністерство юстиції США (DOJ) оголосило, що два фахівці з кібербезпеки, Кевін Мартін з Техасу та Раян Голдберг з Джорджії, визнали себе винними у змові з метою вимагання за свою участь у сумнозвісних атаках з використанням програм-вимагачів BlackCat/Alphv. Мартін, колишній переговірник з питань програм-вимагачів у DigitalMint, та Голдберг, менеджер з реагування на інциденти в Sygnia, були серед трьох осіб, яким у жовтні було висунуто звинувачення у зломі корпоративних систем, крадіжці даних та використанні програми-вимагача BlackCat… Підозрювані були учасниками партнерської програми BlackCat, сплачуючи 20% від суми викупу адміністраторам операції в обмін на доступ до шкідливого програмного забезпечення та платформи для управління вимаганням, і, за повідомленнями, отримали 1,2 мільйона доларів у біткойнах від однієї жертви. Визнання провини відбулося лише через кілька днів після того, як інший учасник програми-вимагача, Артем Стрижак, визнав свою провину в окремій справі. Мартіну і Голдбергу загрожує до 20 років в'язниці, вирок буде винесено 12 березня 2026 року. Операція BlackCat, яка була спрямована проти понад 1000 організацій, була припинена правоохоронними органами наприкінці 2023 року, перш ніж група здійснила остаточну аферу з виходу після отримання викупу в розмірі 22 мільйонів доларів від Change Healthcare». ***(Eduard Kovacs. Two US Cybersecurity Pros Plead Guilty Over Ransomware Attacks // Wired Business Media (https://www.securityweek.com/two-us-cybersecurity-pros-plead-guilty-over-ransomware-attacks/). 02.01.2026).***

***

«Компанія Microsoft очолила глобальну операцію з ліквідації RedVDS, платформи для кіберзлочинності як послуги на базі штучного інтелекту, яка з березня 2025 року сприяла збиткам від шахрайства на суму щонайменше 40 мільйонів доларів (34 мільйони євро) лише в США, причому реальна цифра, ймовірно, є вищою через недооцінку. За всього 24 долари (21 євро) на місяць RedVDS продавала злочинцям доступ до дешевих віртуальних комп'ютерів з неліцензійним програмним забезпеченням, включаючи Windows, які використовувалися для розсилки фішингових листів, розміщення шахрайської інфраструктури та здійснення масштабних шахрайських схем під прикриттям анонімності. Ця послуга часто поєднувалася з генеративними інструментами

штучного інтелекту для виявлення високоцінних цілей і створення переконливих ланцюжків електронних листів, а також з технологіями заміни обличчя, маніпулювання відео та клонування голосу для імітації довірених осіб. Однією з найпоширеніших схем, що використовували RedVDS, було шахрайство з перенаправленням платежів, або компрометація ділової електронної пошти, коли зловмисники перехоплювали законні електронні листи та перенаправляли кошти, видаючи себе за справжніх контрагентів. Основна увага приділялася шахрайству з перенаправленням платежів у сфері нерухомості, коли зловмисники компрометували рахунки ріелторів, ескроу-агентів та титульних компаній, щоб надсилати шахрайські інструкції, які викачували кошти з рахунків та ескроу-платежів. Серед жертв були такі сектори, як початкова та середня освіта, споживчі товари та професійні послуги по всій Європі, особливо сильно постраждали Великобританія, Франція, Німеччина, Італія та Іспанія; серед співпозивачів у справі Microsoft є компанія H2-Pharma з Алабами, яка втратила кошти, призначені для лікування раку, ліків для психічного здоров'я та дитячих ліків від алергії…

Зусилля з ліквідації поєднували цивільний судовий процес і скоординовані дії правоохоронних органів у різних юрисдикціях. Підрозділ Microsoft з боротьби з цифровими злочинами подав позов у Південному окрузі Флориди і вперше розпочав паралельні судові дії у Великобританії, тоді як німецькі органи влади та Європейський центр з боротьби з кіберзлочинністю Європолу вжили заходів для вилучення ключової інфраструктури. Прокуратура Німеччини у Франкфурті та Державне кримінальне управління поліції у Бранденбурзі взяли під контроль критично важливий сервер, на якому працював веб-сайт RedVDS, відрізавши ринок, де злочинці підписувалися на послугу та керували нею. Європол координує ліквідацію додаткових європейських серверів, які активно використовуються клієнтами RedVDS, порушуючи роботу ширшої мережі, що лежить в основі шахрайських дій. Microsoft підкреслила, що жертви таких атак не повинні відчувати сором, оскільки вони є результатом діяльності організованих професійних злочинних угруповань, які перехоплюють і маніпулюють законними повідомленнями між довіреними сторонами. Щоб зменшити ризик подібних шахрайств, компанія закликала організації та приватних осіб не поспішати і ставити під сумнів термінові запити на оплату, перевіряти зміни через відомі канали зв'язку, використовувати багатофакторну автентифікацію, ретельно перевіряти адреси електронної пошти на наявність незначних змін, оновлювати програмне забезпечення та негайно повідомляти про підозрілу діяльність правоохоронним органам…» ***(European schools and businesses hit as Microsoft disrupts global cybercrime subscription service // Euronews (https://www.euronews.com/next/2026/01/14/european-schools-and-businesses-hit-as-microsoft-disrupts-global-cybercrime-subscription-s). 14.01.2026).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Наприкінці грудня 2025 року спільнота з кібербезпеки була стурбована розкриттям інформації про Mongobleed (CVE-2025-14847) — вразливість високого рівня небезпеки, пов'язану з розкриттям пам'яті до аутентифікації в сервері MongoDB, яка дозволяє неаутентифікованим зловмисникам викрадати конфіденційні дані безпосередньо з пам'яті сервера. Ця вразливість, що має оцінку CVSS 8,7, впливає на понад 87 000 потенційно вразливих екземплярів MongoDB по всьому світу. CISA підтвердила, що вона активно експлуатується в реальних умовах, а федеральним агентствам було встановлено термін усунення вразливості до 19 січня 2026 року…

Вразливість виникає через неправильну обробку заголовків мережевих повідомлень, стиснутих за допомогою zlib, що дозволяє неправильно сформованим повідомленням обдурити сервер і змусити його повернути неініціалізовану пам'ять кучі, що містить залишки конфіденційних даних, таких як облікові дані бази даних, ключі API та PII. Критична небезпека полягає в векторі атаки до аутентифікації, який обходить усі традиційні засоби контролю доступу, такі як паролі та MFA, що робить будь-який сервер, підключений до Інтернету, з увімкненим стисненням zlib, негайно вразливим…

Інцидент Mongobleed, який нагадує вразливість Heartbleed 2014 року, наочно демонструє, що організації не можуть покладатися на єдиний засіб захисту. Ключовим уроком у сфері захисту є сегментація мережі: сервери баз даних ніколи не повинні бути безпосередньо доступними з публічного Інтернету. Організації також повинні вживати заходів одразу після виправлення вразливості: оскільки стався витік неініціалізованого вмісту пам'яті, усі потенційно скомпрометовані секретні дані, включаючи паролі до баз даних та облікові дані хмарних сервісів, необхідно негайно замінити після застосування виправлень.

Швидка мілітаризація, коли публічний експлойт-код стає доступним вже через кілька днів після розкриття, підкреслює необхідність швидкого виправлення вразливостей та повної видимості інвентаризації активів, включаючи тіньові IT-бази даних. Організаціям, що використовують непідтримувані версії MongoDB (3.6, 4.0, 4.2), необхідно негайно здійснити міграцію, а тимчасовим обхідним рішенням є вимкнення стиснення zlib для усунення вразливого коду. Цей інцидент підкреслює, що безпека баз даних вимагає комплексного виявлення загроз і захисту під час виконання, що виходить за межі традиційних засобів захисту периметра…» ***(Guru Baran. Lessons From Mongobleed Vulnerability (CVE-2025-14847) That Actively Exploited In The Wild // Cyber Security News (https://cybersecuritynews.com/mongobleed-vulnerability-2/). 02.012026).***

***

«Компанія Microsoft виправила серйозну вразливість у своєму персональному AI-асистенті Copilot, яка дозволяла зловмисникам викрадати конфіденційні дані користувачів одним кліком на, здавалося б, легітимний URL-адресу Copilot. Ця вразливість була виявлена і використана в контрольованому тесті дослідниками з безпеки компанії Varonis, які продемонстрували, що, вбудувавши ретельно розроблений запит в параметр URL-адреси (параметр q), вони могли змусити Copilot надсилати особисту інформацію, включаючи секретні дані користувача, ім'я, місцезнаходження та деталі з історії чату Copilot, на сервер, контрольований зловмисниками. Важливо, що експлойт, названий «Reprompt», продовжував працювати навіть після того, як користувач закрив вкладку чату Copilot, і обходив засоби безпеки кінцевих точок та засоби контролю виявлення підприємств, оскільки вся активність відбувалася в рамках нормальної поведінки веб-сайту та Copilot після натискання на посилання…

Атака працювала шляхом зловживання основною слабкістю великих мовних моделей: нездатністю надійно відрізнити надійні вхідні дані користувача від ненадійних інструкцій, вбудованих у зовнішні дані (непряме введення підказки). Зловмисний URL вказував на домен, контрольований Varonis, і містив довгу «загадку» природною мовою в параметрі q, яка давала Copilot вказівку сформувати і прослідкувати конкретні URL, надіслати секретні дані і контекст до веб-хука, а потім отримати додаткові приховані інструкції з файлу, який виглядав як .jpg. Ці вторинні інструкції спонукали Copilot отримати додаткові приватні дані (такі як ім'я користувача і місцезнаходження) і надіслати їх через додаткові веб-запити. Microsoft намагалася запобігти такому витоку даних за допомогою захисних бар'єрів, але Varonis виявила, що ці захисні заходи застосовувалися лише до початкового запиту; оскільки введений запит явно вказував Copilot повторювати кожен виклик функції, другий і наступні запити обходили захисні бар'єри і успішно витокували приватні дані в декілька етапів…

Varonis розкритикував цю конструкцію як невдалу модель загрози, пов'язану з непрямим введенням команд і багатоступеневими ланцюжками запитів. Після того, як Varonis приватно повідомив про цю проблему, Microsoft оновив Copilot, щоб заблокувати продемонстрований шлях атаки; станом на вівторок експлойт Reprompt більше не працює. Вразливість вплинула тільки на Copilot Personal — Microsoft 365 Copilot не постраждав. Цей інцидент підкреслює більш широку проблему забезпечення безпеки помічників на основі LLM, де ненадійні інструкції, заховані в посиланнях, файлах або іншому вмісті, можуть перехопити поведінку моделі та спричинити ненавмисний витік даних, якщо захист не буде ретельно розроблений для застосування до всіх послідовностей взаємодії, а не тільки до першого запиту». ***(Dan Goodin. A single click mounted a covert, multistage attack against Copilot // Condé Nast (https://arstechnica.com/security/2026/01/a-single-click-mounted-a-covert-multistage-attack-against-copilot/). 15.01.2026).***

***

«Січневий Patch Tuesday від Microsoft виявився далеко не скромним: було виправлено 112 вразливостей — майже вдвічі більше, ніж у грудні — включаючи активно експлуатовану вразливість нульового дня та кілька

недоліків, які, на думку експертів, вимагають негайної уваги. Уразливість нульового дня CVE-2026-20805 (CVSS 5.5) — це помилка розкриття інформації в Desktop Window Manager (DWM), яку зловмисники вже використовують для витоку інформації про адреси пам'яті. Хоча Microsoft оцінює її лише як «помірну», дослідники попереджають, що такий витік пам'яті може бути пов'язаний з іншими помилками для обходу захисту, підвищення привілеїв і забезпечення багатоетапних компрометацій, навіть після отримання початкової опори…

Microsoft позначила вісім вразливостей як «більш ймовірні для експлуатації», включаючи дві помилки віддаленого виконання коду в Windows NTFS — CVE-2026-20840 та CVE-2026-20922 (обидві CVSS 7.8) — які дозволяють довільне виконання коду, якщо зловмисник вже має доступ до системи. Оскільки про ці вразливості повідомила третя сторона, дослідники побоюються, що технічні деталі можуть незабаром стати публічними, що швидко перетворить їх на широко використовувані вразливості n-day. Інші шість проблем з високим пріоритетом — це вразливості підвищення привілеїв в основних компонентах Windows (Інсталятор, Звіт про помилки, Драйвер загальної системи лог-файлів, Служба маршрутизації та віддаленого доступу, Драйвер допоміжних функцій для WinSock та інша в DWM), всі з оцінкою 7,8 і всі потенційно корисні для зловмисників, які прагнуть переміститися вбік і отримати вищий доступ. Експерти також виділили CVE-2026-20876, помилку EoP в Windows Virtualization Based Security (VBS) Enclave, як особливо небезпечну, оскільки вона може проникнути в найнадійніші рівні виконання, де захищені облікові дані та конфіденційні робочі навантаження, забезпечуючи глибоку стійкість і широкий «радіус ураження» в разі використання…

Дві уразливості Office, що дозволяють віддалено виконувати код, CVE-2026-20952 та CVE-2026-20953 (CVSS 8.4), оцінюються як критичні, хоча Microsoft наразі вважає ймовірність їх використання низькою. Обидві уразливості можуть бути активовані через надійний документ або навіть панель попереднього перегляду, що потенційно дозволяє зловмисникам виконувати код без взаємодії з користувачем або підвищених привілеїв, що спонукає дослідників попередити, що «навіть побіжний погляд є ризиком». Січневий випуск продовжує інтенсивний ритм випуску патчів від Microsoft, яка виправила 1275 унікальних CVE в 2025 році і неодноразово випускала великі оновлення з високим рівнем впливу, підкреслюючи необхідність для організацій пріоритезувати і швидко розгортати патчі для найбільш вразливих і ланцюгових помилок у пакеті цього місяця». ***(Jai Vijayan. Microsoft Starts 2026 With a Bang: A Freshly Exploited Zero-Day // TechTarget, Inc. (https://www.darkreading.com/application-security/microsofts-starts-2026-bang-zero-day). 13.01.2026).***

***

«Останній звіт CyberArk «Тенденції в області безпеки PKI: глобальне дослідження тенденцій, викликів та впливу на бізнес» показує, що застарілі системи інфраструктури відкритих ключів (PKI) є серйозною вразливістю для організацій у всьому світі. Дослідження, проведене Ponemon Institute на замовлення CyberArk, охопило майже 2000 фахівців з IT та безпеки і виявило, що

застарілі системи PKI не в змозі впоратися з вибуховим зростанням кількості цифрових сертифікатів, спричиненим ідентифікацією машин і робочих навантажень у сучасних хмарних середовищах та середовищах з нульовим рівнем довіри…

В середньому організації управляють понад 114 000 внутрішніх сертифікатів, маючи в своєму розпорядженні лише чотирьох спеціалізованих співробітників, що змушує 63% з них передавати управління PKI на аутсорсинг через брак ресурсів. Така залежність від ручних процесів і фрагментованих систем має серйозні наслідки: 60% організацій стикалися з порушеннями безпеки через слабку криптографію, 56% стикалися з незапланованими перебоями в роботі через закінчення терміну дії сертифікатів або помилки в конфігурації, а 58% страждали від компрометації сертифікатів сторонніх центрів сертифікації. Крім того, 43% повідомили про крадіжку приватних ключів сервера…

Довіра до поточних можливостей PKI є низькою: менше половини організацій вважають, що їхні системи є ефективними проти кібератак або повністю відповідають нормативним вимогам. У звіті підкреслюється, що організації з вищим рівнем довіри, як правило, мають уніфікований огляд своїх запасів сертифікатів та інтегрували штучний інтелект і автоматизацію у свої стратегії PKI, щоб зменшити операційні навантаження та підвищити рівень безпеки. У міру поширення ідентифікаторів машин та скорочення терміну дії сертифікатів модернізація PKI за допомогою автоматизації стає критично важливою для зменшення фінансових та операційних ризиків…» ***(Sarah Weston. New research shows that legacy PKI puts digital identities at risk, with 56% of organisations experiencing services disruption // A Intelligent Global Media Brand (https://www.intelligentciso.com/2026/01/22/new-research-shows-that-legacy-pki-puts-digital-identities-at-risk-with-56-of-organisations-experiencing-services-disruption/). 22.01.2026).***

***

«Критична уразливість обходу аутентифікації (CVE-2026-24061) в сервері GNU InetUtils telnetd активно експлуатується, і, за даними організації з безпеки Shadowserver, майже 800 000 екземплярів Telnet, підключених до Інтернету, знаходяться під загрозою по всьому світу. Ця вразливість, присутня у версіях GNU InetUtils від 1.9.3 до 2.7 і виправлена у версії 2.8, дозволяє зловмисникам обійти аутентифікацію та отримати root-доступ, надіславши спеціально створену змінну середовища USER…

Найбільш вразливими є застарілі або IoT-системи, особливо в Азії та Південній Америці, які часто працюють на застарілому програмному забезпеченні. Зловживання почалося вже через день після випуску патча: зловмисники використовували автоматизовані та ручні методи для отримання доступу до оболонки та спроб розгортання шкідливого програмного забезпечення Python. Хоча деякі атаки не вдалися через відсутність компонентів системи, ризик залишається високим…

Адміністраторам, які не можуть негайно виконати оновлення, рекомендується вимкнути службу telnetd або заблокувати TCP-порт 23, щоб

зменшити загрозу. Цей інцидент підкреслює небезпеку публічно доступних служб Telnet і важливість своєчасного встановлення виправлень, особливо для застарілих і вбудованих пристроїв». ***(Sergiu Gatlan. Nearly 800,000 Telnet servers exposed to remote attacks // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/nearly-800-000-telnet-servers-exposed-to-remote-attacks/). 26.01.2026).***

***

«Експерти з кібербезпеки компанії SEC Consult, що входить до складу Eviden, яка належить Atos, виявили понад 20 вразливостей у програмному забезпеченні централізованого управління Exos від Dormakaba та пов'язаних з ним апаратних системах доступу, які контролюють вхід за допомогою клавіатур, зчитувачів відбитків пальців або чіп-карт. До недоліків належали жорстко запрограмовані облікові дані, слабкі паролі, відсутність аутентифікації, незахищене генерування паролів, підвищення локальних привілеїв, витік даних, перехід по шляху та вразливості введення команд…

Ці системи широко використовуються великими європейськими підприємствами, включаючи промислові компанії, енергопостачальників, логістичні фірми та аеропорти. Використання цих вразливостей могло б дозволити зловмисникам відчиняти двері, отримувати доступ до PIN-кодів або здійснювати подальші атаки в уражених середовищах. Хоча компанія Dormakaba заявила, що для використання вразливостей необхідний попередній доступ до внутрішньої мережі клієнта, SEC Consult виявила кілька систем, підключених до Інтернету, які могли бути атаковані дистанційно…

Протягом останніх 18 місяців компанія Dormakaba працювала над випуском патчів та рекомендацій щодо посилення захисту, співпрацюючи з основними клієнтами з метою забезпечення безпеки їхніх систем. На сьогоднішній день компанія не повідомляє про жодні відомі випадки зловживання, але цей інцидент підкреслює надзвичайну важливість забезпечення безпеки систем контролю доступу, особливо тих, що підключені до Інтернету». ***(Eduard Kovacs. Access System Flaws Enabled Hackers to Unlock Doors at Major European Firms // SecurityWeek (https://www.securityweek.com/access-system-flaws-enabled-hackers-to-unlock-doors-at-major-european-firms/). 26.01.2026).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Французький постачальник IT-послуг Cyllene розробив RC-DC4/5G «Cyllene Box» — безпечний пристрій для підключення, призначений для посилення кібербезпеки сонячних та інших інфраструктур відновлюваної енергії, а також для допомоги операторам у дотриманні директиви ЄС NIS 2. На тлі зростаючої занепокоєності Європейської ради з сонячної енергетики та

SolarPower Europe щодо кіберризиків для фотоелектричних станцій, Cyllene зазначає, що сучасні сонячні та вітрові електростанції покладаються на високорозподілені мережі для збору операційних даних, що робить їх все більш вразливими до атак. Маючи 400 співробітників у 13 офісах та понад 1500 державних і приватних клієнтів, Cyllene використовує цей пристрій для заміни застарілих ADSL- та супутникових систем на більш надійну та гнучку архітектуру…

Пристрій RC-DC4/5G може керувати різними типами інтернет-з'єднань — оптоволоконним, мобільним 4G/5G та супутниковим, якщо це необхідно — і розташовується вище за мережевою інфраструктурою об'єкта. Він має кілька портів Ethernet та вбудований Wi-Fi, а також включає брандмауер, шифрування та засоби контролю авторизації для захисту всього підключеного обладнання IoT та SCADA. Пристрій інтегрований з платформою SD-WAN компанії Cyllene, розміщеною в трьох французьких дата-центрах, що задовольняє потреби клієнтів енергетичної галузі в розміщенні даних на території країни. Наразі Cyllene управляє 150 фотоелектричними парками у Франції, приблизно половина з яких вже обладнана цим пристроєм, а повне перенесення заплановано до кінця лютого. Супутній портал управління централізує дані з усіх парків, забезпечуючи динамічне відображення мережі та створюючи документацію, необхідну відповідно до NIS 2, таку як матриці потоків, схеми мережі та репліковані резервні копії, тим самим посилюючи кіберстійкість та відповідність нормативним вимогам у всіх активах відновлюваної енергетики…» ***(French IT services provider develops cybersecurity box for PV plants // pv magazine (https://www.pv-magazine.com/2026/01/20/french-it-services-provider-develops-cybersecurity-box-for-pv-plants/). 20.01.2024).***

***

«…У міру того як кіберзагрози стають все більш витонченими та різноманітними, традиційні рішення з безпеки часто виявляються недостатніми, що змушує організації шукати більш уніфікований, проактивний та інтелектуальний підхід. Розширене виявлення та реагування (XDR) задовольняє цю потребу, інтегруючи в єдину платформу кілька інструментів безпеки, таких як виявлення та реагування на кінцевих точках (EDR), аналіз мережевого трафіку (NTA), управління інформацією про безпеку та подіями (SIEM) та аналіз поведінки користувачів (UEBA). XDR забезпечує комплексні можливості виявлення, розслідування та автоматизованого реагування на кінцевих точках, у мережах, хмарних середовищах та серед користувачів, руйнуючи ізольованість традиційних систем безпеки…

Основні переваги XDR включають цілісну видимість безпеки, швидше виявлення загроз і реагування на них, зменшення кількості сповіщень, поліпшення розслідування інцидентів та спрощення управління безпекою. Завдяки кореляції даних з різних джерел і використанню аналітики на основі штучного інтелекту, XDR забезпечує виявлення складних атак у режимі реального часу, автоматизує реагування та оптимізує операції з безпеки за допомогою централізованої панелі управління…

Платформа XDR від Seceon, що працює на базі штучного інтелекту, є прикладом цих переваг, пропонуючи комплексне виявлення загроз, автоматизовану реакцію на інциденти, уніфікований моніторинг, інформацію про загрози в режимі реального часу, розширені можливості криміналістичного аналізу та масштабованість для організацій будь-якого розміру. Рішення Seceon агрегує дані з кінцевих точок, мереж та поведінки користувачів, що дозволяє швидко ідентифікувати та локалізувати загрози, а автоматизовані робочі процеси зменшують навантаження на команди з безпеки…

У сучасному цифровому середовищі, яке швидко розвивається, XDR є необхідним для сучасних організацій. Він дозволяє їм випереджати зловмисників, скорочувати час реагування та підтримувати високий рівень безпеки. У міру розвитку кіберзагроз впровадження XDR, такого як платформа Seceon, стало стратегічною необхідністю для захисту критично важливих активів та забезпечення стійкості бізнесу». ***(Pushpendra Mishra. Extended Detection and Response (XDR): A New Era in Cybersecurity // Techstrong Group Inc. (https://securityboulevard.com/2026/01/extended-detection-and-response-xdr-a-new-era-in-cybersecurity/). 23.01.2025).***

***

Основи кібергігієни

«Кіберінциденти стали звичайним ризиком для бізнесу, що вимагає від керівників організацій вийти за рамки простих контрольних списків і прийняти дисципліновану, превентивну стратегію безпеки в 2026 році. Оскільки більшість успішних атак відбуваються за передбачуваними сценаріями, для керівників, рад директорів та IT-фахівців, які прагнуть досягти реальних результатів, надзвичайно важливо зосередитися на десяти ключових рішеннях…

Стратегія повинна бути зосереджена на ідентифікації (Резолюція 1), що вимагає надійної багатофакторної автентифікації (MFA) для всіх користувачів, щоб запобігти захопленню облікових записів, яке є відправною точкою для більшості порушень. Заходи захисту повинні надавати пріоритет виправленню на основі експлуатації (Резолюція 2), а не суворим оцінкам серйозності, узгоджуючи виправлення з реальними даними про загрози. Крім того, організації повинні розглядати шахрайство з електронною поштою як проблему фінансового контролю (Резолюція 3), впроваджуючи суворі заходи контролю за перевіркою платежів, які не покладаються виключно на електронну пошту, для боротьби з компрометацією ділової електронної пошти.

Вирішення внутрішніх ризиків має першочергове значення: організації повинні активно контролювати поведінку користувачів і застосовувати принцип мінімальних привілеїв доступу, щоб боротися зі зростанням внутрішніх загроз (Резолюція 4). Операційна стійкість залежить від надійності та перевіреності резервних копій (Резолюція 5), використання незмінних або офлайн-копій із регулярними навчаннями з відновлення. Технічна гігієна вимагає стандартизації безпечних конфігурацій (Резолюція 6) на кінцевих точках і в хмарних середовищах

для запобігання неправильним налаштуванням, які є найпоширенішою причиною порушень, а також агресивного обмеження привілейованого доступу (Резолюція 8) для обмеження рухів зловмисників…

Нарешті, організації повинні підвищити рівень готовності: практикувати реагування на інциденти (Резолюція 7) шляхом регулярних навчань за участю керівників та юридичних команд, щоб забезпечити швидше прийняття рішень під час реальних подій. У відповідь на зростаючі загрози необхідно оновлювати навчання з питань безпеки, щоб підготуватися до соціальної інженерії на основі штучного інтелекту (Резолюція 9), яка використовує персоналізовані та правдоподібні обмани. Вся програма безпеки повинна інтегрувати відповідність вимогам безпеки (Резолюція 10), узгоджуючись з такими рамками, як NIST і CMMC, щоб створити захищену, піддається аудиту позицію.

Ключ до успіху в 2026 році — це виконання: лідери повинні зосередитися на якнайшвидшому виконанні цих рішень, а не лише на їх плануванні. Організації, які розглядають кібербезпеку як обов'язок керівництва і діють швидко, будуть працювати впевнено, тоді як ті, хто зволікає, ризикують заплатити високу ціну за інциденти та репутаційні збитки». ***(Emil Sayegh. Top 10 Cybersecurity New Year's Resolutions Leaders Must Keep In 2026 // Forbes Media LLC. (https://www.forbes.com/sites/emilsayegh/2026/01/03/top-10-cybersecurity-new-years-resolutions-leaders-must-keep-in-2026/). 03.01.2026).***

***

«Рада з кібербезпеки ОАЕ закликала громадськість розпочати новий рік із впровадження більш розумних звичок у сфері кібербезпеки.

В офіційному дописі в соціальних мережах рада наголосила на важливості дотримання простих рекомендацій для забезпечення безпеки в Інтернеті. До них належать захист домашніх Wi-Fi-мереж, оновлення пристроїв і програмного забезпечення, перевірка безпеки веб-сайтів і додатків перед використанням, регулярний перегляд дозволів додатків та видалення старих або невикористовуваних облікових записів.

Рада також наголосила на необхідності шифрування електронних листів, використання безпечних цифрових мереж під час підключення до громадських Wi-Fi та створення резервних копій важливих даних.

Вона додала, що дотримання цих заходів може допомогти людям краще захистити себе та свою інформацію на початку нового року». ***(Huda Ata. UAE Cybersecurity Council urges public to boost online safety // Nisr Publishing LLC (https://gulfnews.com/uae/people/uae-cybersecurity-council-urges-public-to-boost-online-safety-1.500397284). 03.01.2026).***

***

«TechQuest, розроблена в Нігерії мобільна гра-головоломка, присвячена кібербезпеці та цифровій обізнаності, набуває всесвітньої популярності у зв'язку із зростанням занепокоєння щодо цифрової безпеки. З понад 10 000 завантажень у Google Play Store та рейтингом користувачів вище 4,5 зірок, TechQuest стає популярним у всьому світі як доступний мобільний інструмент для

вивчення основних понять кібербезпеки та технологій. Інтерактивний формат гри, заснований на головоломках, дозволяє уникнути надмірної кількості тексту, що робить її особливо привабливою для початківців, студентів, професіоналів та випадкових учнів, які віддають перевагу коротким сесіям, що проводяться у власному темпі…

Користувачі хвалять TechQuest за простоту, зручність у використанні та відсутність реклами в додатку або платних оновлень, що відрізняє його від багатьох інших безкоштовних освітніх додатків. У міру зростання кіберризиків, таких як фішинг та крадіжка особистих даних, у всьому світі, цифрова грамотність та обізнаність у питаннях кібербезпеки стають необхідними навичками. Мобільні освітні інструменти, такі як TechQuest, заповнюють цю прогалину, особливо в регіонах з обмеженим доступом до офіційного навчання, оскільки смартфони стають основним обчислювальним пристроєм для мільйонів людей…

Розроблена нігерійським фахівцем з кібербезпеки Бісолою Фейт Кайоде, яка проживає у Великобританії, гра TechQuest є прикладом того, як розробники з діаспори сприяють глобальним технологічним інноваціям, забезпечуючи при цьому доступність для користувачів в Африці та за її межами. Успіх гри підкреслює більш широку тенденцію до мобільного навчання на основі ігор як практичного та цікавого способу формування базових цифрових навичок у світі, що стає дедалі більш пов'язаним». ***(Royal Ibeh. Nigerian-built cybersecurity game gains global traction // Businessday Media Limited (https://businessday.ng/technology/article/nigerian-built-cybersecurity-game-gains-global-traction/). 24.01.2026).***

***