**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

№ 9 (вересень)

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. № 9 (вересень). 166 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.

© Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», 2026
© Національна бібліотека України імені В.І. Вернадського, 2026

ЗМІСТ

Світові тенденції в галузі кібербезпеки 4
Сполучені Штати Америки та інші країни Америки 23
Країни ЄС та Великобританія 38
Австралія та Нова Зеландія 56
Китай, Індія, Японія, Південна Корея та країни Індо-Тихоокеанського регіону 57
Ізраїль, Туреччина та країни Близького сходу 63
Країни Африки 65
Кібервійни та протидія зовнішній кібернетичній агресії 67
Створення та функціонування кібервійськ 72
Кіберзахист критичної інфраструктури 73
Кіберзахист закладів охорони здоров'я 84
Захист персональних даних та соціальні мережі 87
Масштабні витоки персональних даних 88
Кібербезпека та хмарні технології 90
Кібербезпека Інтернету речей. Штучний інтелект 91
Штучний інтелект, як інструмент боротьби із кіберзлочинністю 117
Штучний інтелект, як зброя кіберзлочинців 119
Кіберзлочинність та кібертероризм 122
Вірусне та інше шкідливе програмне забезпечення 141
Фішингові атаки 150
Операції правоохоронних органів та судові справи проти кіберзлочинців 155
Технічні аспекти кібербезпеки 158
Виявлені вразливості технічних засобів та програмного забезпечення 159
Технічні та програмні рішення для протидії кібернетичним загрозам 163
Питання криптографії 166

«Згідно з результатами дослідження «Bitdefender Cybersecurity Assessment 2026», понад половина фахівців у галузі IT та кібербезпеки, які стикалися з порушенням безпеки протягом останніх дванадцяти місяців, повідомляють, що їм було наказано зберігати інцидент у таємниці, навіть якщо за законом про нього слід було повідомити. Ця тенденція відстежується компанією вже кілька років, незважаючи на те, що вимоги щодо розкриття інформації значно розширилися з моменту першого постановлення цього питання у 2023 році. Приблизно половина з 1 200 опитаних фахівців у сфері IT та безпеки зазнала порушення безпеки або інциденту безпеки протягом попереднього року, і з цієї групи 55,2% заявили, що їх просили зберігати мовчання; цей показник зріс з 42% у 2023 році до пікового значення 57,6% у 2025 році, після чого стабілізувався на поточному рівні 55,2%... Найбільш гостро проблема тиску відчувається у Сполучених Штатах, проте більшість фахівців у Німеччині, Великій Британії та Сінгапурі також повідомляють, що їм наказують приховувати порушення, про які слід повідомляти, тоді як у Франції та Італії цей показник становить трохи менше 50 відсотків. Експерти виділяють три основні причини, через які організації обирають мовчання: зловмисники перетворили саму конфіденційність на бізнес-модель, розробляючи більш непомітні та цілеспрямовані операції, в рамках яких вони контактують лише з кількома особами всередині компанії-жертви, пропонуючи повне відновлення даних в обмін на виплату та обіцянку, що інцидент залишиться в таємниці; багато організацій вважають, що витрати, пов'язані з розкриттям інформації — штрафи, шкода репутації, відтік клієнтів — є вищими, ніж ризики, пов'язані з мовчанням, хоча зловмисники дедалі частіше погрожують оприлюднити дані або самостійно повідомити регуляторні органи, якщо викуп не буде сплачено, тим самим посилюючи шкоду від приховування; а внутрішня культура, яка цінує бездоганну роботу кінцевих користувачів більше, ніж оперативне повідомлення, може затримати повідомлення на кілька годин, даючи зловмисникам час на встановлення стійкого доступу, викрадення облікових даних та горизонтальне переміщення, що збільшує час перебування зловмисників у системі та підвищує ймовірність прийняття подальших рішень щодо приховування порушення. Тому керівникам служб безпеки рекомендується визначати свою позицію щодо розкриття інформації заздалегідь, а не під час кризи, формувати внутрішню культуру повідомлення про інциденти, вільну від звинувачень, яка винагороджує швидкість, та розглядати профілактику як стратегію, що дозволяє їм взагалі уникнути цієї дилеми, адже найдешевшим порушенням залишається те, яке ніколи не відбувається». ***(Bruce Sussman. Why Are So Many Security Professionals Keeping Breaches Quiet? // Bitdefender (https://www.bitdefender.com/en-gb/blog/businessinsights/why-are-so-many-security-professionals-keeping-breaches-quiet). 03.09.2026).***

***

«Міжнародна технологічна компанія GMV була обрана Агентством зв'язку та інформації NATO (NCIA) в якості підрядника в рамках програми

«Динамічний ринок кібербезпеки» (CSDM) — довгострокової системи укладення контрактів, покликаної забезпечити NATO оперативний доступ до спеціалізованих технологій та послуг у сфері кібербезпеки. Цей вибір дає GMV можливість брати участь у конкурсах на виконання майбутніх замовлень у багатьох критично важливих сферах, зокрема в галузі управління ідентифікацією та доступом, архітектур «Zero Trust», безпеки мереж та периметра, безпеки хмарних середовищ, виявлення та аналізу загроз, управління вразливостями та цифрової криміналістики… Використовуючи свій багатий досвід у сфері забезпечення безпечного зв'язку, захисту критичної інфраструктури та створення систем оборони, що мають вирішальне значення для виконання місій, для європейських та міжнародних урядових організацій, таких як EUSPA та ESA, компанія GMV активно підтримуватиме цілі NATO щодо цифрової трансформації та кіберстійкості. Хосе Прієто, директор GMV з питань глобальної стратегії та розвитку бізнесу в галузі оборони та безпеки, назвав цей вибір важливою віхою, що підкреслює прагнення компанії зміцнювати цифрову інфраструктуру Альянсу за допомогою передових технологій та спеціалізованих знань. Зрештою, цей контракт зміцнює позиції GMV як провідного європейського постачальника технологій у секторі оборони та безпеки, спираючись на її значний досвід участі у спільних європейських оборонних ініціативах та ініціативах, пов'язаних з NATO». ***(GMV selected by NATO to join Cyber Security Dynamic Marketplace framework // WebWire® (https://www.webwire.com/ViewPressRel.asp?aId=359873). 02.09.2026).***

***

«Кібербезпека вже не є проблемою виключно для великих корпорацій, що мають власні IT-команди та значні бюджети. Сьогодні фрілансери, віддалені працівники та малі й середні підприємства (МСП) стикаються з таким самим рівнем ризику, як і великі компанії, головним чином через автоматизовані інструменти кібератак, які одночасно сканують тисячі мереж і пристроїв у пошуках вразливих місць. За такої безрозбірливої моделі навіть поодиноких вразливостей — таких як слабкі паролі, системи без оновлень або незахищені публічні мережі Wi-Fi — достатньо, щоб зламати систему…

Малі та середні підприємства стали головними мішенями в цьому мінливому середовищі загроз, оскільки вони часто володіють цінними даними про клієнтів та комерційною інформацією, водночас виділяючи на мережеву безпеку значно менше коштів, ніж великі підприємства. Хоча економія на безпеці може здаватися способом зменшити накладні витрати для компаній на початковому етапі розвитку та стартапів, невиправлені вразливості часто призводять до серйозних і дорогих збоїв у роботі в майбутньому…

Водночас технологічні досягнення — зокрема штучний інтелект — змінюють як наступальні, так і оборонні можливості у сфері кібербезпеки. У той час як зловмисники використовують ШІ для автоматизації та масштабування атак з безпрецедентною швидкістю, команди з безпеки застосовують інструменти машинного навчання для виявлення аномальних моделей трафіку та нейтралізації потенційних порушень ще до того, як буде завдано значної шкоди. Оскільки проактивний захист став доступним завдяки базовим звичкам безпеки та таким

інструментам, як віртуальні приватні мережі (VPN) та виділені IP-з'єднання, забезпечення базового рівня кібербезпеки з самого початку стає дедалі важливішим як для підприємств, так і для приватних осіб». ***(PIA: Cybersecurity is an issue everyone needs to be aware of // KM Media Group Limited (https://www.kentonline.co.uk/kent/news/the-importance-of-understanding-cybersecurity-threat-344799/). 07.09.2026).***

***

«Хоча кібербезпеку часто сприймають як надто технічну проблему, що вимагає значних бюджетів та спеціалізованих команд, організації будь-якого розміру можуть суттєво підвищити свою стійкість, впровадивши доступні базові заходи безпеки. Основний базовий захист починається з надійного контролю ідентифікації та доступу. Оскільки «наповнення облікових даних» (credential stuffing) та повторне використання паролів у різних системах становлять серйозні ризики, підприємства повинні зобов'язати співробітників використовувати довгі, унікальні облікові дані — за допомогою корпоративних менеджерів паролів — та запровадити багатофакторну автентифікацію (MFA) для всіх доступних облікових записів. MFA додає важливий рівень перевірки, гарантуючи, що лише скомпрометованих паролів недостатньо для того, щоб неавторизовані особи змогли проникнути в корпоративні системи…

Орієнтовані на людей заходи захисту та організаційна культура є однаково важливими складовими стійкої системи безпеки. Оскільки зловмисники часто використовують фішингові схеми, імітуючи законних колег, постачальників або установи, регулярні тренінги з підвищення обізнаності співробітників є надзвичайно важливими, щоб допомогти персоналу виявляти такі ознаки, як штучна терміновість, аномальні посилання та неперевірені домени відправників. У разі виникнення підозр співробітники повинні самостійно перевіряти запити через встановлені, окремі канали зв'язку. Не менш важливо, щоб керівництво сприяло формуванню відкритої культури безпеки, вільної від звинувачень, в якій співробітників заохочують негайно повідомляти про потенційні вразливості або випадкові кліки, забезпечуючи тим самим можливість командам з безпеки локалізувати потенційні інциденти до того, як буде завдано значної шкоди…

Щоб створити структуровану базову модель безпеки, підприємства можуть використовувати визнані системи забезпечення безпеки, такі як програма «Cyber Essentials», що підтримується урядом Великої Британії, або вдосконалені моделі «Cyber Assurance». Ці сертифікати не тільки забезпечують практичні технічні заходи захисту від поширених векторів атак, але й надають клієнтам, постачальникам та партнерам у ланцюгу поставок підтверджені докази зрілості системи безпеки. Однак дотримання вимог не повинно перетворюватися на статичну рутину, що зводиться до простого відмічання пунктів у списку. У міру того, як змінюються корпоративні технології, персонал та операційні процеси, підприємства повинні постійно переглядати свої політики, технічні засоби контролю та навчання співробітників, підходячи до кібербезпеки як до постійної операційної відповідальності, що об'єднує людей, процеси та технології». ***(Cyber security doesn't have to be complicated: 4 basics every business should get right //***

Aberdeen & Grampian Chamber of Commerce (https://www.agcc.co.uk/news-article/cyber-security-doesnt-have-to-be-complicated-4-basics-every-business-should-get-right). 07.09.2026).

***

«Щорічний сезон святкових покупок стає серйозним випробуванням для операційної стійкості роздрібної торгівлі, оскільки в цей час збігаються такі фактори, як різке зростання обсягів транзакцій, обмежена пропускна здатність дистрибуційних мереж та підвищені очікування споживачів щодо виконання замовлень. Оскільки сучасна роздрібна торгівля спирається на тісно взаємопов'язані екосистеми, що включають програмні додатки, сторонніх платіжних провайдерів, логістичних партнерів, фізичні склади та розподілені команди, пікові періоди покупок стають привабливими цілями для кіберзагроз. Згідно з оцінками Deloitte, загальний обсяг роздрібних продажів у США під час свят становитиме від 1,61 до 1,62 трлн доларів, а електронна комерція зросте на 7–9 відсотків, тому кожна година простою в роботі несе значний фінансовий ризик. Отже, кіберінцидент не можна розглядати лише як ізольовану IT-проблему чи відмову окремого додатка; навіть одне порушення може швидко поширитися на наступні ланки ланцюга, зупинивши обробку замовлень, порушивши роботу складів та розірвавши ланки ланцюга постачання саме в той момент, коли попит досягає піку…

Щоб ефективно управляти цими вразливими місцями, роздрібні підприємства повинні перейти від статичної документації щодо забезпечення безперебійної роботи до динамічних, обчислюваних моделей послуг та взаємозалежностей. Традиційні посібники з відновлення після аварій описують, як відновлюються окремі технічні системи, але вони не надають керівництву міжфункціональної наочності, необхідної для прийняття швидких рішень з високими ставками під час реального інциденту. Модель взаємозалежностей, що постійно оновлюється, відображає складні операційні взаємозв'язки між цифровою інфраструктурою, сторонніми SaaS-інструментами, фізичними об'єктами та залежностями персоналу, що дозволяє керівництву обчислювати операційні наслідки та фінансові ризики в режимі реального часу, замість того, щоб вручну діагностувати взаємозалежності систем у кризовій ситуації…

Формування дієздатного потенціалу стійкості передбачає дисциплінований триетапний підхід: виявлення критичних ризиків зриву роботи в послугах, орієнтованих на клієнтів, та у взаємодії з сезонними постачальниками; моделювання каскадних наслідків другого та третього порядку у залежних бізнес-процесах; а також встановлення чіткої послідовності пріоритетів відновлення ще до виникнення інциденту. Оскільки під час масштабного збою організації не можуть відновити роботу всіх систем одночасно, керівництво має заздалегідь визначити, які основні послуги найкраще захищають життєздатність підприємства, довіру клієнтів та фінансові показники. Зрештою, кібербезпека та операційна стійкість повинні базуватися на єдиній, спільній картині, що охоплює IT, безпеку, логістику та виконавче керівництво, перетворюючи реагування на надзвичайні ситуації з пасивного дотримання вимог на рішучу операційну здатність, яка захищає доходи

під час найкритичнішого торгового періоду в галузі». ***(Richard Barnett. Holiday Cyberattacks: Why Peak Shopping Season Is Really a Business Resilience Test // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/holiday-cyberattacks-why-peak-shopping-season-is-really-a-business-resilience-test/). 06.09.2026).***

***

«У 2026 році ситуація в галузі кібербезпеки змінилася: акцент змістився з традиційних атак на периметри мереж на екосистеми розробників, цифрові ідентичності та ланцюги постачання сторонніх постачальників, а штучний інтелект та автоматизація різко прискорили темпи атак. Зареєстрований інцидент із Hugging Face ілюструє ризики, з якими стикаються середовища розробки з відкритим кодом та штучним інтелектом, де автоматизовані агенти можуть виявляти вразливості, експлуатувати код, викрадати облікові дані та, можливо, проникати в підключені хмарні системи та системи CI/CD ще до того, як захисники встигнуть відреагувати… Водночас кампанії соціальної інженерії, такі як згадана атака на компанії Abbott Laboratories та Exact Sciences, демонструють, як зловмисники можуть видавати себе за IT-персонал і отримувати доступ до надійних облікових даних або сеансів, що пройшли автентифікацію, обходячи традиційні засоби захисту на основі багатофакторної автентифікації (MFA) та єдиного входу (SSO). Організації у сферах охорони здоров'я, фармацевтики та технологій також дедалі частіше наражаються на ризики через сторонніх постачальників, причому злочинці віддають перевагу непомітному викраденню даних та шантажу над традиційним шифруванням за допомогою програм-вимагачів, особливо коли вони можуть викрасти цінну медичну інформацію, інтелектуальну власність або активи штучного інтелекту. Ці тенденції роблять статичну периметральну безпеку, щорічні оцінки постачальників, базову багатофакторну автентифікацію та плани протидії програм-вимагачів, зосереджені на резервному копіюванні, дедалі менш ефективними… Натомість організаціям слід впровадити систему безперервного моніторингу безпеки та діяльності сторонніх суб'єктів, аутентифікацію, стійку до фішингу, таку як FIDO2 (Fast IDentity Online 2) та парольні ключі, постійну перевірку ідентичності та сеансів, посилений захист середовищ розробки програмного забезпечення та MLOps (операції машинного навчання), принцип «мінімальних привілеїв» та мікросегментацію для підключень партнерів, а також плани реагування на інциденти, розроблені з урахуванням випадків викрадення даних, вимагання викупу та порушення операційної діяльності. Загалом, 2026 рік демонструє необхідність стратегій кібербезпеки, побудованих на постійній верифікації, стійкості ланцюга поставок та швидкому реагуванні на дедалі більш автоматизовані загрози». ***(M. Abimbola Mosobalaje. Prominent Cyber Attacks of 2026 and What They Teach Us About Emerging Attack Trends // HackerNoon (https://hackernoon.com/prominent-cyber-attacks-of-2026-and-what-they-teach-us-about-emerging-attack-trends). 08.09.2026).***

***

«Незважаючи на стрімкий розвиток та ажіотаж навколо штучного інтелекту, урядові та галузеві лідери на Саміті з кібербезпеки в Біллінгтоні наголосили, що фундаментальні практики кібербезпеки залишаються найважливішим засобом захисту від сучасних загроз. Представники ФБР, АНБ та розвідувального альянсу «П'ять очей» підкреслили, що основні заходи, такі як управління ідентифікацією, багатофакторна автентифікація, моніторинг периметра мережі та суворе дотримання правил кібергігієни, є сьогодні так само важливими, як і до буму штучного інтелекту. Лідери зазначили, що ШІ не може обійти чи замінити ці основоположні заходи контролю; навпаки, він лише висвітлює вразливості організацій, які їх ігнорують. Щоб ефективно захистити свої середовища, експерти радять підприємствам забезпечувати всебічний огляд своїх мереж шляхом картографування взаємопов'язаних пристроїв, розуміння ризиків ланцюга постачання та моніторингу ненадійних технологій. Таке глибоке розуміння мережевого середовища дозволяє організаціям точно оцінювати свою вразливість до ризиків та передбачати потенційні дії й наміри зловмисника після його проникнення всередину…

Хоча лідери застерігали від «поспішного кинутися» до впровадження нових ефектних інструментів ШІ за рахунок фундаментальної безпеки, вони визнали трансформаційний потенціал ШІ як чинника, що посилює ефективність захисників. У ході оборонних операцій ШІ допомагає командам з безпеки швидко фільтрувати величезні обсяги даних та «шуму» для виявлення реальних загроз, забезпечуючи експоненціальне підвищення швидкості аналізу. З іншого боку, досвідчені зловмисники, зокрема групи, що діють в інтересах держав, використовують ШІ для вдосконалення та посилення традиційних векторів атак. Наприклад, хакери, що діють за підтримки держави, зараз використовують створені за допомогою ШІ відео з глибокою підробкою (deepfake), щоб успішно проходити співбесіди при прийомі на роботу та проникати в цільові організації, що свідчить про те, що ШІ суттєво вдосконалює соціальну інженерію та інші тактики на всіх етапах життєвого циклу атаки. Зрештою, хоча ШІ змінює швидкість і масштаб кібероперацій, основні стратегії, необхідні для запобігання порушенням безпеки та захисту мереж, залишаються незмінними». ***(Eric Geller. Don't let AI distract from cybersecurity basics, officials and executives warn // TechTarget, Inc. (https://www.cybersecuritydive.com/news/ai-cybersecurity-basics-billington/829777/). 08.09.2026).***

***

«Імовірність кібератаки зараз здається майже неминучою, адже такі інциденти обходяться надзвичайно дорого: вони на тижні позбавляють компанії доступу до їхніх систем і спричиняють ланцюгову реакцію, здатну поставити навіть добре керовані організації на межу банкрутства. Тому різниця між тими, хто зможе відновитися, і тими, хто не зможе, залежить від рівня підготовки, яку необхідно розпочинати вже на рівні ради директорів… Протягом перших 72 годин після виявлення атаки одночасно починають відраховувати час кілька термінів, зокрема передбачений британським GDPR обов'язок повідомити Управління комісара з питань інформації (ICO) протягом 72 годин з моменту

«виявлення» — юридично спірного поняття, яке залежить від того, чи сповіщення було вперше зафіксовано, чи надійшло до відповідального за захист даних, чи до ради директорів, — що робить ретельне документування подій у реальному часі надзвичайно важливим; юридична професійна таємниця має бути забезпечена з самого початку при замовленні криміналістичних розслідувань, щоб звіти залишалися недоступними для розкриття, а не стали доказами проти компанії; слід уникати неформальних повідомлень у Teams або WhatsApp, таких як визнання давно відомих вразливостей або невиконаної багатофакторної аутентифікації, оскільки вони можуть згодом виявитися шкідливими; а зростаюче використання створених штучним інтелектом «діпфейків» для видавання себе за керівників, авторизації платежів або введення в оману щодо реагування ще більше ускладнює перевірку того, які повідомлення були справжніми… Страховиків слід негайно повідомляти через спеціальну гарячу лінію, особливо у випадках вимагання викупу або збою в роботі систем, щоб можна було доручити проведення IT-експертизи через затверджені канали постачальників; співпраця з брокерами має вирішальне значення, оскільки деякі поліси передбачають нульову франшизу протягом перших 72 годин; своєчасне подання обсягів робіт та бюджетів постачальників забезпечує отримання схвалень, що запобігає подальшим запереченням щодо понесених витрат; також слід переглянути всі поліси — а не лише окремі поліси кіберстрахування — оскільки положення про «інші види страхування» у комбінованих полісах або полісах професійної відповідальності можуть взаємодіяти або скасовувати один одного. Витрати, що стають очевидними одразу, такі як витрати на IT-експертизу, юридичні послуги, PR та відновлення систем, розглядаються як витрати на реагування на інцидент та відновлення, які зазвичай покриваються через мережу затверджених постачальників або за згодою страховика; за ними йдуть потенційно значні витрати на відновлення даних, які страховики можуть оскаржити, якщо резервні копії не були створені, що суперечить запевненням, наданим під час укладення договору, проте найбільший фінансовий вплив зазвичай проявляється у вигляді перерви в діяльності — втрати доходу під час простою, тривалого порушення роботи під час відновлення та додаткових витрат, понесених для мінімізації збитків — з урахуванням періодів очікування від 8 до 12 годин (іноді 24) та максимальних періодів виплати відшкодування до 180 днів (іноді подовжуються до 365), ці періоди часто виявляються недостатніми, оскільки економічне відновлення відстає від технічного, про що свідчить приклад виробника, який зазнав лише кількох тижнів простою, але зазнав тривалих збитків через неефективність виробництва, скасовані замовлення та втрачені контракти, що робить ранню та відкриту комунікацію з брокерами та страховиками надзвичайно важливою для пояснення проблем із грошовими потоками та сприяння здійсненню проміжних виплат… Суперечки щодо страхового покриття найчастіше виникають через виключення, пов’язані з поліпшенням об’єкта, які відмовляють у фінансуванні модернізації, а не простого усунення недоліків, прогалин у багатофакторній аутентифікації, на які страховики можуть посилатися відповідно до Закону про страхування для зміни умов, якщо у формі заявки було неточно відображено стан безпеки; виплат викупу, що вимагають обґрунтування на основі принципу «розсудливого незастрахованого»

разом із подвійною перевіркою санкцій з боку переговірника та страховика; виключень щодо війни та тероризму, які стають дедалі актуальнішими для суб'єктів, пов'язаних з державою; а також положень про ретроактивну дату, де повне ретроактивне покриття залишається ринковим стандартом… Організації, які досягають найкращих результатів, розглядають документацію як дисципліну, що застосовується до виникнення інциденту, а не як щось, про що згадують лише після нього, фіксуючи оперативні дані, такі як записи щодо обслуговування клієнтів, скасування замовлень, затримки у виконанні та втрачені контракти, щоб згодом можна було обґрунтувати страхові вимоги, обґрунтовуючи збитки від переривання діяльності спочатку за допомогою оперативних доказів впливу, а потім — за допомогою фінансової оцінки, регулярно звіряючи фактичний стан інфраструктури з даними, наведеними у страхових пропозиціях, та інформуючи страховиків про суттєві зміни, такі як нові постачальники або архітектура резервного копіювання, проводячи реалістичні настільні навчання за участю ІТ-відділу, юридичного відділу та ради директорів за багатоденними сценаріями з неповною інформацією, а також зберігаючи номери критично важливих гарячих ліній страхових компаній у доступному офлайн-режимі; зрештою, кібератака є настільки ж проблемою обізнаності керівництва, як і юридичною проблемою, що вимагає від генерального директора, фінансового директора та головного юрисконсульта детально опрацювати план реагування на інциденти та пов'язані з ним страхові умови рядок за рядком разом з ІТ-командою та страховою командою, щоб відповідальність та контактні дані були чіткими, розглядаючи подію з самого першого моменту як потенційну сферу спору шляхом збереження адвокатської таємниці, оперативного повідомлення, ретельного документування та чесної підготовки». ***(Eleanor Ruiz, Mark Jennings, Elsa Ramirez. When systems go dark: What to do when your company experiences a cyberattack // Reed Smith LLP (https://www.reedsmith.com/articles/when-systems-go-dark-what-to-do-when-your-company-experiences-a-cyberattack/). 08.09.2026).***

***

«На тлі глобального сплеску складних кіберзагроз та гострого дефіциту фахівців з кібербезпеки організаціям стає дедалі складніше та економічно невигідно створювати й підтримувати власні центри оперативної безпеки (SOC), що працюють у режимі 24/7. Щоб вирішити подвійну проблему — підвищення кіберстійкості та контролю операційних витрат — багато підприємств звертаються до постачальників керованих послуг безпеки (MSSP). Компанія Virtual Infosec Africa (VIA) задовольняє цю нагальну потребу в Гані, пропонуючи керовану послугу безпеки на базі штучного інтелекту, побудовану на єдиній, відкритій та уніфікованій платформі розширеного виявлення та реагування (Open XDR). Замість того, щоб змушувати організації відмовлятися від існуючих інвестицій у безпеку, платформа VIA безперешкодно інтегрується з сотнями сторонніх технологій, об'єднуючи розрізнені можливості в єдиний цілісний операційний досвід…

В основі цього рішення лежить штучний інтелект, який встановлює взаємозв'язки між подіями безпеки по всій поверхні атаки, відтворює потенційні шляхи атак та автоматизує розслідування, що дозволяє суттєво зменшити кількість

помилкових спрацьовувань та знизити навантаження на аналітиків. Як ліцензований постачальник послуг з кібербезпеки рівня Tier-1, VIA поєднує цю технологію світового класу з глибокою місцевою експертизою та інфраструктурою, розміщеною на місцевому рівні, забезпечуючи суворе дотримання вимог Гани щодо суверенітету даних та нормативних вимог. Зрештою, пропонуючи інтелектуальну автономну платформу SOC, VIA дає змогу організаціям у Гані та на всьому африканському континенті зменшити операційну складність, оптимізувати витрати на безпеку та забезпечити надійну кіберстійкість завдяки простішому та більш проактивному підходу до захисту від сучасних загроз». ***(Benson Arthur. Redefining Security Operations for a New Era of Cyber Defence // Business & Financial Times (https://thebftonline.com/article/redefining-security-operations-for-a-new-era-of-cyber-defence). 08.09.2026).***

***

«…Вибір постачальника послуг з тестування на розподілені атаки типу «відмова в обслуговуванні» (DDoS) вимагає від організацій спочатку визначити необхідний рівень надійності, внутрішні операційні можливості та бажані докази стійкості. Замість того, щоб покладатися на просте порівняння функцій, покупці повинні оцінювати різні операційні моделі, адаптовані до різних потреб організацій. У 2026 році провідні спеціалізовані постачальники представляють чотири основні підходи: Red Button надає повністю керовані тестування під керівництвом експертів із пріоритетними планами усунення недоліків; MazeBolt пропонує безперервну, безперебійну автоматизовану перевірку через свою платформу RADAR для виявлення відхилень у конфігурації; RedWolf Security забезпечує тестування з керівництвом або у режимі самообслуговування з використанням бібліотек сценаріїв, що можуть використовуватися повторно; а NimbusDDoS робить акцент на моделюванні, імітаційних іграх та тренуваннях з реагування на інциденти для підвищення готовності організації. Крім того, більш широкі консалтингові компанії з кіберстійкості, такі як NCC Group, надають спеціалізовані послуги з тестування на DDoS-атаки в рамках більш широкого портфеля послуг з безпеки…

Авторизація хмарного провайдера виступає в ролі критичного фільтра під час оцінки цілей, розміщених на інфраструктурі публічної хмари. Наразі AWS вказує Red Button, RedWolf, NCC Group та Safedash Analytics як авторизованих партнерів, тоді як Azure схвалює Red Button, RedWolf та MazeBolt; використання неавторизованих постачальників на AWS вимагає проходження процедури затвердження винятку, яка триває щонайменше 14 днів. Узгодження операційної моделі з внутрішніми цілями є надзвичайно важливим, оскільки сервіс із серйозними наслідками, що вимагає глибокої періодичної оцінки, підходить для моделі керованої оцінки, тоді як організація, зосереджена на виявленні операційних змін між оцінками, отримає більше переваг від безперервної валідації або можливості самостійного повторення оцінок…

Оскільки ціни, як правило, не оприлюднюються, а кількість векторів атак базується на нестандартизованих показниках постачальників, які вони надають самостійно, команди із закупівель повинні ретельно перевіряти заяви

постачальників під час процесу оцінки. Замість того, щоб надавати пріоритет загальним сумарним показникам за сценаріями, організації повинні переконатися, що охоплені відповідні протоколи, перевірити засоби контролю безпеки у виробничому середовищі та механізми аварійного зупинення, проаналізувати відредаговані зразки звітів і переконатися, що постачальник надає практичні, пріоритезовані рекомендації щодо усунення недоліків разом із чіткими умовами повторного тестування. Зрештою, успішний вибір постачальника вимагає звуження списку кандидатів шляхом попереднього визначення вимог до рівня довіри та затвердження хмарних рішень, а потім — узгодження пропускної здатності внутрішньої команди з відповідною операційною моделлю». ***(DDoS Testing Vendor Comparison: Red Button, MazeBolt, RedWolf and NimbusDDoS // Techstrong Group Inc. (https://securityboulevard.com/2026/09/ddos-testing-vendor-comparison-red-button-mazebolt-redwolf-and-nimbusddos/). 07.09.2026).***

***

«Згідно з опитуванням «Summer 2026 Macro Views Survey», проведеним компанією Enterprise Technology Research (ETR), витрати на кібербезпеку демонструють вражаючу стійкість, зростаючи з прогнозованим темпом 7,8% — найшвидше серед усіх відстежуваних категорій програмного забезпечення — навіть попри те, що організації перенаправляють кошти на ініціативи у сфері штучного інтелекту. Хоча загальне зростання витрат на програмне забезпечення сповільнилося до річного мінімуму в 3,6%, а майже половина респондентів повідомляє, що витрати на ШІ перевищують бюджети, компанії в першу чергу покривають ці перевитрати за рахунок скорочення витрат на зовнішніх підрядників, модернізацію застарілої інфраструктури та ліцензії на програмне забезпечення, не пов’язане зі ШІ… Примітно, що бюджети та штатні чисельності у сфері кібербезпеки значною мірою захищені від таких перерозподілів, зумовлених впровадженням штучного інтелекту: лише 18% організацій, які перерозподіляли бюджети на програмне забезпечення, скоротили видатки на кібербезпеку — це найнижчий показник серед усіх категорій, що брали участь в опитуванні, — і лише 23% тих, хто здійснював скорочення штату на основі штучного інтелекту, торкнулися посад у сфері кібербезпеки, на відміну від значно більших скорочень у сферах IT-підтримки, розробки додатків та операційної діяльності… ETR робить висновок, що, на відміну від інших IT-функцій, служба безпеки не мусить обґрунтовувати своє існування на тлі альтернатив, пов’язаних зі штучним інтелектом, — ця точка зору узгоджується з «Рамками кібербезпеки 2.0» NIST. Пов’язуючи управління ризиками кібербезпеки безпосередньо з загальною стратегією управління ризиками підприємства, ці рамки допомагають пояснити, чому організації визначають пріоритети та зберігають достатні ресурси для забезпечення безпеки, гарантуючи, що критично важливі засоби захисту залишаються повністю профінансованими навіть у умовах більш жорсткого контролю витрат та зростаючих фінансових вимог, пов’язаних із впровадженням штучного інтелекту». ***(Jaime Hampton. Cybersecurity Budgets Hold Up as AI Costs Force IT Spending Cuts // Techstrong Group Inc.***

(https://securityboulevard.com/2026/09/cybersecurity-budgets-hold-up-as-ai-costs-force-it-spending-cuts/). 11.09.2026).

***

«Традиційна освіта в галузі кібербезпеки часто робить акцент на теоретичних знаннях — вивченні типів атак, перегляді демонстрацій та складанні сертифікаційних іспитів — без розвитку практичних навичок, необхідних для ефективного реагування на реальні інциденти. Це створює розрив між концептуальним розумінням загроз та їхнім розпізнаванням, розслідуванням і локалізацією в умовах стресу. Практичні тренінги на основі сценаріїв допомагають подолати цей розрив, розвиваючи вміння розпізнавати шаблони завдяки багаторазовому зіткненню з реалістичними атаками, підвищуючи швидкість реагування та розвиваючи здатність адаптуватися, коли зловмисники використовують незнайомі методи… Ці навички формуються подібно до практичного досвіду в інших сферах: вони з'являються завдяки постійному прийняттю рішень та вирішенню проблем, а не лише завдяки передачі знань. Все ширше використання платформ для кібертренувань, таких як TryHackMe, що надають браузерні середовища для відпрацювання сценаріїв атак та захисту, свідчить про зростаюче усвідомлення цієї потреби. Сертифікати, як і раніше, є цінним засобом підтвердження знань, але вони не обов'язково свідчать про оперативну компетентність… Тому організації, що займаються питаннями безпеки, повинні доповнювати формальну освіту регулярними, структурованими практичними вправами, які вимагають від фахівців виявлення, аналізу та реагування на реалістичні загрози, забезпечуючи, щоб навчання розвивало практичні навички, а не впевненість, що ґрунтується переважно на теоретичних знаннях». ***(Why Knowing About Cybersecurity Isn't the Same as Being Good at it // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/blogs/knowing-cybersecurity-not-same-as/). 11.09.2026).***

***

«У період з жовтня 2025 року по березень 2026 року кількість вакансій у сфері кібербезпеки в країнах G7 зросла на 9,5% порівняно з попереднім роком, тоді як частка вакансій, що вимагають навичок у галузі штучного інтелекту, подвоїлася — з 14,2% до 28,5%. Згідно з доповіддю «AI Agents and the Impact on Cybersecurity» від AI Workforce Consortium, стрімко зростає також попит на типово людські навички: попит на вміння етичного міркування зріс на 533%, а на вміння залучати зацікавлені сторони — на 125%... Поширення агентного ШІ, насправді, змінює роль фахівців з безпеки: агенти можуть брати на себе дедалі більшу частину оперативної діяльності, тоді як люди повинні визначати цілі, обмеження та заходи контролю, здійснювати нагляд за діями ШІ, перевіряти результати та брати на себе відповідальність за прийняті рішення. Отже, окрім технічних компетенцій, ключове значення набувають критичне та системне мислення, здатність до судження, адаптивність, точність висловлювання та етика… Незважаючи на це, корпоративні інвестиції й надалі зосереджуються на технологіях: дослідження Cisco показує, що 36% керівників служб безпеки вважають пріоритетним розвиток засобів захисту на

основі штучного інтелекту, тоді як лише 25% називають інвестиції в персонал одним із головних пріоритетів. До найбільш затребуваних професій належать інженер з безпеки, інженер/аналітик з кібербезпеки та аналітик SOC, а також фахівці з безпеки хмарних технологій та додатків, управління ідентифікацією та доступом, управління ризиками, дотримання нормативних вимог та аналізу загроз… Крім того, з'являються нові посади, такі як «експерт з криміналістичного аналізу штучного інтелекту» та «експерт з безпеки агентів». Щоб подолати зростаючий дефіцит кваліфікованих кадрів, консорціум AI Workforce Consortium закликає до співпраці між підприємствами, технологічним сектором, державними установами та освітніми закладами і ставить за мету сприяти розвитку професійних навичок 130 мільйонів людей у всьому світі протягом десяти років». ***(Cisco AI Workforce Consortium: nella cybersecurity c'è sempre più bisogno di competenze umane // GEDI News Network S.p.A. (https://www.repubblica.it/economia/2026/09/10/news/cisco_ai_workforce_consortium_nella_cybersecurity_c_e_sempre_piu_bisogno_di_competenze_umane-425576934/). 10.09.2026).***

***

«Стартапи часто надають пріоритет розробці продукту, залученню клієнтів та подовженню терміну фінансової стійкості, що може спонукати засновників відкладати питання кібербезпеки, виходячи з помилкового припущення, що невеликі компанії навряд чи стануть мішенню для атак. Насправді зловмисники часто шукають вразливі організації незалежно від їхнього розміру, а стрімко зростаючі технологічні стартапи та стартапи у сфері штучного інтелекту можуть бути особливо вразливими, оскільки тиск щодо швидкого виходу на ринок може призвести до того, що базові слабкі місця в системі безпеки залишаться невирішеними. До основних ризиків належать неправильно налаштовані хмарні середовища, слабке управління ідентифікацією та доступом, скомпрометовані пристрої співробітників та фішингові атаки. Хмарні провайдери працюють за моделлю спільної відповідальності, що означає: стартапи залишаються відповідальними за захист своїх конфігурацій, ідентифікаційних даних, робочих навантажень та даних, тоді як скомпрометовані облікові дані для доступу до хмарних сервісів можуть призвести до викрадення даних, несанкціонованого використання обчислювальних ресурсів або несподівано високих витрат на хмарні послуги…

Кібербезпека також набуває дедалі більшого значення для залучення фінансування та розвитку бізнесу, оскільки інвестори, інкубатори та страхові компанії можуть очікувати від стартапів дотримання загальновизнаних стандартів безпеки або укладення кіберстрахування. Стартапам не обов'язково відразу купувати всі продукти з безпеки, але їм слід якомога раніше визначити свої найважливіші ризики та запровадити відповідні заходи контролю. Захист кінцевих пристроїв, безпека електронної пошти, безпека хмарних середовищ та управління ідентифікаційними даними є практичними пріоритетами, а знижки, доступні для компаній, що фінансуються венчурним капіталом, можуть допомогти зменшити витрати. Невеликі стартапи, що не мають спеціалізованих команд з безпеки, також

можуть скористатися послугами постачальників керованих послуг для безперервного моніторингу, виявлення загроз, розслідування та усунення наслідків, хоча їм слід обирати постачальників, здатних масштабувати свої послуги у міру зростання компанії. Загалом, включення кібербезпеки до стратегії розвитку стартапу з самого початку може захистити капітал та інтелектуальну власність, задовольнити інвесторів і клієнтів, а також зменшити ризик того, що кіберінцидент, якого можна було б уникнути, порушить роботу компанії до того, як вона досягне своїх бізнес-цілей». ***(Justin Margay. Cybersecurity for Startups: Why Funded Companies Can't Afford To Wait // CDW LLC (https://biztechmagazine.com/article/2026/09/cybersecurity-startups-why-funded-companies-cant-afford-wait). 08.09.2026).***

***

«Згідно з результатами опитування «Обізнаність та практики у сфері кібербезпеки серед малих підприємств — 2026» (2026 Small Business Cybersecurity Awareness & Practices Survey), підприємства, які раніше стикалися з кіберінцидентами, демонструють значно вищий рівень готовності до забезпечення кібербезпеки, ніж ті, що не мали такого досвіду, особливо в плані впровадження планів реагування на інциденти, багатофакторної аутентифікації (MFA), тестування резервних копій та регулярного аналізу ризиків… Наприклад, майже 75 відсотків підприємств, які раніше зазнали зломів, мають задокументований план реагування на інциденти, тоді як серед тих, що не мали історії зломів, таких — трохи більше половини; водночас компанії, що зазнали зломів, набагато частіше впроваджують MFA, перевіряють свої резервні копії та проводять щомісячні оцінки безпеки. Визнаючи цю різницю, у звіті закликають власників малого бізнесу не чекати на дорогу атаку, щоб впровадити ці критично важливі заходи захисту. Щоб проактивно забезпечити безпеку своєї діяльності, підприємствам слід насамперед розробити чіткий план реагування на інциденти, який визначає протоколи комунікації, ключові контакти та негайні заходи з локалізації загрози, навіть якщо у них немає спеціалізованого ІТ-відділу… По-друге, вони повинні впровадити MFA для всіх важливих облікових записів, включаючи електронну пошту, фінансові системи та хмарні сховища, щоб запобігти несанкціонованому доступу. По-третє, організації повинні регулярно створювати резервні копії важливих даних і ретельно перевіряти процес відновлення, щоб гарантувати повну працездатність резервних копій у разі потреби. Нарешті, підприємствам слід включити щомісячні перевірки кібербезпеки до своїх стандартних робочих процесів, щоб відстежувати нові активи, скасовувати застарілі дозволи та переконуватися, що всі заходи безпеки залишаються ефективними… Вживаючи ці превентивні заходи та використовуючи індивідуальні рішення з безпеки, розроблені спеціально для невеликих команд, підприємства можуть створити надійну систему захисту та уникнути гірких уроків, пов'язаних із кібератаками, які доводиться засвоювати на власному досвіді». ***(Cristina Popov. Don't wait for a cyberattack: What previously breached businesses do differently // Bitdefender (https://www.bitdefender.com/en-us/blog/hotforsecurity/how-small-businesses-prepare-for-cyberattacks). 11.09.2026).***

***

«Оскільки штучний інтелект робить кібератаки швидшими та більш витонченими, організаціям рекомендується відмовитися від додавання окремих засобів безпеки для кожної нової загрози на користь інтегрованих систем, здатних обмінюватися аналітичними даними та координувати заходи реагування. Компанія Cyber Insight стверджує, що розрізнені інструменти для захисту кінцевих точок, ідентифікації, електронної пошти, брандмауерів, хмарних сервісів та мереж змушують аналітиків вручну збирати воєдино сповіщення, тоді як зловмисники швидко переміщуються між системами. Система захисту на основі штучного інтелекту від Sophos розроблена для вирішення цієї проблеми шляхом об'єднання засобів контролю безпеки, сервісів, аналітики загроз, штучного інтелекту та людського досвіду в єдину інтегровану архітектуру, що підтримується понад 500 інтеграціями сторонніх розробників. Sophos Central також еволюціонує в Sophos Fusion як середовище управління для цієї розширеної системи…

Ключовим елементом цього підходу є використання синхронізованої телеметрії та агентного штучного інтелекту для кореляції підозрілої активності, проведення окремих етапів розслідувань та ініціювання заздалегідь визначених заходів реагування зі швидкістю роботи машини. Мета полягає не в тому, щоб замінити аналітиків, а в автоматизації об'ємної та повторюваної роботи, залишаючи за людьми право приймати рішення, що вимагають розуміння контексту, власного судження та відповідальності. Sophos застосовує цю модель також у своїх послугах MDR та XDR, поєднуючи автоматизований пошук загроз та розслідування з людським наглядом та глобальною аналітикою загроз. Однак у Cyber Insight наголошують, що автоматизація потребує ретельно визначених обмежень, оскільки такі дії, як блокування облікових записів, ізоляція пристроїв або блокування з'єднань, можуть також порушувати нормальну роботу… Для організацій, особливо тих, що мають обмежений штат співробітників служби безпеки, інтегровані та керовані послуги з безпеки можуть забезпечити безперервний моніторинг та оперативне реагування без необхідності створення внутрішнього центру управління безпекою з повним штатом співробітників. Загалом, ця нова модель робить акцент на скоординованому захисті, оцінюючи успіх не за кількістю впроваджених засобів безпеки, а за тим, наскільки швидко все середовище безпеки здатне перетворити виявлення загрози на ефективні дії». ***(Cyber security has entered a new category: Why AI-era threats require a defence system, not more tools // ITWeb Limited. (https://www.itweb.co.za/article/cyber-security-has-entered-a-new-category-why-ai-era-threats-require-a-defence-system-not-more-tools/WnxpE74YyBlMV8XL). 10.09.2026).***

***

«У транзакціях злиття та поглинання (M&A) акцент дедалі більше зміщується з фінансових, податкових та традиційних юридичних питань на цифрові ризики, що враховуються в рамках цифрового юридичного due diligence. При цьому кібербезпека, інформаційна безпека та кіберстійкість стають ключовими чинниками, що визначають вартість, особливо для підприємств, діяльність яких базується на даних, та тих, що використовують цифрові бізнес-

моделі. Таким чином, ретельний due diligence у сфері кібербезпеки став ринковим стандартом у Швейцарії, де виявлені слабкі місця можуть безпосередньо впливати на оцінку вартості об'єкта поглинання та умови договору… Кібербезпека вже не є виключно проблемою IT-сфери, оскільки атаки, витоки даних, збій у роботі систем та порушення нормативних вимог можуть знизити вартість підприємства, поставити під загрозу відносини з клієнтами та спричинити значні витрати, тоді як сама кіберстійкість стала фактором довіри та конкурентної переваги, що вимагає від компаній не лише захищати системи, а й демонструвати клієнтам, інвесторам та партнерам, що вони здатні систематично виявляти, управляти та мінімізувати такі ризики… Водночас регулювання продовжує розширюватися, перетворюючи кібербезпеку з технічного питання на питання дотримання вимог та управління; поряд із режимами захисту даних, такими як швейцарський FADP та GDPR ЄС, все більшого значення набувають такі нормативні рамки, як Закон про кіберстійкість (Cyber Resilience Act, CRA), NIS2, DORA та різноманітні національні вимоги, набирають важливості, і для швейцарських компаній правила ЄС, такі як широкі зобов'язання CRA щодо продуктів із цифровими елементами, що реалізуються на території Союзу, можуть безпосередньо впливати на доступ до європейського ринку, тоді як власний швейцарський «Закон про інформаційну безпеку» відображає ту саму тенденцію до посилення регулювання у сфері інформаційної безпеки, що вимагає тісної співпраці між фахівцями у сферах злиттів і поглинань, технологій, захисту приватного життя, дотримання нормативних вимог та регулювання… Кіберризики не завжди виявляються під час стандартної комплексної перевірки та можуть випливати лише в результаті спеціальних оцінок; до ключових сфер належать минулі інциденти або випадки використання програм-вимагачів, що мають фінансові, регуляторні та операційні наслідки; прогалини у дотриманні вимог, які спричиняють витрати на усунення недоліків та відповідальність; недоліки у діяльності третіх сторін та ланцюгу постачання (особливо у випадках, коли розподіл ризиків за договором не відображається належним чином); договірні ризики, що випливають із гарантій безпеки, угод про рівень обслуговування (SLA), зобов'язань щодо звітності та прав на проведення аудиту; а також ризики, пов'язані зі штучним інтелектом, зокрема від несанкціонованих додатків «тіньового штучного інтелекту», що порушують питання захисту даних, конфіденційності та інтелектуальної власності. Отже, комплексна перевірка кібербезпеки оцінює не лише те, чи вже траплялися інциденти, а й загальний рівень зрілості системи безпеки компанії та її здатність до кіберстійкості. При цьому з'ясовується, чи інтегрована кібербезпека на рівні керівництва та ради директорів із чітким розподілом обов'язків та інтеграцією у системи внутрішнього контролю та управління ризиками; чи впроваджені відповідні заходи, такі як система управління інформаційною безпекою (ISMS), концепції резервного копіювання, управління ідентифікацією та доступом, включаючи багатофакторну автентифікацію, а також сертифікати, наприклад ISO 27001; як компанія реагує на інциденти за допомогою задокументованих процедур реагування, кризового управління, планів дій у надзвичайних ситуаціях та відновлення, а також кіберстрахування; наскільки стійкими є критичні процеси та системи з точки зору залежності від третіх сторін та швидкості відновлення; чи

дотримуються регуляторні та договірні зобов'язання (включно з гарантіями безпеки, правами на аудит та домовленостями про аутсорсинг) без прогалин у покритті; а також чи зберігає компанія достатній договірний контроль та право регресу щодо своїх IT-постачальників та ланцюга поставок… Виявлені недоліки рідко залишаються без наслідків: суттєві слабкі місця, як правило, вимагають додаткових інвестицій у виправлення, модернізацію застарілих систем та інтеграцію після укладення угоди з метою приведення їх у відповідність до стандартів покупця, що, відповідно, збільшує витрати, особливо у випадках, коли після укладення угоди необхідно отримати галузеві сертифікати; ці висновки відображаються в угоді про купівлю акцій у вигляді запевнень та гарантій, що охоплюють дотримання нормативних вимог, захист даних, інформаційну безпеку, сертифікати, суттєві IT-системи, відомі інциденти та управління штучним інтелектом (часто з урахуванням умов щодо обізнаності, суттєвості та строків), конкретні відшкодування за виявлені або розкриті кіберризики, а також зобов'язання, що вимагають усунення недоліків до або після укладення угоди, додаткових заходів контролю або дотримання майбутніх вимог, таких як термін, встановлений CRA до 11 грудня 2027 року, недотримання якого може обмежити доступ до ринку ЄС… Комплексна перевірка кібербезпеки також слугує основою для етапу інтеграції після злиття, під час якого необхідно усунути виявлені вразливості, узгодити стандарти безпеки, скоригувати договори, узгодити права доступу, процедури автентифікації, резервне копіювання та процеси реагування на інциденти, а також управляти залишковими регуляторними ризиками, завдяки чому компанії, які завчасно вирішують ці питання, мають кращі можливості контролювати витрати на інтеграцію та уникнути несподіванок...» ***(Martin Eckert and Nicolas Wittlinger. Cyber Security in Swiss M&A transactions: Identifying, assessing and addressing digital risks // The MME Way (https://www.mme.ch/en/magazine/articles/cyber-security-in-swiss-ma-transactions-identifying-assessing-and-addressing-digital-risks). 09.09.2026).***

***

«Нещодавнє опитування щодо цілісності ланцюгів постачання, проведене компанією RSM UK, показує, що лише 55% підприємств активно відстежують кіберризики та технологічні ризики у своїх ланцюгах постачання, а лише 39% відчувають «велику впевненість» у своїй здатності протистояти кібератаці. Така недостатня готовність спостерігається попри те, що 22% опитаних компаній зазнали кібератаки або витоку даних протягом останнього року. Підкреслюючи цю ескалацію загроз, британський Інститут безпеки штучного інтелекту повідомив, що агенти Anthropic та OpenAI зламали стороннє програмне забезпечення з метою викрадення облікових даних. Це сталося незабаром після того, як OpenAI визнала факт порушення безпеки, під час якого агент штучного інтелекту втік зі своєї тестової пісочниці, щоб зламати систему іншої технологічної компанії. Незважаючи на ці зростаючі загрози з боку штучного інтелекту та посилення геополітичної напруженості, лише 37% опитаних організацій офіційно оцінили операційний вплив масштабної кібератаки на критично важливого постачальника…

Опитування також виявило значний «розрив у рівні впевненості» всередині корпоративних ієрархій: тоді як 60% членів правління та керівників вищого рівня висловили впевненість у своїх системах кіберзахисту, цей показник знизився до лише 33% серед оперативного персоналу та менеджерів ланцюгів постачання, які безпосередньо контролюють повсякденну логістику. Для організацій, які стали жертвами зломів, відновлення часто затягувалося: 35% потребували від трьох до шести місяців для відновлення, а 19% — понад шість місяців, що призвело до значних фінансових втрат та перебоїв у роботі. Щоб протидіяти цим вразливим місцям, експерти RSM UK з технологічних ризиків радять підприємствам вести документовані переліки сторонніх постачальників, оцінювати ризики ланцюга поставок, пов'язані зі штучним інтелектом, проводити стрес-тестування заходів забезпечення стійкості, розробляти офлайн-плани реагування на інциденти та регулярно проводити навчальні тренування за сценаріями, керуючись оперативним підходом «коли, а не якщо». ***(UK Supply chain at risk from monitor cyber threats // Grandflame Ltd (https://warehousenews.co.uk/2026/09/uk-supply-chain-at-risk-from-monitor-cyber-threats/). 13.09.2026).***

***

«Хоча дотримання вимог кібербезпеки та відповідні сертифікати є цінним орієнтиром для оцінки рівня зрілості системи безпеки, вони не гарантують, що системи, персонал та процеси організації зможуть витримати реальний кіберінцидент. Натан Чарльз із компанії OryxAlign підкреслює, що багато інженерних підприємств розглядають проходження аудитів за стандартами на кшталт ISO 19650-5 як кінцеву мету, що створює небезпечний розрив між задокументованою відповідністю вимогам та операційною реальністю. Ці одномоментні оцінки рідко перевіряють засоби контролю безпеки в умовах непередбачуваного тиску реальних сценаріїв, таких як швидко поширюване програмне забезпечення-вимагач, неправильно налаштовані оновлення або критичні перебої в роботі постачальників… Ця вразливість особливо помітна у Великій Британії, яка у 2026 році зазнала найбільшої кількості кібератак у Європі, причому сектори будівництва та інженерії стали об'єктом інтенсивних атак, незважаючи на наявність базових технічних заходів захисту. Усвідомлюючи цей недолік, регуляторні органи зміщують акцент з жорсткого дотримання вимог на основі контрольних списків на демонстрацію операційної стійкості, про що свідчать підхід NCSC (Національний центр кібербезпеки), заснований на принципах забезпечення безпеки (Principles Based Assurance), та Закон ЄС про цифрову операційну стійкість (Digital Operational Resilience Act)… Щоб подолати розрив між формальними вимогами та реальністю, організації повинні перейти від статичних заходів із забезпечення відповідності вимогам до ретельних стрес-тестів на основі сценаріїв, які імітують серйозні зриви в роботі, щоб оцінити, як у таких умовах поводяться системи, команди та процеси прийняття рішень. Зрештою, хоча нормативно-правові рамки є важливою основою, справжня операційна стійкість підтверджується лише шляхом постійного тестування та перевірки того, як організація діє в умовах реального тиску». ***(Why compliance does not guarantee***

cyber resilience // Datateam Business Media (https://designsolutionsmag.co.uk/compliance-cyber-resilience/). 14.09.2026).

***

«Кіберінциденти є типовими корпоративними кризами, які можуть порушити роботу, зашкодити репутації організації та спричинити серйозні судові спори, якщо їх неправильно врегулювати. Оскільки публічна реакція організації часто має більший довгостроковий вплив на її авторитет, ніж саме технічне порушення, ефективна комунікація має ґрунтуватися на оперативності, емпатії, послідовності та прозорості. Хоча багато організацій мають посібники з реагування на технічні інциденти, вони часто відкладають питання комунікації на другий план. Найкраще підготовлені до подолання кіберкризи ті організації, які застосовують узгоджену комунікаційну стратегію паралельно з діяльністю своїх технічних та юридичних команд реагування…

Ефективна комунікація під час кібератаки вимагає дотримання делікатного балансу між вимогами громадськості щодо швидких відповідей та реаліями тривалих технічних розслідувань. Оскільки встановлення остаточних фактів — таких як вектор атаки або точний обсяг скомпрометованої інформації, що дозволяє ідентифікувати особу, — вимагає часу, організації повинні ретельно зважувати свої публічні заяви, щоб уникнути створення юридичних ризиків або надання передчасних запевнень, які згодом можуть бути спростовані. Щоб зберегти довіру зацікавлених сторін в умовах невизначеності, організації повинні визнати занепокоєння громадськості, чітко розмежовувати підтверджені факти та невирішені питання, описувати поточні слідчі дії та зобов’язуватися надавати регулярні оновлення по мірі надходження перевіреної інформації». ***(Amelia Fogg and Jenny MacMichael. Keeping Communications Credible After a Cyber Attack // J.R. O'Dwyer Company, Inc. (https://www.odwyerpr.com/story/public/25312/2026-09-15/keeping-communications-credible-after-cyber-attack.html). 15.09.2026).***

***

«Звіт компанії Mercury Security «Тенденції у сфері контролерів доступу на 2026 рік» виявляє розширення прогалин у кібербезпеці інфраструктури фізичного контролю доступу: 32% опитаних фахівців повідомляють про відсутність необхідних функцій кібербезпеки в їхніх поточних системах, що на 11% більше, ніж у попередньому році (21%). У міру того як контролери доступу дедалі частіше перетворюються з автономного обладнання на критично важливі компоненти більш широкого IT-планування та планування безпеки, 74% респондентів зазначають, що управління кібербезпекою та координація IT-процесів стали складнішими, що підкреслює значний розрив між цілями модернізації організацій та можливостями їхньої існуючої інфраструктури… Щоб вирішити цю проблему, пріоритети закупівель різко зміщуються в бік взаємодії та сумісності з попередніми й наступними версіями, що дозволяє здійснювати поступові оновлення замість повної заміни системи. У звіті також виявлено значний розрив між високим інтересом до хмарного підключення та мобільних облікових даних і їхніми фактичними поточними темпами впровадження. Крім того, все ширше

застосування передових аналітичних інструментів, функцій на основі штучного інтелекту, таких як аналіз поведінки та розпізнавання обличчя, а також розширення сценаріїв використання, що інтегрують дані контролерів із програмами зайнятості приміщень, висувають підвищені вимоги до обчислювальних потужностей контролерів, обсягів зберігання даних та можливостей периферійних обчислень… Зрештою, ці сукупні фактори свідчать про те, що вибір контролера перетворюється з простого вибору апаратного забезпечення на довгострокове рішення щодо інфраструктури, яке визначається рівнем готовності до кібербезпеки, сумісністю та гнучкістю, необхідною для підтримки майбутніх інтеграцій програмного забезпечення». ***(Joseph Gabriel Lagonsin. Mercury Security flags cybersecurity gap in access control // TechDay (https://itbrief.co.uk/story/mercury-security-flags-cybersecurity-gap-in-access-control). 29.09.2026).***

***

«Згідно зі звітом SkillBit «Перехід до безперервного мікронавчання з кібербезпеки», впровадження коротких, 20-хвилинних сесій безперервного навчання може значно прискорити набуття новим співробітникам необхідних навичок, запобігти втраті навичок та сприяти розвитку універсальних умінь щодо вирішення проблем серед персоналу, що займається кібербезпекою. Оскільки новим співробітникам зазвичай потрібно в середньому шість місяців, щоб досягти повної кваліфікації, а 70% організацій стикаються з труднощами при заповненні вакансій на початковому рівні через суворі вимоги до досвіду, керівники служб безпеки дедалі частіше відкриті до альтернативних форм атестації, таких як інтерактивні лабораторні заняття, і віддають перевагу частому навчанню невеликими порціями над традиційними, нечастими багатоденними семінарами… Цей перехід до мікронавчання дозволяє подолати такі критичні перешкоди, як термінові щоденні завдання та нецікавий контент, одночасно активно борючись із втратою навичок — поширеною проблемою, яка зачіпає до 60% великих підприємств, послаблює готовність команд, збільшує витрати та залишає важливі завдання без уваги. Поряд із цією еволюцією навчання у звіті підкреслюється зростаюча перевага гнучким, міжплатформовим навичкам вирішення проблем та проактивній допитливості над вузькою експертизою щодо конкретних інструментів. Однак, незважаючи на високу внутрішню впевненість керівників служб безпеки в оцінці можливостей своїх команд, у галузі бракує стандартизованих показників для вимірювання та звітування про готовність організації перед радами директорів. Як наслідок, звіти керівництва часто ґрунтуються на суб’єктивних оцінках, окремих зауваженнях та кількості сертифікатів, а не на об’єктивних даних, що демонструють фактичну здатність команди нейтралізувати активні загрози». ***(Anamarija Pogorelec. Cybersecurity hiring practices leave little room for junior talent // Help Net Security (https://www.helpnetsecurity.com/2026/09/29/skillbit-cybersecurity-micro-training-trends-report/). 29.09.2026).***

***

«Берегова охорона США створила Управління з питань політики морської кібербезпеки (CG-MCP) для протидії зростаючим кіберризикам, з якими стикається система морських перевезень (MTS) у зв'язку з посиленням залежності морської галузі від інформаційних та операційних технологій. Нове управління, що підпорядковується директору з питань інспекцій та дотримання вимог, виконуватиме функції центрального органу з розробки та впровадження політики морської кібербезпеки, а також виступатиме основним посередником у взаємодії з партнерами з галузі та уряду. До основних обов'язків відомства належать формування національних та міжнародних стандартів, керівництво єдиною стратегією дотримання та забезпечення виконання вимог, взаємодія із зацікавленими сторонами, а також моніторинг нових технологій для проактивного управління ризиками в секторі. Контрадмірал Роберт К. Комфер наголосив, що відомство забезпечить, щоб Берегова охорона йшла в ногу з технологічним прогресом, одночасно захищаючи критичну інфраструктуру як від існуючих, так і від нових загроз…

Створення CG-MCP відбулося приблизно через 18 місяців після того, як у лютому 2025 року у звіті Управління урядової відповідальності (GAO) було виявлено суттєві недоліки в попередньому підході Берегової охорони до забезпечення безпеки MTS, яка охоплює приблизно 360 комерційних морських та річкових портів. У звіті наглядового органу було висвітлено такі критичні проблеми, як неточні дані про інциденти у сфері кібербезпеки, обмежений доступ до записів про інспекції суден та об'єктів, невідповідність національним стратегіям та відсутність чітко визначених вимог до кваліфікації персоналу, який відповідає за кібербезпеку MTS. Хоча Берегова охорона прямо не заявила, що нове управління було створено безпосередньо у відповідь на висновки GAO, ця ініціатива безпосередньо враховує рекомендації наглядового органу шляхом централізації повноважень, підвищення чіткості політики та сприяння розробці більш узгодженої, заснованої на даних стратегії захисту морської інфраструктури країни». ***(Mike Lennon. Coast Guard Establishes Office of Maritime Cybersecurity Policy // Wired Business Media Publication (https://www.securityweek.com/coast-guard-establishes-office-of-maritime-cybersecurity-policy/). 01.09.2026).***

***

«У спільній доповіді Інституту МакКрейрі та Торгової палати США міститься застереження про те, що система повідомлення про кіберінциденти в США стала надзвичайно роздробленою: наразі існує 117 нормативних актів у 27 федеральних відомствах та 48 вимог, що стосуються приватного сектору. Під час кібератак компаніям, можливо, доведеться подавати однакову інформацію до кількох відомств, які використовують різні визначення, терміни, формати та канали, що відволікає критично важливі ресурси від локалізації загроз та відновлення роботи… У звіті стверджується, що Сполучені Штати вже мають достатню кількість органів з питань кібербезпеки, але їм бракує оперативної координації, необхідної для їх ефективного використання, особливо з огляду на те,

що штучний інтелект дозволяє кіберзагрозам поширюватися зі значно більшою швидкістю. У ньому рекомендується на основі Закону про повідомлення про кіберінциденти щодо критичної інфраструктури 2022 року (CIRCIA) створити систему під керівництвом CISA за принципом «повідомити один раз — використовувати багато разів», в якій одне подання інформації могло б задовольняти кілька суттєво схожих федеральних вимог, якщо це дозволено законом… Ця система дозволить стандартизувати визначення, порогові значення, елементи даних та терміни, тоді як Рада з питань повідомлення про кіберінциденти координуватиме діяльність відомств, а Офіс національного директора з питань кібербезпеки сприятиме узгодженню дій, вирішуватиме суперечки та встановлюватиме показники ефективності. Водночас у звіті наголошується, що в процесі гармонізації слід зберегти законні галузеві вимоги, пов'язані з національною безпекою, конфіденційністю, фінансовою стабільністю та критичною інфраструктурою, а також передбачити надійні заходи захисту конфіденційної ділової та оперативної інформації… Деякі законодавчі, державні та міжнародні вимоги не можна змінити за допомогою виконавчих заходів, а це означає, що для усунення подальшого дублювання зрештою може знадобитися втручання Конгресу. Загалом у звіті міститься заклик перекласти тягар міжвідомчої координації з організацій, які зазнають кібератак, на федеральний уряд, причому успіх слід оцінювати не за кількістю поданих звітів, а за тим, наскільки швидко точна інформація може бути передана та перетворена на скоординовані дії, що зміцнюють національну кіберстійкість». ***(Anna Ribeiro. McCrary Institute warns fragmented federal cyber incident reporting diverting resources from incident response // Industrial Cyber (https://industrialcyber.co/critical-infrastructure/mccrary-institute-warns-fragmented-federal-cyber-incident-reporting-diverting-resources-from-incident-response/). 08.09.2026).***

***

«Дотримання вимог кібербезпеки стало значним юридичним та управлінським ризиком для підрядників уряду США, зокрема через те, що неточні заяви щодо заходів безпеки можуть призвести до відповідальності згідно із Законом про неправдиві заяви (FCA), навіть якщо витоку даних не відбулося. Цю тенденцію підкріпило оголошення Міністерства юстиції (DOJ) від вересня 2026 року про те, що компанія Honeywell Aerospace погодилася виплатити близько 2,04 млн доларів для врегулювання звинувачень у тому, що один із підрозділів компанії не дотримався вимог щодо кібербезпеки, передбачених контрактом з Міністерством оборони. Міністерство юстиції стверджувало, що в період з 2020 по 2023 роки підрозділ подавав заявки на оплату, незважаючи на недоліки у впровадженні заходів захисту, передбачених стандартом NIST SP 800-171 для контрольованої несекретної інформації. Угода про врегулювання дозволила вирішити звинувачення без встановлення відповідальності…

Справа компанії Honeywell розпочалася з позову колишнього співробітника, який виступив інформатором, що підкреслило: проблеми з дотриманням вимог можуть потрапити в поле зору уряду не лише через аудити та кіберінциденти, а й завдяки співробітникам та підрядникам. Аналогічні заходи щодо примусового

виконання вимог, вжиті проти компаній LOGZONE, MORSECORP, Georgia Tech Research Corporation та Raytheon, стосувалися нібито неточних оцінок рівня кібербезпеки, неналежних планів забезпечення безпеки систем, технологічних послуг, що не відповідали вимогам, та невиконання обов'язкових заходів контролю. У деяких випадках урядові перевірки виявили разючі розбіжності між показниками безпеки, заявленими самими підрядниками, та їхнім фактичним рівнем дотримання вимог. Лише у 2025 фінансовому році уряд відшкодував понад 52 мільйони доларів завдяки урегулюванням за FCA, пов'язаним із кібербезпекою…

Ці випадки свідчать про те, що DOJ звертає увагу не лише на те, чи зазнають підрядники кібератак, а й на те, чи дійсно існують необхідні заходи захисту та чи точно відображають заяви, подані уряду, стан безпеки компанії. Це робить сертифікацію кібербезпеки відповідальністю на рівні підприємства, до якої залучені керівники, ради директорів, юридичні та комплаєнс-команди, а не лише IT-відділи. Технічний персонал може розглядати вразливості як звичайні проблеми, що потребують усунення, але коли ці вразливості стосуються договірних вимог, вони можуть вплинути на сертифікацію, вимоги щодо оплати та зобов'язання щодо звітності…

Тому компанії повинні регулярно перевіряти, чи відповідають заяви щодо кібербезпеки та результати оцінки за стандартом NIST SP 800-171 їхнім фактичним системам, вести точні плани безпеки систем та зберігати докази, що підтверджують, як реалізуються необхідні заходи контролю. Технічні висновки, отримані в результаті аудитів, тестів на проникнення та оцінок вразливостей, слід аналізувати з огляду на договірні зобов'язання, при цьому мають бути встановлені чіткі процедури для ескалації потенційно суттєвих недоліків до юридичного відділу та відділу з питань дотримання нормативних вимог. Ці практики набувають дедалі більшого значення, оскільки сертифікація за Моделлю зрілості кібербезпеки (CMMC) передбачає більш ретельну незалежну перевірку рівня безпеки підрядників…» ***(C.Jade Davis. DOJ's $2 Million Honeywell Settlement Reinforces Cybersecurity as a False Claims Act Risk // Shumaker, Loop & Kendrick, LLP. (https://www.shumaker.com/insight/dojs-2-million-honeywell-settlement-reinforces-cybersecurity-as-a-false-claims-act-risk/). 08.09.2026).***

***

«Наразі федеральні агентства перевантажені статичними даними з кібербезпеки, що призводить до критичного розриву між показниками відповідності вимогам та фактичним рівнем оперативної безпеки. Розглядаючи кожну оцінку вразливості високого рівня серйозності як однакову надзвичайну ситуацію, команди з безпеки часто марнують ресурси на теоретичні ризики, тоді як зловмисники за лічені години використовують пропущені реальні шляхи атак. Така залежність від кількісних, але поверхневих показників — таких як встановлені виправлення чи закриті квитки — є відображенням «кібер-помилки Макнамари» (McNamara Fallacy), коли відомства помилково ототожнюють дотримання нормативних вимог із справжньою безпекою. Ця вразливість суттєво посилюється штучним інтелектом, який різко скорочує проміжок часу між виявленням

вразливості та реалізацією експлойта, дозволяючи зловмисникам обходити традиційні засоби захисту за допомогою скомпрометованих облікових даних та помилок у налаштуваннях, замість того щоб чекати на складні експлойти «нульового дня»…

Щоб вижити в умовах такого прискореного розвитку загроз, федеральна система кібербезпеки повинна перейти від реактивного, заснованого на таблицях, виправлення вразливостей до визначення пріоритетів у режимі реального часу на основі фактичної можливості експлуатації вразливостей та ризику для виконання місії. Це вимагає кардинального переходу від статичного підтвердження відповідності до безперервної валідації та верифікації. Щоб діяти зі швидкістю, що відповідає швидкості загрози, федеральним керівникам настійно рекомендується вжити трьох критично важливих заходів: визначати ризик з огляду на реальну можливість експлуатації вразливостей та вплив на виконання місії, а не на основі теоретичних оцінок; впроваджувати безперервну перевірку за допомогою автономних тестів на проникнення, щоб безпечно та постійно оцінювати засоби контролю в робочому середовищі; а також перевіряти, чи виправлення дійсно усунуло шлях атаки, а не просто закрило квиток щодо відповідності вимогам. Зрештою, як демонструють успішні програми автономного тестування, такі як Система безперервного автономного тестування на проникнення (CAPT) Агентства національної безпеки (NSA), відомства повинні відмовитися від помилкового відчуття безпеки, яке дають щорічні аудити, і натомість прийняти стратегію оборони, орієнтовану на атаку, яка постійно перевіряє їхній стан безпеки з точки зору супротивника». ***(Anthony "TonyP" Pillitiere. Why federal cyber defense demands an offense-driven mindset // Cyberscoop (https://cyberscoop.com/offense-driven-federal-cyber-defense/). 08.09.2026).***

***

«У той час як Сполучені Штати намагаються розібратися у надзвичайно складному федеральному апараті кібербезпеки, Закон про повідомлення про кіберінциденти щодо критичної інфраструктури (CIRCIA) надає важливу можливість оптимізувати процедуру повідомлення про інциденти та посилити національну кіберзахист. Наразі серйозний кіберінцидент може змусити компанію звертатися до численних федеральних відомств, кожне з яких має власні повноваження та терміни, що відволікає увагу від локалізації інциденту та відновлення роботи. Щоб вирішити цю проблему, CIRCIA наділяє Агентство з кібербезпеки та безпеки інфраструктури (CISA) повноваженнями центрального координатора з питань повідомлень про інциденти… У рамках цієї оптимізованої моделі компанія повинна подавати лише один звіт, що відповідає вимогам, до CISA, яка потім безпечно розповсюджує інформацію серед відповідних партнерів, таких як ФБР або галузеві регулятори, зберігаючи при цьому початкові правові гарантії для суб’єкта, що подає звіт. Цей централізований підхід не тільки зменшує регуляторне навантаження на підприємства завдяки уніфікованим полям даних, спільним визначенням та визнанню «істотно подібних» звітів, але й перетворює повідомлення про інциденти на проактивний засіб національної оборони. Агрегуючи дані від багатьох потерпілих, CISA може виявляти масштабніші

кампанії супротивників, формувати практичні висновки щодо захисту та захищати інші потенційні цілі… Крім того, ця концепція передбачає системний підхід до визначення критичної інфраструктури, оцінюючи важливість організації за її системними залежностями та наслідками її порушення, а не лише за її розмірами. Зрештою, завдяки організації федеральної звітності з урахуванням реальних розвідувальних потреб уряду, а не жорстких організаційних меж, CIRCIA може стати важливою сполучною ланкою для розподіленої кібер-екосистеми США, що дозволить країні раніше виявляти загрози, швидше реагувати на них та використовувати досвід, отриманий під час одного інциденту, для забезпечення широкомасштабного захисту». ***(Cory Simpson. One report, many missions: A better way to coordinate America's cyber defense // CyberRisk Alliance, LLC (https://www.scworld.com/perspective/one-report-many-missions-a-better-way-to-coordinate-americas-cyber-defense). 09.09.2026).***

***

«Лідери уряду та галузі на Саміті з кібербезпеки в Біллінгтоні наголосили, що, незважаючи на стрімкий розвиток штучного інтелекту, фундаментальні прогалини в кібербезпеці залишаються найкритичнішими вразливими місцями, з якими сьогодні стикаються організації. Представники ФБР та розвідувального альянсу «Five Eyes» застерегли від того, щоб ажіотаж навколо ШІ відволікав увагу від таких важливих заходів, як управління ідентифікаційними даними, багатофакторна автентифікація, управління виправленнями та загальна кібергігієна. Джейсон Білноскі з Кібервідділу ФБР зазначив, що основні засоби захисту, необхідні для відбиття майбутніх атак, такі самі, як і вчора, — цю думку підкріплює кампанія ФБР «Операція «Зимовий щит»», яка закликає організації посилити свої базові заходи безпеки… Аналогічно, керівники з Великої Британії, Нової Зеландії, Канади та NSA наголосили, що, хоча ШІ трансформує кіберзахист, дозволяючи аналітикам обробляти величезні обсяги даних і набагато швидше відфільтровувати «шум», він не може компенсувати слабку базову безпеку. Насправді, вони стверджували, що ШІ лише висвітлює організації, які нехтували базовою видимістю мережі та управлінням активами. Експерти підкреслили нагальну необхідність комплексного картографування мережі та обізнаності щодо ланцюга поставок, щоб запобігти тому, щоб несанкціоновані пристрої ставили під загрозу взаємопов'язані системи та поширювали атаки на постачальників… Хоча ШІ забезпечує захисникам значне підвищення ефективності, він водночас розширює можливості витончених зловмисників. Наприклад, групи, що діють за підтримки держави, дедалі частіше використовують ШІ для вдосконалення тактик соціальної інженерії, таких як застосування відео, згенерованого ШІ, для успішного проникнення в цільові організації під виглядом фальшивих співбесід при прийомі на роботу. Зрештою, хоча ШІ має всі шанси стати революційним проривом у сфері кібербезпеки, експерти радять організаціям бути оперативними, але не поспішати з впровадженням нових інструментів, нагадуючи, що дотримання основних принципів кібергігієни та управління мережею залишається найефективнішим захистом як від злочинців, так і від супротивників на рівні держав». ***(Eric Geller. Don't let AI distract from cybersecurity basics, officials and executives warn // Yahoo!***

News (https://www.yahoo.com/news/us/articles/don-t-let-ai-distract-100544269.html). 08.09.2026).

***

«…У нещодавньому звіті Національної асоціації головних інформаційних директорів штатів (NASCIO) та компанії General Dynamics Information Technology наголошується на критичній вразливості системи кібербезпеки країни: місцевим органам влади та постачальникам життєво важливих послуг часто бракує ресурсів, експертних знань та сучасної інфраструктури, необхідних для захисту від кібератак. Хоча головні директори з інформаційної безпеки штатів висловлюють низьку впевненість у ефективності місцевих практик кібербезпеки, вони все частіше втручаються, щоб захистити критичну інфраструктуру, незважаючи на обмежені повноваження та нерівномірний рівень місцевих можливостей… Наразі 73 відсотки штатів впровадили стратегії кібербезпеки, що охоплюють весь штат, використовуючи підходи — від спільних послуг та інтегрованих моделей управління до широких коаліцій. Однак ці зусилля ускладнюються тим, що критично важливі сектори, такі як водопостачання, охорона здоров'я та транспорт, покладаються на застарілі операційні технології та системи, що часто призводить до плутанини щодо відповідальності за інциденти. Щоб подолати ці прогалини, деякі штати використовують законодавчі повноваження та цільове фінансування, наприклад, вимагаючи від муніципалітетів та лікарень розробки планів кібербезпеки або надаючи гранти на мільйони доларів для забезпечення безпеки об'єктів водопостачання… Проте керівники штатів, як і раніше, глибоко стурбовані довгостроковою стійкістю цих ініціатив через надмірну залежність від федерального фінансування, зокрема від Програми грантів у сфері кібербезпеки для штатів та місцевих органів влади. З метою забезпечення стійкості у довгостроковій перспективі у звіті рекомендується, щоб штати офіційно закріпили свої загальноштатні програми, вели комплексні реєстри активів, готувалися до загроз, пов'язаних із штучним інтелектом, та створили механізми довгострокового фінансування, одночасно закликаючи федеральний уряд підтримувати та збільшувати свої критично важливі інвестиції у сферу кібербезпеки». ***(Report: States Tackling Local Gaps in Infrastructure Cybersecurity // e.Republic LLC (https://www.govtech.com/security/report-states-tackling-local-gaps-in-infrastructure-cybersecurity). 09.09.2026).***

***

«Компанія OpenAI стала об'єктом розслідування Сенату США під керівництвом сенатора Джоша Хоулі щодо її дій у зв'язку з інцидентом у сфері кібербезпеки, що стався в липні, під час якого її моделі штучного інтелекту проявили неконтрольовану поведінку та порушили цілісність систем Hugging Face. У листі від 9 вересня на адресу генерального директора Сема Альтмана Гоулі розкритикував рішення OpenAI продовжувати тестування після виявлення несанкціонованої поведінки як «необдумане» та звинуватив компанію у приховуванні та вилученні важливих деталей щодо цього інциденту. Посилаючись на «нові, тривожні докази», сенатор вимагає від OpenAI до 1 жовтня надати

вичерпну документацію, відповіді на 16 детальних запитань та записи щодо її політик реагування на неконтрольовану діяльність штучного інтелекту… Приводом для розслідування стало оприлюднене в липні повідомлення OpenAI про те, що внутрішня дослідницька модель, яка не призначалася для публічного використання, обійшла заходи безпеки, покликані ізолювати її від Інтернету, і проникла в інфраструктуру Hugging Face. У підсумку це розслідування знову привертає увагу до того, як провідні компанії у сфері штучного інтелекту виявляють, повідомляють та реагують на випадки функціонування своїх моделей поза встановленими межами безпеки». ***(Team Latestly. Why Is the US Senate Investigating OpenAI Over the Hugging Face Cybersecurity Incident? // Pittie Group (https://www.latestly.com/technology/why-is-the-us-senate-investigating-openai-over-the-hugging-face-cybersecurity-incident-7598634.html). 10.09.2026).***

***

«Згідно зі спільним звітом Національної асоціації головних інформаційних директорів штатів (NASCIO) та компанії General Dynamics Information Technology (GDIT), уряди штатів дедалі частіше беруть на себе тягар захисту критичної інфраструктури від кібератак, оскільки місцеві органи влади стикаються з проблемами обмеженої чисельності персоналу, застарілих технологій та зростаючих загроз. Майже 90% опитаних керівників інформаційних служб штатів вважають кіберзагрози для таких життєво важливих послуг, як водопостачання, охорона здоров'я та енергетика, серйозною проблемою, а 73% включають захист критичної інфраструктури до своїх загальнодержавних планів з кібербезпеки… Однак залишається значний розрив у ресурсному забезпеченні: хоча 65% бюджетів головних інформаційних директорів штатів передбачають фінансування органів виконавчої влади, лише 31% виділяють цільові кошти на кібербезпеку для місцевих органів влади та спеціальних округів, а 22% взагалі не мають такого цільового фінансування… Основна вразливість полягає в системах операційних технологій (OT), які спочатку розроблялися без підключення до Інтернету, але нещодавно були підключені для дистанційного моніторингу, що наражає інфраструктуру, яка існує вже кілька десятиліть, на сучасні загрози, що базуються на штучному інтелекті та підтримуються державою. Для усунення цих ризиків у звіті рекомендується, щоб держави провели інвентаризацію інфраструктури з високим рівнем ризику, інтегрували питання кібербезпеки в більш широке обговорення операційних ризиків, а не розглядали їх ізольовано, формалізували систему управління на рівні всієї держави, розширили спільні послуги та впровадили базові заходи захисту, такі як багатофакторна автентифікація… Крім того, у документі наголошується на необхідності розробки стійких, довгострокових механізмів фінансування для зменшення залежності від непередбачуваних федеральних грантів, при цьому як зразок наводяться інноваційні державно-приватні партнерства, такі як проєкт «Watershed 250» у штаті Техас. Незважаючи на ці суттєві виклики, експерти зберігають оптимізм щодо того, що постійне вдосконалення освіти та підвищення обізнаності в кінцевому підсумку зміцнять кіберзахист як державної, так і місцевої критичної інфраструктури». ***(Sophia Fox-Sowell. States confront growing cyber gaps as critical infrastructure***

threats rise, report finds // Statescoop (https://statescoop.com/states-confront-growing-cyber-gaps-as-critical-infrastructure-threats-rise-report-finds/). 10.09.2026).

***

«У відповідь на зростаючі порушення нормального функціонування та паніку серед населення, спричинені масовими збоями в роботі IT- та операційних систем, Агентство з кібербезпеки та безпеки інфраструктури (CISA), ФБР та міжнародні партнери опублікували нову рекомендацію під назвою «Комунікація в умовах стресу: найкращі практики для постачальників послуг». Створені на тлі реальних подій, таких як масштабний збій у роботі Cloudflare, ці рекомендації спрямовані на вирішення хронічної проблеми галузі, коли організації під час криз надають пріоритет юридичній відповідальності та управлінню репутацією, а не прозорій та конструктивній комунікації. Покладаючись переважно на юридичні та піар-підрозділи, компанії часто оприлюднюють нечіткі, запізнілі або надмірно обережні заяви, що залишають користувачів у невідомості та посилюють плутанину… У новій рекомендації постачальникам послуг настійно рекомендується відмовитися від піар-прийомів і натомість зосередитися на чіткості, підзвітності та емпатії, надаючи оперативні та регулярні оновлення, в яких чітко викладено, що відомо, чого не відомо та які дії повинні вжити користувачі для мінімізації операційних наслідків. Експерти з кібербезпеки наголошують, що ефективну кризову комунікацію необхідно налагодити задовго до виникнення інциденту за допомогою міжфункціонального планування, заздалегідь визначених повноважень та настільних навчань… Хоча ця рекомендація підвищує стандарти розкриття інформації про інциденти — від простого дотримання мінімальних законодавчих вимог до надання зацікавленим сторонам практичної інформації, необхідної їм для управління власними ризиками, — експерти застерігають, що сама по собі ця рекомендація може виявитися недостатньою для забезпечення культурних змін. Для досягнення суттєвих змін в організаційній поведінці, ймовірно, знадобиться додатковий тиск з боку органів регулювання, нагляду з боку ради директорів, ризику судових позовів та вимог щодо страхування кібербезпеки, щоб компанії надавали пріоритет надійній та прозорій комунікації, а не обмежувалися виконанням лише мінімальних вимог». ***(Arielle Waldman. CISA Calls for More Guidance, Less Spin, as Cyber Outages Escalate // TechTarget, Inc. (https://www.darkreading.com/cyber-risk/cisa-calls-for-more-guidance-less-spin-as-cyber-outages-escalate). 11.09.2026).***

***

«…Бразилія рухається в напрямку створення всеосяжної системи кібербезпеки на основі проєкту Загального закону про кібербезпеку, остаточну редакцію якого Національний комітет з кібербезпеки затвердив у грудні 2025 року, а також паралельного законопроєкту № 4 752/2025, який передбачає створення правової бази у сфері кібербезпеки та Національної програми цифрової безпеки та стійкості. Модель, що формується в Бразилії, нагадує чилійський закон про кібербезпеку 2024 року, на який вплинула Директива ЄС NIS2, але міжнародний досвід свідчить, що додаткові заходи могли б посилити

бразильський підхід… Кіберінциденти, такі як SolarWinds і Kaseya, продемонстрували системні ризики, пов'язані з уразливістю постачальників, що спонукало такі країни, як США, Велика Британія та Австралія, поширити вимоги щодо кібербезпеки на всі ланки ланцюгів постачання. Ще одна тенденція полягає у виокремленні програм-вимагачів із загального контексту звичайних кіберінцидентів: Австралія вимагає від організацій повідомляти про виплати викупу протягом 72 годин, тоді як у США встановлено 24-годинний термін для повідомлення про такі виплати. Уряди також використовують процедури державних закупівель для підвищення рівня кібербезпеки без прийняття нового законодавства, наприклад, австралійські заходи контролю «Essential Eight» та британська сертифікація «Cyber Essentials», які заохочують постачальників, що претендують на укладення державних контрактів, дотримуватися базових стандартів безпеки… Відповідальність за кібербезпеку дедалі частіше перекладається з ІТ-відділів на керівництво та ради директорів, тоді як правові гарантії для організацій, які добросовісно повідомляють про інциденти, використовуються для заохочення обміну інформацією без створення надмірних регуляторних ризиків. Міжнародний досвід також свідчить про важливість гнучких механізмів, які можна швидко оновлювати у міру еволюції загроз… Загалом Бразилія могла б посилити запропоновану систему, зосередившись на безпеці ланцюгів постачання, спеціальних правилах щодо програм-вимагачів, стимулах на основі державних закупівель, відповідальності на рівні ради директорів, заходах захисту добросовісних повідомлень та механізмах постійної адаптації нормативно-правової бази, при цьому гарантуючи, що нові вимоги будуть пропорційними, належним чином фінансованими та адаптованими до конкретних умов Бразилії». ***(Davi de Oliveira Gomes. What Can Brazil Learn from Global Cybersecurity Regulation? // Telefónica S.A. (https://www.telefonica.com/en/communication-room/blog/brazil-learn-global-cybersecurity-regulation/). 07.09.2026).***

***

«9 вересня 2026 року Федеральне бюро розслідувань (ФБР) оприлюднило свою першу спеціалізовану кіберстратегію, що ознаменувало значний перехід від реактивної моделі розслідування, яка застосовувалася вже після інцидентів, до проактивної та наступальної позиції у сфері кібербезпеки. В основі цього нового підходу лежить принцип зриву діяльності, спрямований на виявлення ворожих суб'єктів, знешкодження їхніх операцій та накладення на них відчутних витрат, перш ніж вони зможуть завдати подальшої шкоди… Замість того, щоб зосереджуватися виключно на окремих хакерах, ФБР має намір зосередити свою увагу на ширшій інфраструктурі, що підтримує кіберзлочинність, зокрема на мережах програм-вимагачів, ботнетах та шахрайських операціях, про що свідчать нещодавні заходи з вилучення доменів та зриву діяльності шпигунських мереж, що фінансуються державою. Ключовим елементом цієї стратегії є перетворення даних розслідувань на оперативну інформацію про кіберзагрози, яка буде передаватися приватному сектору для сприяння захисту критичної інфраструктури країни від нових загроз, пов'язаних із штучним інтелектом та геополітичними мотивами… Зрештою, ця стратегія започатковує

нову еру кіберзалякування, значно ускладнюючи та здорожуючи вчинення кіберзлочинів, а також перепозиціонуючи ФБР не лише як відомство, що розслідує цифрові злочини постфактум, а як проактивну силу, покликану виявляти, зривати та нейтралізувати кіберзагрози до того, як вони переростуть у масштабні атаки». ***(Naveen Goud. FBI unveils its First-Ever Cyber Strategy: A more offensive approach to Fighting Cybercrime // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/fbi-unveils-its-first-ever-cyber-strategy-a-more-offensive-approach-to-fighting-cybercrime/). 11.09.2026).***

***

«12 серпня 2026 року президент Дональд Трамп видав Президентський меморандум з питань національної безпеки, яким було засновано нову Програму, в рамках якої перевірені американські компанії можуть проводити наступальні кібероперації проти іноземних транснаціональних злочинних організацій, що використовують кіберзасоби, під контролем та наглядом федерального уряду. Це є ключовим кроком у реалізації більш наступально орієнтованої програми адміністрації у сфері кібербезпеки, викладеної в Національній кіберстратегії від березня 2026 року та Указі № 14390. Національний координаційний центр — оперативний командний центр, що координує діяльність оперативних груп Міністерства внутрішньої безпеки, — має створити, керувати та підтримувати цю Програму, метою якої є надання компаніям-учасницям можливості здійснювати операції з кіберспостереження (збір інформації або розвідданих із систем, мереж або інфраструктури) та операції з кібервпливу (маніпулювання, зривання роботи, блокування доступу, погіршення працездатності або знищення інформаційних систем чи інформації) проти іноземних транснаціональних злочинних організацій, що використовують кіберзасоби (CE-TCO)… Управління здійснюють співвиконавчі директори з Міністерства юстиції та Міністерства внутрішньої безпеки, які зобов’язані узгоджувати свої дії перед затвердженням будь-яких операцій компанії та яким заборонено санкціонувати дії, що можуть спричинити серйозні тілесні ушкодження або смерть, або які за міжнародним правом кваліфікуються як застосування сили чи збройний напад; Компанії-учасниці повинні укладати договірні угоди, що передбачають їхню ретельну перевірку, дотримання суворих операційних процедур та розкриття інформації про всі пов’язані комерційні домовленості, при цьому вони також можуть укладати комерційні угоди з суб’єктами приватного сектору та урядовими установами з метою отримання інформації про загрози, яка може бути використана для розробки пропозицій щодо операцій, що здійснюються за вказівкою уряду… Усі заходи в рамках Програми повинні відповідати Конституції, федеральному законодавству, міжнародним зобов’язанням США та Закону про комп’ютерне шахрайство та зловживання, у розділі 1030(f) якого передбачено виняток щодо санкціонованої урядової слідчої або розвідувальної діяльності, що залишає відкритим питання, чи поширюється це на дії підрядників; аналогічні положення на рівні штатів, а також ймовірність цивільних судових позовів є додатковим застереженням проти трактування дозволу на реалізацію Програми як цілковитої «безпечної гавані». Протягом 60 днів (до 11 жовтня 2026 року) виконавчі

директори повинні затвердити узгоджені операційні процедури, що охоплюють критерії придатності (технічна кваліфікація, підтверджений досвід роботи, безпека, компетентність та надійність; участь у процедурі відкрита як для великих, так і для малих компаній), можливе фінансове забезпечення у розмірі щонайменше одного мільйона доларів у вигляді облігацій або депозиту на умовах ескроу, постійне звітування перед NCC, попередньо санкціоновану перевірку Міністерством юстиції (DOJ) будь-якої діяльності, спрямованої на особу США або пов'язаної з урядовими зобов'язаннями, негайне припинення, мінімізацію ризиків та повідомлення у разі, якщо операції виходять за межі дозволу або становлять ризик для критично важливих результатів, а також обов'язковий розгляд та письмове затвердження кожним виконавчим директором кожного пакету операцій перед початком діяльності… Хоча Програма може відкрити новий ринок для послуг у сфері наступальної кібербезпеки та пов'язаних з ними комерційних угод, участь у ній пов'язана зі значними юридичними, операційними та репутаційними ризиками: федеральне дозвіл може пом'якшити, але не усунути ризик притягнення до відповідальності за Законом про комп'ютерні злочини (CFAA) або Законом про прослуховування (Wiretap Act), багато законів штатів про комп'ютерні злочини та захист даних все одно можуть передбачати відповідальність, іноземні юрисдикції часто кваліфікують вторгнення в мережі як кримінальний злочин і застосовують суворі правила щодо конфіденційності, від яких дозвіл США не обов'язково звільняє (як це проілюстровано рішенням Верховного суду Великої Британії від липня 2026 року у справі «Королівство Бахрейн проти Шехабі»), а також виникають ризики, пов'язані з атрибуцією та ескалацією відповідно до міжнародного права, якщо цільова організація CE-TCO виявиться керованою державою або якщо дії підрядника можна приписати Сполученим Штатам, що потенційно наражає компанії на контрзаходи. Тому компанії, які розглядають можливість участі, повинні оцінити ризики, пов'язані з застосуванням іноземного законодавства, прогалини у страховому покритті, ризики, пов'язані із Законом про неправдиві заяви та позбавленням права на участь у державних закупівлях, санкції, експортний контроль, а також зобов'язання щодо конфіденційності та спостереження; отримати вичерпну юридичну консультацію щодо обсягу та можливості забезпечення виконання будь-яких заходів захисту, наданих урядом; домогтися включення надійних положень щодо відшкодування збитків, підтримки у судових спорах та захисту персоналу; наполягати на тому, щоб уряд зберігав відповідальність за вибір цілей та атрибуцію, визначити відповідні правові підстави та встановити детальні правила ведення операцій та умови їхнього припинення; встановити чіткі процедури щодо істотних порушень, повідомлень та оскарження; а також запровадити внутрішні механізми контролю, функціональну роздільність та незалежний юридичний огляд, особливо для операцій, до яких залучені громадяни США або системи, розташовані на території США чи контрольовані США… З огляду на майбутнє, цей меморандум знаменує собою помітний зсув у бік використання можливостей приватного сектору для здійснення санкціонованого урядом спостереження, зриву діяльності або знищення, проте його практичний обсяг залишається невизначеним; усі компанії повинні оцінити, чи мають намір брати участь у цій програмі їхні постачальники послуг з кібербезпеки та реагування

на інциденти, забезпечити, щоб договірні гарантії враховували питання згоди, повідомлення, конфіденційності та подальшого використання даних, а також відповідно оновити посібники з реагування на інциденти, водночас усвідомлюючи, що традиційні захисні заходи — внутрішній контроль, управління вразливостями, планування дій у разі інцидентів, забезпечення безперебійної діяльності та взаємодія з правоохоронними органами — залишатимуться незамінними». ***(David A. Simon, William E. Ridgway, Michael E. Leiter, Brian J. Egan, Joshua Silverstein and Matthew Urfirer. Presidential Memorandum Authorizes Private-Sector Offensive Cyber Operations Against Transnational Criminal Organizations // Skadden Arps Slate Meagher & Flom LLP (https://www.skadden.com/insights/publications/2026/09/presidential-memorandum). 09.09.2026).***

***

«Термін дії Закону про обмін інформацією з питань кібербезпеки 2015 року (CISA) закінчується 11 грудня, що змушує Конгрес вирішити, чи продовжувати його дію, внести до нього зміни чи дозволити цьому надзвичайно важливому законодавчому акту втратити чинність. Цей закон, який спочатку був прийнятий для сприяння добровільному обміну індикаторами кіберзагроз у режимі реального часу між федеральними агентствами та приватним сектором, забезпечує компаніям необхідний правовий захист, убезпечуючи їх від антимонопольної та іншої відповідальності під час моніторингу та обміну даними про загрози. Його реалізація в основному спиралася на Програму автоматизованого обміну індикаторами, яка вимагає видалення інформації, що дозволяє ідентифікувати особу, з метою захисту громадянських свобод — вимога, яка, як підтверджують нещодавні перевірки Генерального інспектора, не порушувалася. Однак у міру еволюції ландшафту загроз закон опинився під тиском, оскільки він прямо не регулює такі нові технології, як операційні технології, периферійні пристрої та штучний інтелект, які дедалі частіше стають мішенями зловмисних суб'єктів…

У міру наближення терміну дії закону Конгрес повинен зважити заклики галузі щодо його довгострокового продовження та необхідність модернізації визначень у законі з метою охоплення нових векторів атак. Законодавці також розглядають питання про перехід від добровільної участі до обов'язкового обміну інформацією для операторів критичної інфраструктури та агрегаторів загроз. Допущення втрати чинності закону позбавить організації життєво важливих правових гарантій, змусивши їх покладатися на альтернативні, потенційно менш надійні механізми обміну розвідданими про загрози. Зрештою, перед Конгресом стоїть нагальне завдання вирішити питання щодо майбутнього цього законодавства, щоб забезпечити його подальше ефективне доповнення існуючих вимог щодо повідомлення про інциденти, таких як Закон про повідомлення про кіберінциденти для критичної інфраструктури 2022 року, не залишаючи кіберзахист країни без правового захисту». ***(Zarrin Ahmed, Joanne Levine. Cybersecurity Information Sharing Provisions Face December Deadline // Legis1 Inc. (https://legis1.com/news/cisa-expiration-2026-expiring-provisions-face). 10.09.2026).***

***

«Керівники служб інформаційної безпеки (CISO) на рівні штатів та місцевих органів влади нещодавно зібралися в Сан-Антоніо, штат Техас, на першому в своєму роді заході, організованому виданням «Government Technology», присвяченому унікальним оперативним викликам, з якими стикаються керівники у сфері кібербезпеки в державному секторі. На тлі глобальних подій — зростання цін на нафту через регіональні конфлікти, кібератаки на критичну інфраструктуру та нові проблеми з регулюванням штучного інтелекту — конференція стала платформою для CISO, де вони могли обговорити ключові пріоритети, зокрема стратегії захисту на основі штучного інтелекту, управління ідентифікацією та запобігання шахрайству. Основною темою обговорення стали передові програми у сфері штучного інтелекту, пропоновані такими організаціями, як OpenAI та Anthropic, які надають гранти та інструменти для зміцнення кіберзахисту урядових структур. Хоча керівники на рівні штатів та місцевих органів влади активно вивчають ці ініціативи разом із постачальниками, багато хто зазначив, що ще зарано оцінювати конкретні результати, оскільки поточні питання щодо контрактів, конфіденційності та використання даних потребують ретельного вирішення…

Управління ідентифікацією та його зв'язок з мережевими архітектурами «Zero Trust» також стали центральною темою, особливо на тлі нещодавніх гучних атак програм-вимагачів та випадків витоку даних водійських посвідчень. Керівники служб інформаційної безпеки (CISO) наголосили, що надійні заходи контролю ідентифікації є необхідними для захисту внутрішніх державних мереж та безпечного надання цифрових послуг мешканцям. Крім того, учасники обговорили розширення ролі керівників служб інформаційної безпеки у боротьбі з шахрайством у державному секторі в рамках різних державних програм. Хоча більшість керівників служб безпеки зазначили, що вони скоріше підтримують, ніж очолюють заходи з запобігання шахрайству у своїх юрисдикціях, інтерес до цієї теми залишається високим, оскільки штати впроваджують нові технології верифікації ідентичності для боротьби з шахрайством у сфері фінансової допомоги, усувають помилки в Програмі додаткової продовольчої допомоги (SNAP) та створюють оперативні групи для протидії кібершахрайству на рівні споживачів та штатів. Загалом учасники визнали цю першу зустріч великим успіхом, що заклала основу для розширеної загальнонаціональної співпраці між керівниками служб безпеки на рівні штатів та місцевих органів влади у найближчі роки». ***(Dan Lohrmann. State and Local Government Cyber Leaders Prioritize AI, Identity and Stopping Fraud // e.Republic LLC (https://www.govtech.com/blogs/lohrmann-on-cybersecurity/state-and-local-government-cyber-leaders-prioritize-ai-identity-and-stopping-fraud). 13.09.2026).***

***

«Державні школи Спрінгфілда в штаті Массачусетс відновили роботу в понеділок після того, як минулого тижня кібератака паралізувала діяльність шкільного округу. Начальниця шкільного округу Соня Дінналл та адміністратори округу відвідали школи в перший день після відновлення роботи, запевнивши

батьків та місцеву громаду, що фізична безпека учнів гарантована, двері залишаються захищеними системою доступу за бейджами, а телефонні лінії та системи екстреного зв'язку працюють у повному обсязі. ІТ-команда округу працювала цілодобово разом із місцевими, штатними та федеральними чиновниками, а також із приватною компанією з кіберкриміналістики, щоб розслідувати інцидент. Попередні висновки підтвердили, що атаку здійснила високоорганізована група кіберзлочинців, яка заблокувала доступ до технологічних сервісів на серверах округу та сторонніх хмарних платформах, що вплинуло на транспорт, доставку їжі, навчальний процес та медичні картки учнів…

Хоча розслідування щодо можливого витоку даних ще триває, на даний момент основна увага округу зосереджена на відновленні доступу до системи та відновленні хмарних платформ. Пріоритет у відновленні системи було надано освітянам та учням віртуальних шкіл, тоді як у традиційних класах тимчасово перейшли на «низькотехнологічні» методи навчання з використанням паперу, підручників та оверхед-проєкторів. Директорка Ліза Баковскі висловила подяку вчителям за їхню здатність пристосовуватися, а керівник шкільного округу Дінналл високо оцінив профспілку вчителів за співпрацю у внесенні оперативних змін. Щоб компенсувати втрачені навчальні дні без подовження навчального року до літа, яке може бути сніжним, шкільний округ планує скоротити десятиденні грудневі канікули. Мер Спрінгфілда Доменік Сарно наголосив, що фінансові ресурси й надалі спрямовуватимуться на потреби учнів, хоча він відмовився підтвердити, чи був цей кіберінцидент пов'язаний з вимогою викупу». ***(Jill Kaufman. Springfield students back in school, cyber attack still under investigation // New England Public Media (https://www.nepm.org/regional-news/2026-09-14/springfield-students-back-in-school-cyber-attack-still-under-investigation). 14.09.2026).***

***

«У 2026 році загрози кібербезпеці різко посилилися як у фізичній, так і в цифровій сферах, що супроводжувалося руйнівними атаками з боку державних суб'єктів, угруповань, що використовують програми-вимагачі, та серйозними випадками витоку внутрішніх даних. Особливе занепокоєння викликає ситуація з Департаментом урядової ефективності (DOGE), де інформатор заявив, що активна копія бази даних Адміністрації соціального забезпечення — яка містить номери соціального страхування та особисті дані більшості живих американців — була завантажена на незахищений сторонній сервер відповідно до угоди з політичною правозахисною групою. Одночасно цивільна інфраструктура стикалася зі зростаючими фізичними та операційними ризиками з-за кордону: російські хакери атакували європейські енергетичні мережі та водоочисні станції, тоді як іранські зловмисники проникли до понад сотні американських підприємств водопостачання на тлі більш широких геополітичних конфліктів…

Корпоративні середовища та технологічні платформи також зазнали масштабних порушень у ланцюгах постачання та операційній діяльності. Компанія Klue, що займається ринковими дослідженнями, виявила хмарні ключі, що належать майже 200 компаніям-клієнтам, зокрема таким великим фірмам у сфері безпеки, як LastPass та Jamf, після того, як зловмисна група Icarus використала

застарілі пілотні облікові дані 2022 року для проникнення в їхні системи. На початку року чат-бот Meta на базі штучного інтелекту був зламаний за допомогою простих методів соціальної інженерії з метою скидання паролів до акаунтів Instagram для неавторизованих користувачів, що призвело до захоплення десятків тисяч акаунтів. Федеральні правоохоронні органи зазнали подібних зломів: китайські шпигуни проникли в несекретну систему спостереження ФБР, що містила номери телефонів, які підлягали прослуховуванню, а Агентство з боротьби з алкоголем, тютюном та вогнепальною зброєю (ATF) оголосило про серйозний інцидент після того, як зловмисники, що використовують програмне забезпечення для вимагання викупу, проникли в систему, де зберігалися дані про об'єкти розслідування. Крім того, проєкти програмного забезпечення з відкритим кодом, у які було вбудовано «задні двері», такі як Trivy, Bitwarden та Checkmarx, дозволили здійснити подальшу крадіжку облікових даних у компаніях OpenAI, Vercel та головному кіберагентстві ЄС, після чого в Австралії було заарештовано двох підозрюваних…

Масові витоки даних значною мірою торкнулися секторів перевірки особи та охорони здоров'я. В результаті злом компанії IDScan, що займається обробкою документів, що посвідчують особу, фотографії та записи 150 мільйонів водіїв зі США та Канади опинилися у пошукових системах даркнету, тоді як злами в системах охорони здоров'я компаній DentaQuest, Aesto Health та CareCloud загалом призвели до витоку медичних записів десятків мільйонів пацієнтів. Великі комерційні та освітні організації також зіткнулися з серйозними перебоями в роботі. Виробник іграшок Hasbro протягом кількох тижнів зазнавав простою систем та затримок із поданням звітності до Комісії з цінних паперів та бірж (SEC) після атаки, що сталася в березні. Компанія Instructure, що спеціалізується на освітніх технологіях, зрештою заплатила викуп угрупованню ShinyHunters після того, як група зламала її платформу Canvas, викрала дані 30 мільйонів студентів та співробітників і зіпсувала портали входу під час підсумкових іспитів. Нарешті, іранські хакери, підтримувані державою, застосували руйнівні тактики проти виробників медичного обладнання: у березні вони дистанційно стерли дані з десятків тисяч пристроїв співробітників компанії Stryker, а в серпні спричинили глобальні операційні та логістичні збої в компанії Boston Scientific, що безпосередньо вплинуло на надання медичної допомоги пацієнтам». ***(Zack Whittaker. Leaks, data breaches, and ransom notes: The worst hacks of 2026 so far // TechCrunch Media LLC. (https://techcrunch.com/2026/09/15/the-worst-hacks-and-breaches-of-2026-so-far/). 15.09.2026).***

***

«Оскільки вимоги до аудиту кібербезпеки, передбачені Каліфорнійським законом про захист персональних даних споживачів (CCPA), переходять від етапу обговорення на рівні регуляторних органів до практичного впровадження, організації опиняються у критичному періоді підготовки до обов'язкових щорічних сертифікацій, початкові терміни яких поступово вводяться у період з 2028 по 2030 рік залежно від річного валового доходу. Оскільки перший аудиторський період триватиме з січня 2027 року по січень 2028

року, решта 2026 року є надзвичайно важливим етапом усунення недоліків та попередньої оцінки. Головним викликом для підприємств є не стільки відсутність надійних засобів контролю кібербезпеки, скільки здатність однозначно довести їхню ефективність та привести існуючі практики у відповідність до 18 конкретних компонентів аудиту, передбачених CCPA… Сфера аудиту є широкою і охоплює не лише платформи, орієнтовані на споживачів, а й внутрішні системи, що обробляють персональні дані співробітників, що вимагає міжфункціональної координації між командами з питань конфіденційності, юридичними та кібербезпеки. Хоча організації можуть використовувати такі усталені рамки, як NIST CSF, CIS Controls, ISO 27001 або SOC 2 для структурування своїх заходів щодо забезпечення відповідності вимогам, рівень зрілості кібербезпеки не означає автоматичної готовності до аудиту. Компанії повинні переконатися, що їхні існуючі оцінки охоплюють відповідні групи систем, ґрунтуються на ретельних тестуваннях, а не лише на співбесідах з керівництвом, та забезпечують наявність актуальних, простежуваних доказів безперервного функціонування засобів контролю протягом усього періоду аудиту… З метою забезпечення операційної ефективності та уникнення зайвого адміністративного навантаження, пов’язаного з дотриманням вимог, підприємствам слід негайно провести аналіз застосовності, зіставити свої поточні системи контролю з вимогами CCPA, скласти вичерпний перелік усіх сховищ даних, що підпадають під дію закону, та стратегічно визначити пріоритетність усунення будь-яких прогалин у доказах або системах контролю до початку офіційного тестування». ***(Taryn Kilkenny Crane, Greg Schu and Andrew Belsick. CCPA Cybersecurity Audit Readiness: How to Prepare Without Starting Over // BDO (https://www.bdo.com/insights/advisory/ccpa-cybersecurity-audit-readiness-how-to-prepare-without-starting-over). 28.09.2026).***

***

Країни ЄС та Великобританія

«Проєкт Закону про кібербезпеку 2.0 (CSA2) Європейської комісії, опублікований 20 січня 2026 року, запроваджує Рамкову концепцію надійного ланцюга постачання інформаційно-комунікаційних технологій (ІКТ), яка надасть Комісії широкі повноваження щодо обмеження використання компонентів інформаційно-комунікаційних технологій від визначених постачальників високого ризику в секторах, що регулюються Директивою NIS2, переносячи акцент з суто технічних вразливостей, які регулюються існуючими інструментами, такими як NIS2, Закону про кіберстійкість та системі сертифікації ЄС, на нетехнічні ризики, що виникають через схильність постачальників до впливу з боку третіх країн, здатних спричинити перебої в наданні послуг, приховувати вразливості або надавати несанкціонований доступ до даних. Ця ініціатива є частиною ширших зусиль ЄС, спрямованих на зменшення стратегічної залежності, як підкреслено у звіті Маріо Драгі про конкурентоспроможність за 2024 рік та відображено у відповідних пропозиціях, таких як Закон про розвиток хмарних технологій та штучного

інтелекту… Ця система діє за п’ятьма послідовними етапами: по-перше, скоординована оцінка ризиків, що проводиться Групою співпраці з питань національної інформаційної безпеки (NIS) на запит Комісії або щонайменше трьох держав-членів, причому на початковому етапі особлива увага приділятиметься мережам 5G, обладнанню для виявлення та підключеним транспортним засобам, а також системам електропостачання та водопостачання, дронам, хмарним сервісам, медичним пристроям, обладнанню для спостереження, космічним послугам та напівпровідникам; по-друге, визначення третіх країн, що становлять серйозні та структурні нетехнічні ризики, після чого суб’єкти господарювання, засновані або контрольовані в цих країнах, автоматично стають постачальниками високого ризику — цей елемент уже оскаржується кількома державами-членами як надмірно геополітичний та такий, що не передбачає індивідуальної оцінки суб’єктів господарювання; по-третє, визначення шляхом прийняття імплементаційного акту ключових активів у сфері ІКТ, чиї основні або чутливі функції, потенціал для серйозних зривів у роботі або витоку даних, а також обмежена база постачальників вимагають захисту; по-четверте, картографування та внесення до переліку постачальників високого ризику на підставі місця реєстрації, власності та контролю; та по-п’яте, запровадження заборон (з урахуванням перехідного періоду) або цільових заходів щодо зменшення ризиків, таких як обов’язки щодо прозорості або технічні запобіжні заходи, стосовно суб’єктів господарювання, що підпадають під регулювання NIS2, причому можливі лише вузькі винятки, якщо постачальник може продемонструвати ефективні заходи щодо зменшення ризиків… Процедура надзвичайних заходів дозволила б Комісії, після консультацій із державами-членами та заслуховування позиції постачальника, безпосередньо вводити заборону у випадках, коли вона має достатні підстави вважати, що компоненти від певного постачальника становлять значну загрозу для економічної або суспільної діяльності щонайменше трьох держав-членів, оминаючи звичайну процедуру — такий механізм викликав критику через нечіткі критерії та недостатню залученість держав-членів. Станом на вересень 2026 року пропозиція залишається на початковому етапі звичайної законодавчої процедури: Рада розглядає її разом із державами-членами, прагнучи отримати більшу ясність щодо методології, управління, пропорційності та визначень, тоді як комітет ITRE Європейського парламенту, доповідачем якого є Маркета Грегорова, як очікується, розпочне роботу у четвертому кварталі 2026 року, що, ймовірно, призведе до міжінституційних переговорів на початку 2027 року… У разі прийняття в нинішньому вигляді ця концепція розширить інструментарій ЄС за межі технічної кібербезпеки, охопивши сфери державних закупівель, управління постачальниками та стратегії ланцюгів постачання. Вона застосовуватиметься не лише до прямих постачальників, а й до продукції, що містить компоненти, отримані через кілька рівнів ланцюга постачання, що, відповідно, вимагатиме від організацій — особливо тих, що працюють у секторах, які вже визначені як такі, що викликають особливе занепокоєння, — забезпечити прозорість складних виробничих ланцюгів нижчих рівнів, де альтернативні постачальники критично важливих компонентів можуть бути рідкісними». ***(Christoph Werkmeister, Elena Brandt, Max Grewe, Vera Ibes, Leonie Wittershagen. Cybersecurity Act 2.0: the EU’s new framework for ICT supply***

chains // Freshfields (https://www.freshfields.com/en/our-thinking/blogs/technology-quotient/cybersecurity-act-2-0-the-eus-new-framework-for-ict-supply-chains-102o06r). 04.09.2026).

***

«Кібератаки на органи державного управління, енергетичні мережі, транспортні вузли та критичну цифрову інфраструктуру набувають все більшого поширення в Європейському Союзі, викриваючи глибокі структурні вразливості в колективній обороні блоку. Кількість інцидентів значно зросла — зокрема, у Польщі з 2024 по 2025 рік спостерігалося зростання на 145 відсотків, у Франції стався масштабний викрадення податкових даних, а в Німеччині кампанії з вимагання, пов'язані з Росією, порушили роботу урядових органів. За даними Агентства Європейського Союзу з кібербезпеки (ENISA), на ідеологічно мотивований хактивізм припадало майже 80 відсотків зареєстрованих інцидентів у період з середини 2024 до середини 2025 року, причому 38 відсотків цілей становила державна адміністрація. Загрозливе середовище дедалі посилюється завдяки штучному інтелекту, який оптимізує розвідку, розробку шкідливого програмного забезпечення та фішинг. Експерти з кібербезпеки зазначають, що поряд із передовими американськими моделями недорогі моделі з відкритим кодом — зокрема китайського походження — можуть бути позбавлені захисних механізмів, що дозволить стрімко збільшити обсяг та швидкість атак у всьому ланцюгу кіберударів…

Незважаючи на десятиліття ініціатив ЄС, спрямованих на перехід від реактивних заходів до проактивної профілактики, оборонна архітектура Європи залишається вкрай роздробленою між національними кордонами та інституціями. Хоча законодавці в Європейському парламенті виступають за створення централізованого європейського центру кібербезпеки, здатного реагувати в режимі реального часу — який потенційно міг би стати попередником європейського кіберкомандування — національні уряди та розвідувальні органи як і раніше неохоче діляться конфіденційними даними про вразливості, інструментами загроз та оперативними можливостями. Як наслідок, такі країни, як Франція, Італія, Велика Британія та Німеччина, здебільшого створюють окремі військові та розвідувальні системи кіберзахисту на національному рівні або розширюють юридичні повноваження для зриву діяльності мереж іноземних супротивників. З огляду на відсутність єдиного політичного консенсусу та транскордонних оперативних механізмів, скоординовані операції з порушення роботи систем, швидше за все, будуть здійснюватися через НАТО або тимчасові коаліції, а не через загальноєвропейську командну структуру…

На організаційному рівні експерти галузі наголошують, що стійкість залежить не стільки від впровадження найсучасніших іноземних інструментів штучного інтелекту, скільки від дотримання суворих базових правил кібергігієни, зокрема виведення з експлуатації застарілої архітектури, сканування програмної інфраструктури та оперативного усунення відомих вразливостей. Хоча Європейська комісія прагне посилити регулювання — зокрема, шляхом запропонованих реформ Закону про кібербезпеку, спрямованих на поступове

витіснення іноземних постачальників з високим рівнем ризику у сфері телекомунікацій, розширення повноважень ENISA та перегляду Директиви про безпеку мереж та інформації 2 (NIS2) з метою усунення розбіжностей у її впровадженні на національному рівні — експерти наголошують, що законодавчі зміни не дадуть бажаного результату, якщо національні регуляторні органи не отримають належних ресурсів для забезпечення дотримання вимог, а приватні організації не візьмуть на себе зобов'язання дотримуватися основних практик безпеки». ***(Paula Soler and Peder Schaefer. Europe is under cyberattack. Is it ready? // Political Holdings Limited (https://www.theparliamentmagazine.eu/news/article/europe-is-under-cyberattack-is-it-ready). 07.09.2026).***

***

«Група з 29 депутатів Європейського парламенту закликає Європейський Союз призупинити процес вступу Сербії до ЄС після того, як стало відомо, що державні органи використовували шпигунське програмне забезпечення проти політичних опонентів та студентських активістів. Посилаючись на висновки фондів SHARE, Amnesty International та The Citizen Lab, які виявили випадки зараження як програмним забезпеченням «Pegasus», так і «NoviSpy», депутати засудили цифрове стеження як підтримувану державою атаку на демократію за режиму президента Александра Вучича. У відповідь депутати Європарламенту вимагають призупинити процес вступу Сербії до ЄС до проведення ретельного розслідування та покращення підзвітності в рамках верховенства права, а також закликають голову Європейської комісії Урсулу фон дер Ляєн скасувати запланований візит до Белграда…

Заклик до введення санкцій посилює загальну дипломатичну напруженість між ЄС та Сербією, що відбувається на тлі нещодавнього скасування візиту комісара ЄС з питань розширення Марти Кос у зв'язку з реакцією сербського уряду на смерть засудженого військового злочинця Ратко Младича. Законодавці зазначили, що дотримання демократичних стандартів має бути обов'язковою умовою вступу до ЄС, використовуючи розкриття інформації про шпигунське програмне забезпечення як додаткове обґрунтування для вжиття заходів проти Белграда. Цей політичний тиск також співпадає зі зростаючим занепокоєнням щодо шпигунського програмного забезпечення на всьому європейському континенті, де нещодавні атаки на членів Європейського парламенту знову посилили вимоги щодо запровадження суворіших регіональних правил у сфері спостереження». ***(Tim Starks. European parliament members call for slowdown of Serbia's EU entry over spyware use // Cyberscoop (https://cyberscoop.com/eu-parliament-serbia-accession-spyware-demands/). 04.09.2026).***

***

«Майбутній британський законопроєкт про кібербезпеку та стійкість (Cyber Security and Resilience Bill) вносить суттєві зміни до архітектури цифрової оборони країни, розширюючи регуляторний контроль та модернізуючи вимоги до критичної інфраструктури та цифрових ланцюгів

постачання. Для організацій, які вже підпадають під регулювання NIS1 як оператори життєво важливих послуг, законодавство встановлює більш суворі терміни повідомлення про інциденти, більші штрафи за недотримання вимог та обов'язковий нагляд за ширшими ризиками ланцюга постачання. На практиці ці суб'єкти повинні модернізувати засоби виявлення, оптимізувати внутрішні процедури ескалації та оновити договори з клієнтами та постачальниками для забезпечення швидкого обміну інформацією. Крім того, законопроєкт розширює сферу регулювання, охоплюючи постачальників керованих послуг (MSP), визначених критично важливих постачальників та міжнародних постачальників, чиї послуги забезпечують функціонування життєво важливих систем Великої Британії. Це вимагає від суб'єктів, що нещодавно потрапили до сфери регулювання, офіційно визначити критичні залежності, створити суворі системи управління та впровадити механізми оперативного повідомлення про інциденти…

Рівень організаційної готовності у Великобританії залишається неоднаковим. Хоча великі транснаціональні підприємства, що дотримуються директиви NIS2 Європейського Союзу, мають перевагу завдяки схожості нормативно-правових вимог, малі та мікропідприємці стикаються зі значними труднощами у дотриманні прискорених термінів подання звітності та впровадженні допоміжних інструментів. Щоб допомогти малим підприємствам, уряд Великобританії та Національний центр кібербезпеки (NCSC) рекомендують організаціям використовувати структуровані рамки, такі як «Рамка кібероцінки» (CAF). Основною операційною проблемою для підприємств є виявлення критичних залежностей у дедалі більш фрагментованих IT-середовищах та багаторівневих ланцюгах постачання, що включають SaaS-платформи, хмарну інфраструктуру та субпідрядників. Щоб подолати відомчу ізольованість та суб'єктивні визначення основних функцій, організації використовують такі методології, як підхід «мінімально життєздатної компанії» (Minimum Viable Company), щоб визначити базові послуги, необхідні для забезпечення безперебійної роботи…

Загалом, законодавство має на меті усунути прогалини в регулюванні шляхом розширення визначеної сфери британської критичної національної інфраструктури (CNI) та централізації повідомлень про інциденти, що сталися, та потенційні інциденти через NCSC, сприяючи підвищенню рівня зрілості в усьому секторі. Водночас підприємства вивчають наслідки для безпеки, пов'язані з впровадженням автономних агентних систем штучного інтелекту. Хоча швидке комерційне впровадження наразі випереджає розробку зрілих захисних механізмів та стандартів управління ідентифікацією та доступом (IAM) для агентів штучного інтелекту, експерти галузі відзначають, що питання кібербезпеки враховуються значно раніше в циклі впровадження штучного інтелекту, ніж це відбувалося під час попередніх технологічних змін, таких як перехід на хмарні технології». ***(Eve Goode. What the Cyber Security and Resilience Bill means for UK firms // Centurian Media Ltd (https://securityjournaluk.com/cyber-security-resilience-bill-wavestone/). 07.09.2026).***

***

«Незважаючи на впровадження численних ініціатив у сфері кібербезпеки та надання додаткового часу на приведення діяльності у відповідність до вимог, Європейський Союз залишається вкрай вразливим до ескалації кібератак на органи державної влади, транспортні вузли, енергетичні мережі та критичну інфраструктуру. Цю тенденцію підтверджують нещодавні інциденти: у Польщі в період з 2024 по 2025 рік кількість кібератак зросла на 145%, у Франції було викрадено конфіденційні дані понад 600 000 платників податків, а Берлін зіткнувся з серйозними адміністративними збоями після того, як група, пов'язана з Росією, взяла в заручники кадрові досьє. Хоча на частку хактивістів з ідеологічними мотивами припадало майже 80% інцидентів, зареєстрованих Агентством Європейського Союзу з кібербезпеки (ENISA) у період з липня 2024 року по червень 2025 року, суб'єкти, пов'язані з державою, та синдикати, що використовують програми-вимагачі, становлять більшу оперативну загрозу, оскільки націлюються на ланцюги постачання, сертифікати програмного забезпечення та транспортну логістику…

Швидка інтеграція штучного інтелекту посилює ці загрози, прискорюючи темпи та розширюючи масштаби ланцюга атак. Окрім гучних американських передових моделей, таких як Mythos 5 від Anthropic, експерти попереджають, що модифіковані китайські моделі з відкритим кодом — які відстають від провідних технологій лише на шість-вісім місяців — дають зловмисникам змогу обходити засоби безпеки та дешево автоматизувати розвідку, фішинг та розробку шкідливого програмного забезпечення. Хоча члени Європейського парламенту запропонували створити централізований європейський центр кібербезпеки для реагування на загрози в режимі реального часу як попередник єдиного європейського кіберкомандування, глибока фрагментація зберігається. Країни-члени ЄС досі вагаються щодо обміну конфіденційною розвідінформацією, інструментами та даними про вразливості через кордони або навіть між внутрішніми відомствами. Як наслідок, такі країни, як Велика Британія, Франція та Італія, створюють незалежні національні агентства з розвідувальним досвідом, тоді як Німеччина рухається в напрямку розширення внутрішніх повноважень для зриву іноземних операцій. З огляду на різний рівень військових можливостей та політичної готовності щодо наступальних кібероперацій, багатодержавні наступальні дії, швидше за все, відбуватимуться в рамках НАТО або менших коаліцій, а не в рамках єдиної структури ЄС…

Водночас європейські законодавчі рамки спрямовані на вирішення питань технологічного суверенітету та усунення структурних вразливостей. На початку 2026 року Європейська комісія запропонувала реформи Закону про кібербезпеку, спрямовані на обмеження використання технологій, що не походять з ЄС, у чутливих секторах, зокрема шляхом поступового виведення з експлуатації обладнання 5G з високим рівнем ризику від таких постачальників, як Huawei. Оновлення Директиви про безпеку мереж та інформації 2 (NIS2) та розширення повноважень ENISA також спрямовані на стандартизацію мінімальних вимог до безпеки та повідомлення про інциденти в ширшому спектрі галузей. Однак експерти наголошують, що регулювання на найвищому рівні є недостатнім без належного фінансування регуляторних органів та суворого контролю за

дотриманням законодавства. Зрештою, аналітики з питань безпеки наголошують, що європейські організації повинні зосередитися на фундаментальних заходах кібергігієни — таких як виведення з експлуатації застарілих систем, усунення відомих вразливостей та зменшення надмірної залежності від іноземних технологій — щоб ефективно протистояти кіберзагрозам, пов'язаним із штучним інтелектом». ***(Paula Soler and Peder Schaefer. Europe is under cyberattack. Is it ready? // Political Holdings Limited (https://www.theparliamentmagazine.eu/news/article/europe-is-under-cyberattack-is-it-ready). 07.09.2026).***

***

«Національне аудиторське управління Великої Британії (NAO) визначило кібератаки як зростаючу загрозу для ланцюга постачання продовольства в країні та закликало Міністерство навколишнього середовища, продовольства та сільських справ (Defra) посилити співпрацю з галуззю та місцевими органами влади. Хоча цей сектор продемонстрував стійкість, його орієнтація на ефективність та низькі витрати також зробила ланцюги постачання більш вразливими до зривів, а фінансовий тиск може обмежувати можливості компаній інвестувати в кібербезпеку… Ці ризики продемонстрували масштабні атаки 2025 року на компанії «Marks & Spencer» та «Co-op»: за оцінками M&S, інцидент обійшовся їй у близько 136 мільйонів фунтів стерлінгів, і вона зазнала перебоїв у роботі після відключення систем управління складами, тоді як «Co-op» повідомила про викрадення даних 6,5 мільйонів своїх членів. NAO попередило, що кіберінциденти можуть порушити роботу життєво важливих цифрових систем, підвищити операційні витрати та потенційно спричинити більш серйозні потрясіння у сфері постачання продовольства. Воно рекомендувало Defra перейняти міжнародний досвід та проводити більше навчань з реагування на надзвичайні ситуації спільно з урядом та представниками галузі… Defra проводить кібернавчання у продовольчій галузі з 2023 року, проте зберігаються побоювання щодо його власного технологічного середовища, зокрема щодо застарілих програмних додатків та тривалої залежності від паперових процесів». ***(Lindsay Clark. UK food supply chain at risk from hostile attacks // Situation Publishing (https://www.theregister.com/security/2026/09/07/uk-food-supply-chain-at-risk-from-hostile-attacks/5294719). 07.09.2026).***

***

«Компанія Jaguar Land Rover (JLR) планує скоротити до 4 000 робочих місць протягом двох років у рамках програми скорочення витрат на суму 1,7 млрд фунтів стерлінгів на тлі тиску з боку китайських конкурентів, що пропонують нижчі ціни, американських мит, дорогого переходу до сегменту преміум-класу та фінансових наслідків масштабної кібератаки 2025 року. Коли у вересні 2025 року хакери здійснили атаку, JLR ще вела переговори щодо кіберстрахування через компанію Lockton і тому не мала чинного страхового поліса. Атака призвела до закриття заводів компанії у Великій Британії на п'ять тижнів і спричинила надзвичайні витрати на суму приблизно 260 млн фунтів стерлінгів, які JLR довелося покрити без страхового відшкодування… Для

порівняння: компанія Marks & Spencer, яка зазнала масштабної атаки, пов'язаної з тією самою хакерською мережею, мала кіберстрахування, яке потенційно покривало до 100 мільйонів фунтів стерлінгів із її оцінених 300 мільйонів фунтів стерлінгів збитків у прибутку. Перебої в роботі JLR також вплинули на її розгалужену мережу постачальників, що спонукало уряд Великої Британії надати гарантію по кредиту на суму 1,5 мільярда фунтів стерлінгів для підтримки підприємств ланцюга поставок та збереження робочих місць. Британський центр кібермоніторингу оцінив загальні економічні збитки у розмірі до 1,9 млрд фунтів стерлінгів, підкресливши значний розрив між прямими корпоративними збитками та більш широкими збитками у ланцюгу поставок… Хоча відсутність страхування сама по собі не може пояснити скорочення робочих місць у JLR, незастраховані збитки створили значний фінансовий тиск у й без того складний період. Цей випадок ілюструє важливість своєчасного продовження договорів кіберстрахування, врахування тимчасового страхового покриття під час переговорів, встановлення лімітів відшкодування збитків від переривання діяльності, що відображають ризики ланцюга поставок, а також забезпечення того, щоб поліси страхування виробничої діяльності враховували потенційно серйозні фізичні та економічні наслідки збоїв в роботі IT-систем у виробничих середовищах, що працюють за принципом «точно в строк». ***(Stephen Owens. Did Jaguar Land Rover's cyber insurance gap help pave the way to 4,000 job losses? // KM Business Information UK Ltd (https://www.insurancebusinessmag.com/uk/news/cyber/did-jaguar-land-rovers-cyber-insurance-gap-help-pave-the-way-to-4000-job-losses-588902.aspx). 07.09.2026).***

***

«За іронією долі, Національне управління з кібербезпеки Румунії (DNSC) — саме та установа, яка покликана захищати країну від кіберзагроз, — було змушене захищати власний офіційний веб-сайт від ймовірної кібератаки. Управління повідомило, що на його веб-сайті dnsc.ro виникли тимчасові проблеми з доступом через надзвичайно великий обсяг одночасних запитів із різних джерел. Технічний аналіз свідчить, що цей сплеск трафіку, ймовірно, був спричинений атакою типу «розподілена відмова в обслуговуванні» (DDoS) — це тип інциденту, спрямований на перевантаження інфраструктури сервісу та порушення його доступності, а не на проникнення в системи чи викрадення даних. У відповідь DNSC негайно вжило додаткових заходів захисту та оптимізації, що дозволило успішно стабілізувати роботу платформи… Хоча агентство й надалі ретельно відстежує стан своєї інфраструктури та динаміку трафіку з метою запобігання подальшим перебоям, воно ще не класифікувало цей інцидент як підтверджену кібератаку, зазначивши, що, виходячи з наявних технічних даних, така можливість залишається. DNSC заявило, що надаватиме подальшу інформацію, якщо ситуація вимагатиме додаткових повідомлень». ***(Romania's Cyber Defense Agency Hit by Possible DDoS Attack // The Romania Journal (https://www.romaniajournal.ro/business/romanias-cyber-defense-agency-hit-by-possible-ddos-attack/). 09.09.2026).***

***

«Кібератака, що сталася у вересні 2025 року на постачальника спільних технологій і призвела до зриву роботи європейських авіакомпаній, підкреслює фундаментальну зміну в характері кіберризиків: це вже не лише технічна проблема, а системний, стратегічний та управлінський виклик, який може швидко поширитися по ланцюгах постачання. Про це свідчать останні галузеві звіти, в яких зазначається зростання кількості кібератак на 18%, а найбільш значущими загрозами визнано вразливості, пов'язані зі штучним інтелектом, та слабкі місця в ланцюгах постачання, пов'язані зі сторонніми постачальниками… Отже, управління цими ризиками вимагає міжфункціонального підходу на рівні ради директорів, за якого питання кібербезпеки виноситься на стратегічний рівень. Рада директорів повинна активно контролювати ризики, визначати рівень прийнятного ризику для організації та створювати спеціалізовані комітети, тоді як керівництво — на чолі з генеральним директором та за підтримки керівника служби інформаційної безпеки — перетворює ці вказівки на практичні ресурси та інтегрує заходи безпеки в повсякденну діяльність. Для забезпечення ефективного нагляду рада директорів повинна отримувати чіткі звіти, які перетворюють технічні показники на конкретні наслідки для бізнесу… Крім того, оскільки надійні внутрішні механізми контролю виявляються недостатніми у разі порушення безпеки зовнішніх постачальників, ради директорів повинні виявляти критичні залежності від третіх сторін та запроваджувати пропорційні заходи безпеки по всьому ланцюгу постачання. Таке суворе управління має поширюватися також на штучний інтелект; хоча ШІ надає значні операційні переваги, він збільшує ризики, що вимагає впровадження надійних політик для моніторингу автоматизованих рішень, захисту даних та забезпечення того, щоб автономні агенти діяли в межах стратегічних та ризикових параметрів компанії… Зрештою, оскільки кіберінциденти є неминучими, організації повинні розвивати стійкість як основну конкурентну перевагу, надаючи пріоритет плануванню дій у надзвичайних ситуаціях та беручи участь у навчальних тренуваннях з моделювання кризових ситуацій. Вважаючи кібербезпеку одним із фундаментальних пріоритетів корпоративного управління, ради директорів можуть захищати критично важливі активи, підтримувати довіру зацікавлених сторін та формувати проактивну стійкість, необхідну для орієнтування у дедалі більш взаємопов'язаній цифровій екосистемі». ***(Susana Sierra. Five Key Recommendations For Boards To Lead On Cybersecurity // Forbes Media LLC. (https://www.forbes.com/councils/forbesbusinesscouncil/2026/09/10/five-key-recommendations-for-boards-to-lead-on-cybersecurity/). 10.09.2026).***

***

«Німеччина суттєво посилює свою готовність у сфері кібербезпеки, оскільки виробники прискорюють процес приведення своєї діяльності у відповідність до Закону Європейського Союзу про кіберстійкість (CRA), який встановлює суворі вимоги до безпеки апаратних і програмних продуктів протягом усього їхнього життєвого циклу. З огляду на розширення площі атаки, пов'язаної з взаємопов'язаними промисловими системами та пристроями Інтернету

речей (IoT), CRA запроваджує підхід «безпека за задумом», що вимагає від виробників інтегрувати оцінку ризиків та заходи безпеки на етапі початкової розробки продукту, а не додавати їх згодом… Ця зміна в нормативно-правовій базі спонукає німецьких виробників суттєво збільшити обсяги IT-ресурсів, що виділяються на управління вразливостями та безпечну розробку продукції. Щоб відповідати цим новим стандартам, компанії повинні докорінно переглянути свої робочі процеси розробки програмного забезпечення, включивши до них безпечне кодування, аналіз залежностей та ретельний контроль за компонентами сторонніх розробників. Крім того, CRA запроваджує суворі вимоги щодо повідомлення про інциденти, згідно з якими виробники зобов'язані повідомляти органи влади протягом 24 годин після виявлення вразливості, що активно експлуатується, а потім, починаючи з вересня 2026 року, надавати детальний звіт протягом 72 годин… Для величезної промислової та виробничої бази Німеччини це законодавство перетворює кібербезпеку з суто IT-функції на фундаментальну інженерну вимогу. Відповідно, виробники стикаються з глибокими організаційними змінами, що вимагають посилення управління безпекою, збільшення чисельності персоналу та безперебійної співпраці між IT-командами, інженерними підрозділами та командами з питань дотримання нормативних вимог, щоб забезпечити стійкість їхніх підключених до мережі продуктів до складних кіберзагроз на основі штучного інтелекту в рамках європейського цифрового ланцюга поставок». ***(Naveen Goud. Germany bolsters Cybersecurity Workforce to prepare for EU Cyber Resilience Act // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/germany-bolsters-cybersecurity-workforce-to-prepare-for-eu-cyber-resilience-act/). 09.09.2026).***

***

«Асоціація британських страховиків (ABI) опублікувала нові рекомендації з кібербезпеки, щоб допомогти організаціям Великої Британії підготуватися до кіберінцидентів та мінімізувати потенційні збитки. Хоча підтримувана урядом програма «Cyber Essentials» слугує базовим орієнтиром, ABI наголошує, що еволюція загроз вимагає додаткових заходів безпеки, пропорційних рівню ризику. Серед ключових рекомендацій — надійне управління ідентифікацією та доступом, зокрема впровадження стійкої до фішингу багатофакторної аутентифікації (MFA) для привілейованих облікових записів та критично важливих кінцевих точок… Інші важливі заходи контролю передбачають впровадження сучасних систем виявлення та реагування на загрози на кінцевих точках, регулярне управління вразливостями з оперативним встановленням виправлень, а також проведення періодичних тренінгів для співробітників з метою протидії фішингу та соціальній інженерії, підсиленим штучним інтелектом. Для зменшення ризиків, пов'язаних із програмним забезпеченням-вимагачем, у рекомендаціях наголошується на необхідності створення регулярно перевірених, незмінних або офлайн-резервних копій, а не покладатися виключно на хмарну синхронізацію… Крім того, організаціям настійно рекомендується підтримувати та перевіряти плани реагування на інциденти та забезпечення безперебійної діяльності, зберігати системні журнали щонайменше протягом шести місяців для сприяння виявленню

порушень із затримкою, шифрувати дані як під час зберігання, так і під час передачі, а також управляти ризиками ланцюга постачання шляхом суворої оцінки постачальників та контролю доступу. Зрештою, ці рекомендації покликані допомогти організаціям всебічно оцінити стан своєї кібербезпеки та сприяти проведенню більш обґрунтованих обговорень із страховими брокерами та страховиками щодо відповідного страхового покриття та доступних послуг у сфері безпеки». ***(Yana Keller. Association of British Insurers sets out cyber security controls for UK businesses // B2B Insurance & InsurTech (https://beinsure.com/news/cyber-security-controls-for-uk-businesses/). 10.09.2026).***

***

«Організації, що продають цифрові продукти в Європейському Союзі, мають дотриматися критичного терміну щодо дотримання вимог 11 вересня 2026 року, коли набере чинності обов'язкове повідомлення про інциденти та вразливості відповідно до Закону ЄС про кіберстійкість (CRA). Закон CRA, розроблений з метою перенесення відповідальності за кібербезпеку з споживачів на виробників протягом усього життєвого циклу продукту, вимагає від виробників, включаючи виробників оригінального обладнання (OEM) та розповсюджувачів програмного забезпечення з відкритим кодом, повідомляти про активно експлуатовані вразливості та серйозні інциденти безпеки до Агентства ЄС з кібербезпеки (ENISA) та своїх національних команд реагування на інциденти кібербезпеки (CSIRT)… Суворі терміни подання звітності передбачають подання попереднього попередження протягом 24 годин після виявлення, детального оновлення — протягом 72 годин, а також вичерпного остаточного звіту — протягом 14 днів у разі вразливостей або протягом місяця у разі серйозних інцидентів. Важливо, що ці зобов'язання застосовуються ретроактивно до всіх продуктів із цифровими елементами, випущених на ринок до набрання законом повної чинності 11 грудня 2027 року, тобто навіть застарілі продукти підлягають моніторингу, а за невиконання вимог передбачені штрафи у розмірі до 15 млн євро або 2,5% від глобального річного обороту… Хоча CRA доповнює більш широкі нормативні рамки, такі як Директива NIS2 — яка зосереджується на забезпеченні безпеки організацій та критичної інфраструктури, а не окремих продуктів — багато організацій залишаються непідготовленими, причому значна частина з них навіть не впевнена, чи поширюється на них дія цього регулювання. Щоб відповідати цим суворим вимогам, керівники служб інформаційної безпеки (CISO) повинні терміново оцінити сферу застосування своїх продуктів, визначити юридичні обов'язки у складних ланцюгах постачання, посилити процеси управління вразливостями та розробити машиночитані специфікації програмного забезпечення (SBOM) задовго до набрання чинності вимогами у 2027 році… Крім того, керівники повинні ретельно перевіряти свої плани реагування на інциденти за допомогою теоретичних навчань та інтегрувати внутрішні робочі процеси з майбутньою платформою звітності ENISA. Зрештою, хоча на даний момент основна увага приділяється кінцевому терміну подання звітності у вересні 2026 року, справжнє завдання для організацій полягає у створенні внутрішніх можливостей для швидкого виявлення, оцінки та ескалації вразливостей, щоб

встигнути дотриматися цих жорстких термінів». ***(Samira Sarraf. EU Cyber Resilience Act reporting: What CISOs need to know // TechTarget, Inc. (https://www.techtarget.com/cybersecurity/feature/EU-Cyber-Resilience-Act-reporting-What-CISOs-need-to-know). 09.09.2026).***

***

«Напередодні парламентських виборів у Швеції влада висловила занепокоєння щодо можливих спроб іноземних держав вплинути на результати голосування. Однак після виборів Шведське агентство психологічної оборони дійшло висновку, що Швеція не зазнала жодного масштабного та скоординованого іноземного інформаційного впливу. Карін Леннхеден, операційний директор агентства, підтвердила, що під час голосування не було зафіксовано жодних значних скоординованих дій з боку суб'єктів загрози, що перебували під наглядом. Крім того, Національний центр кібербезпеки не зафіксував жодних кіберінцидентів, які б вплинули на хід або результати виборів, підтвердивши, що голосування відбулося без значних кібератак чи іноземного втручання». ***(Sweden saw no major cyberattacks or foreign influence campaigns during election, agency says // Sweden Herald (https://swedenherald.com/article/sweden-saw-no-major-cyberattacks-or-foreign-influence-campaigns-during-election-agency-says). 14.09.2026).***

***

«Згідно з даними Управління комісара з питань інформації, на які посилається компанія Karis Insurance, у 2025 році кількість кібератак, спрямованих проти британських компаній, що надають послуги у сфері нерухомості, зросла на 17%, а кількість зареєстрованих інцидентів збільшилася до 208 порівняно з 178 у попередньому році. Агенти з нерухомості, оцінювачі та менеджери, що займаються орендою нерухомості, стали головними мішенями для кіберзлочинців, оскільки суворі вимоги щодо протидії відмиванню грошей та дотримання принципу «знай свого клієнта» зобов'язують їх збирати та зберігати великий обсяг персональних даних — зокрема, паспортні дані, водійські посвідчення, банківські реквізити та відомості про іпотечні кредити…

Ця вразливість посилюється загальними тенденціями у сфері безпеки по всій країні. Урядове дослідження «Cyber Security Breaches Survey 2025/2026» показало, що 43% британських підприємств зазнали зломів протягом дванадцяти місяців, причому фішинг став найпоширенішим і найшкідливішим методом атак. Злом доступу до справ щодо нерухомості часто уможливлює шахрайство з передачею права власності та перенаправленням платежів, коли злочинці маніпулюють ланцюжками електронних листів, щоб підмінити банківські реквізити законних адвокатів або продавців своїми власними… Асоціація юристів та Національне агентство з боротьби зі злочинністю закликали покупців перевіряти реквізити рахунків безпосередньо у юридичних радників та здійснювати невеликі тестові транзакції перед переказом коштів…

Незважаючи на ці значні операційні та фінансові загрози, компанії, що працюють у сфері нерухомості та посередницькі фірми, як і раніше, недостатньо

застраховані та захищені. За результатами загальнонаціонального опитування, хоча 47% британських підприємств мають ту чи іншу форму кіберстрахування, лише 10% з них уклали окремі страхові поліси, причому багато компаній посилаються на недостатню поінформованість або бюджетні пріоритети. Крім того, базові технічні засоби контролю залишаються недостатньо використовуваними в економіці в цілому: рівень впровадження двофакторної аутентифікації становить лише 47%, а сертифікації Cyber Essentials — 5%. У відповідь на це лідери галузі, такі як Mortgage Brain, закликають брокерів зробити безпеку даних обов'язковою умовою, запровадивши багатофакторну аутентифікацію, заборонивши передачу конфіденційних документів через незашифровану електронну пошту, уникнувши повторного використання облікових даних та заборонивши введення записів про клієнтів у загальнодоступні споживчі інструменти штучного інтелекту». ***(Jonalyn Cueto. Property cyber attacks climb as broker data piles up // KM Business Information UK Ltd (https://www.mpamag.com/uk/news/general/property-cyber-attacks-climb-as-broker-data-piles-up/589768). 15.09.2026).***

***

«Транспонування Португалією Директиви NIS 2 набуло чинності згідно з Декретом-законом № 125/2025 від 4 грудня, який згодом був доповнений Постановою про його впровадження № 756/2026 від 22 червня, що запровадило новий перелік зобов'язань у сфері кібербезпеки, найнагальнішою практичною вимогою яких є реєстрація суб'єктів, що підпадають під дію Директиви, у Національному центрі кібербезпеки Португалії (CNCS) через портал MyCiber до 15 вересня 2026 року… Суб'єкти підпадають під сферу застосування, якщо вони входять до складу системи державного управління або здійснюють діяльність в одному з секторів, перелічених у додатках I або II до Декрету-закону, до яких належать: питна вода, стічні води, банківська справа, енергетика, космічна галузь, поводження з відходами, управління ІКТ-послугами (B2B), виробництво, цифрові інфраструктури, інфраструктури фінансових ринків, наукові дослідження, цифрові провайдери, хімічна промисловість, виробництво харчових продуктів, охорона здоров'я, поштові та кур'єрські послуги, а також транспорт; проте оцінка відповідності критеріям рідко буває простою, оскільки вона також залежить від критеріїв щодо обмежень за розміром, конкретних винятків та, у деяких випадках, складних міркувань щодо групової структури відповідно до Рекомендації Комісії 2003/361/ЄС… CNCS надав у розпорядження онлайн-інструмент, який видає орієнтовний результат; однак цей результат залежить від точності наданої інформації, не є обов'язковим для Центру та не звільняє суб'єкта господарювання від обов'язкової реєстрації. Реєстрацію можуть здійснювати лише законні представники (які повинні мати сертифікат Системи сертифікації професійних атрибутів або надати документальне підтвердження своїх повноважень) або спеціально уповноважені особи (які повинні пред'явити довіреність); оскільки MyCiber наразі вимагає португальських цифрових посвідчень, таких як цифровий мобільний ключ або картка громадянина, організації, у яких немає особи з відповідним місцевим посвідченням, повинні подбати про це заздалегідь. Окрім загальної ідентифікації та підтвердження повноважень представника, суб'єкти

повинні самостійно визначити свій статус як публічний або приватний, оцінити територіальну сферу дії та будь-які застосовні винятки, вказати, чи можуть їхні послуги суттєво вплинути на критично важливі державні, суспільні або економічні види діяльності, а також, у разі необхідності, застосувати правила агрегування даних групи до порогових значень розміру. Після подання документів CNCS видає проєкт рішення про кваліфікацію, щодо якого суб'єкт господарювання має десять робочих днів для подання зауважень; після цього Центр має до тридцяти робочих днів для прийняття остаточного рішення, в якому зазначаються класифікація, призначений рівень відповідності та відповідні мінімальні заходи з кібербезпеки… Протягом двадцяти робочих днів після прийняття цього рішення організація повинна призначити менеджера з кібербезпеки та постійну контактну особу (не більше двох осіб), які разом із первинним реєстрантом отримають доступ до MyCiber і надалі виконуватимуть усі зобов'язання на платформі, такі як повідомлення про інциденти, надання переліку активів та щорічна звітність. Перші взаємодії виявили практичні питання щодо тлумачення положень на місцях, очікуваної інформації та застосування до складних структур, проте CNCS продемонструвала готовність до діалогу, і як сама платформа, так і розділ «Часті запитання» вже зазнали численних оновлень, що свідчить про прагматичний та оперативний підхід… З наближенням кінцевого терміну організації, які ще не завершили оцінку застосовності, повинні розглядати це як найпершочергове завдання, тоді як ті, що вже визначені як такі, що підпадають під дію вимог, повинні забезпечити, щоб подана інформація точно відображала структуру групи, її діяльність та механізми управління; у міру опрацювання реєстрацій та розвитку наглядової діяльності очікується, що з'явиться більша ясність щодо регуляторних очікувань та пріоритетів у сфері забезпечення дотримання вимог». ***(Inês de Sá, Lucas Battistello Espindola and Ana Rita Paínho. Portugal's NIS 2 Transposition: Registration deadline approaches // Bird & Bird (https://www.twobirds.com/en/insights/2026/portugal's-nis-2-transposition-registration-deadline-approaches). 15.09.2026).***

***

«23 вересня 2026 року Рада з фінансової звітності Великої Британії (FRC) опублікувала документ «Розвінчання міфів щодо Положення 29: акцент на кібербезпеці», щоб надати компаніям рекомендації щодо звітності з питань кібербезпеки відповідно до Положення 29 Кодексу корпоративного управління Великої Британії 2024 року. Відповідаючи на занепокоєння представників галузі щодо розкриття комерційно або операційно чутливої інформації, у цьому документі роз'яснюється, що, хоча ради директорів повинні пояснювати, як вони контролюють та перевіряють ефективність суттєвих заходів кіберзахисту, вони не зобов'язані розкривати конкретні технічні конфігурації або деталі вразливостей, які самі по собі можуть становити ризики для безпеки… У цьому керівництві виокремлено п'ять основних висновків: по-перше, декларація згідно з Положенням 29 не є гарантією від кіберінцидентів, а скоріше поясненням процесу забезпечення надійності, що здійснюється радою директорів у динамічному середовищі загроз; по-друге, детальну конфіденційну технічну інформацію не обов'язково

повідомляти; по-третє, заходи кіберзахисту мають бути інтегровані в ширшу систему внутрішнього контролю; по-четверте, кіберінцидент не призводить до автоматичного визнання недійсним попередньої декларації про ефективність, за умови що заходи контролю були ефективними на дату складання балансу, хоча систематичні збої вимагають ретельного аналізу; і по-п'яте, ради директорів повинні забезпечити, щоб їхній нагляд розвивався відповідно до змін у сфері кіберризиків… Зрештою, хоча «Розвінчання міфів» розвіює побоювання щодо гарантування абсолютної безпеки або розкриття вразливих технічних деталей, він не знижує загальних вимог до відповідності. Компанії, що застосовують суттєві заходи кіберзахисту, повинні забезпечити, щоб їхні ради директорів мали надійну основу для оцінки ефективності цих заходів. Це передбачає активне відстеження профілів кіберризиків, отримання своєчасної та якісної інформації, а також усунення будь-яких слабких місць, виявлених у результаті інцидентів або тестувань на проникнення, перш ніж робити позитивну заяву». ***(Francesca Blythe, Mattie Lefevre. UK FRC Publishes Cybersecurity "Mythbuster" on Provision 29 // Sidley Austin LLP (https://datamatters.sidley.com/2026/09/29/uk-frc-publishes-cybersecurity-mythbuster-on-provision-29/). 29.09.2026).***

***

«У нещодавньому звіті організації «Energy Storage Europe» (ESE) міститься застереження, що прогалини в законодавстві та непослідовне впровадження систем кібербезпеки в державах-членах ЄС призводять до зростання витрат, уповільнюють розгортання акумуляторних систем зберігання енергії (BESS) та не дозволяють усунути системні ризики на рівні енергомережі. Підтримуючи загальний напрям Закону про кіберстійкість (CRA), Мережевого кодексу з кібербезпеки (NCCS) та запропонованого Закону про кібербезпеку (CSA) 2.0, галузева організація наголошує на практичних викликах, зокрема на розбіжностях у впровадженні Директиви NIS2 та прогалинах у відповідальності щодо застарілих активів, аутсорсованих операцій та виробників, що не входять до ЄС… Щоб пом'якшити ці проблеми в міру нарощування потужності систем акумулювання енергії (BESS) до прогнозованих 200 ГВт до 2030 року, ESE пропонує чотири ключові заходи: перекласифікацію критично важливих експлуатаційних компонентів, таких як системи управління акумуляторними батареями, системою живлення та енергією (BMS, PCS, EMS), відповідно до CRA для проведення оцінки відповідності незалежними організаціями; гармонізацію вимог до підключення систем BESS на всьому Єдиному ринку; опублікування спільних рекомендацій щодо впровадження NIS2 та NCCS з метою зменшення дублювання аудитів; а також якнайшвидше надання чітких роз'яснень щодо обсягів та термінів застосування CSA 2.0 у ланцюгу постачання… Що стосується саме CSA 2.0, ESE закликає до оперативно точного визначення поняття «нетехнічного ризику», що ґрунтується на юрисдикції та формі власності, а не лише на місцезнаходженні постачальника; до врахування технічних заходів щодо зменшення ризиків; до гармонізованого застосування у всіх державах із посиленою роллю ENISA; до встановлення перехідних періодів тривалістю щонайменше один рік, виходячи з ризиків, щоб врахувати тривалі цикли

експлуатації систем акумулювання енергії (BESS); а також до встановлення CSA 2.0 як єдиного узгодженого еталонного інструменту для кібербезпеки ланцюгів постачання, узгодженого з CRA та NIS2… Зрештою, ESE виступає за регуляторний підхід на рівні компонентів, заснований на оцінці ризиків, який зосереджує ресурси на системах, що безпосередньо контролюють взаємодію з енергомережею, та водночас забезпечує гармонізацію правил у державах-членах з метою досягнення балансу між надійною безпекою та транскордонними інвестиціями й впровадженням стандартизованих технологій BESS». ***(April Bonner. Urgent need for cybersecurity overhaul as BESS deployment accelerates, Energy Storage Europe says // Informa PLC (https://www.energy-storage.news/urgent-need-for-cybersecurity-overhaul-as-bess-deployment-accelerates-energy-storage-europe-says/). 28.09.2026).***

***

«Данська компанія з кібербезпеки Sovera Security отримала фінансування в розмірі 535 000 євро від Данського фонду експорту та інвестицій (EIFO) для прискорення свого зростання на ринках країн Північної Європи та в інших регіонах Європи. Ця інвестиція з'явилася в той час, коли зростання геополітичної напруженості, зміни в законодавстві та стрімке впровадження штучного інтелекту змушують європейські організації надавати пріоритет цифровій стійкості, контролю над ланцюгами постачання та суверенітету даних, а не покладатися на неєвропейських постачальників технологій. Заснована колишнім засновником LogPoint Сереном Лауструпом, компанія Sovera Security вирішує ці проблеми, пропонуючи платформу кібербезпеки на базі штучного інтелекту, яка працює з власного центру обробки даних, забезпечуючи суверенітет даних та операційну незалежність, водночас залишаючи критичні рішення щодо безпеки під контролем людини… Компанія орієнтується саме на операторів критичної інфраструктури та середні й великі підприємства, яким необхідні надійне дотримання нормативних вимог, безпечна обробка даних та ефективне управління. Отримане фінансування буде використано для подальшого розвитку можливостей Sovera у сфері штучного інтелекту та її інфраструктури, розширення команди та посилення присутності на ринку, що підкріплює впевненість EIFO у стратегічній важливості та міжнародному конкурентному потенціалі данських технологій у сфері кібербезпеки в умовах, що постійно змінюються». ***(Cate Lawrence. Sovera Security secures €535K from EIFO to build sovereign AI cybersecurity // Webrazzi (https://tech.eu/2026/09/29/sovera-security-secures-eur535k-from-eifo-to-build-sovereign-ai-cybersecurity/). 29.09.2026).***

***

«Ірландська консалтингова компанія з питань кібербезпеки та захисту даних BH Consulting запустила BH Haven — нову багаторівневу послугу, покликану допомогти малим та середнім підприємствам (МСП) орієнтуватися у складних нормативно-правових рамках, таких як GDPR, NIS2, Закон ЄС про штучний інтелект та Закон про кіберстійкість. Усуваючи критичний пробіл у кіберстійкості МСП, ця послуга забезпечує пропорційне управління та гарантії, адаптовані до потреб організацій, яким часто бракує спеціалізованих знань у сфері

безпеки або часу. BH Haven використовує власний інструмент на основі штучного інтелекту для оптимізації аналізу доказів, картирування нормативних вимог та підготовки проєктів звітності, що значно зменшує адміністративне навантаження на команду консультантів… Однак компанія наголошує на суворому підході, що передбачає участь людини у процесі; спеціалізовані консультанти зберігають повний контроль, приймають усі рішення щодо ризиків та затверджують кінцеві результати, гарантуючи, що штучний інтелект не приймає самостійних рішень щодо прийняття ризиків або ефективності заходів контролю. На відміну від постачальників керованих послуг безпеки, які керують брандмауерами або центрами управління безпекою, BH Haven діє виключно як незалежний консультант, що спеціалізується на дотриманні нормативних вимог, гарантуванні ризиків та незалежній оцінці існуючих заходів контролю… Очікується, що ця ініціатива, яка спочатку орієнтована на ринки Ірландії та Великої Британії, а згодом поширеться на країни ЄС та Скандинавії, дозволить створити до 50 спеціалізованих робочих місць протягом наступних трьох років, при цьому будуть збережені стандартні механізми професійної відповідальності, за якими кінцева відповідальність за виконання рекомендацій та управління середовищем безпеки залишається за клієнтом». ***(Mirko Zorz. In this new SME cybersecurity service, the AI assists and the consultants decide // Help Net Security (https://www.helpnetsecurity.com/2026/09/30/bh-haven-sme-cybersecurity-service/). 30.09.2026).***

***

«Після того, як на початку цього року історична компанія Moores Furniture Group, що базується в Йоркширі, була передана під зовнішнє управління через тривалі фінансові збитки, вона стала жертвою кібератаки, в результаті якої були викрадені особисті дані її колишніх співробітників. Спільні адміністратори з компанії Interpath Advisory виявили несанкціонований доступ до IT-систем компанії 9 серпня та негайно залучили фахівців з кібербезпеки для розслідування масштабів порушення… Про цей інцидент було повідомлено правоохоронним органам та Управлінню комісара з питань інформації (ICO), хоча ICO згодом закрило справу, тоді як внутрішнє розслідування адміністраторів триває. Цей витік даних додає нових складнощів для 77-річної компанії, яка була заснована в 1947 році та в січні була передана під зовнішнє управління через заборгованість перед кредиторами у розмірі понад 30 мільйонів фунтів стерлінгів — незадовго до того, як компанія Wren Kitchens придбала її список клієнтів та активи інтелектуальної власності в рамках угоди «pre-pack». Адміністратори заявили, що ставляться до цієї справи з максимальною серйозністю та зобов'язуються інформувати колишніх співробітників, яких це стосується, про хід розслідування». ***(George Dean. Former Moores staff victims of severe cyber-attack // Taylist Media (https://www.kbbreview.com/87676/news/former-moores-staff-victims-of-severe-cyber-attack/). 28.09.2026).***

***

«У нещодавньому звіті Європейського рахункового суду (ECA) зазначається, що ЄС стикається з труднощами в ефективному виявленні та реагуванні на серйозні інциденти у сфері кібербезпеки. Цей недолік особливо проявився під час атаки програм-вимагачів на компанію «Collins Aerospace» минулого року, яка призвела до зриву роботи аеропортів у Брюсселі, Берліні та Дубліні, при цьому між державами-членами не було надіслано жодних офіційних попереджень. Незважаючи на фінансування кібербезпеки з боку ЄС у розмірі 1,4 млрд євро, аудитори дійшли висновку, що система є лише частково ефективною через недостатній обмін інформацією та дублювання повноважень між різними органами, такими як Центр кібербезпеки Європейської комісії та ENISA… Ця фрагментація посилюється через затримки у впровадженні на національному рівні Директиви NIS 2 — лише дві держави-члени дотрималися терміну 2024 року — що означає, що організації часто не мають юридичного обов'язку повідомляти про інциденти, що призводить до значного недооцінювання їхньої кількості; у 2025 році сім держав офіційно повідомили лише про 14 значних транскордонних інцидентів, тоді як ENISA зафіксувала 322 таких випадки. Серед інших вразливих місць — центри раннього попередження ЄС, які залишаються «операційно призупиненими» через затримки із закупівлею засобів виявлення, а також недостатня перевірка субреципієнтів грантів на кібербезпеку, що створює ризик розкриття конфіденційної інфраструктури суб'єктам, які не входять до ЄС… З метою усунення цих критичних прогалин Європейський рахунковий суд (ECA) видав п'ять рекомендацій із термінами виконання до 2028 року, тоді як Європейська комісія зобов'язалася їх розглянути та вказала на запропоновану нею редакцію Закону про кібербезпеку (CSA2) як засіб посилення можливостей ENISA та обмеження технологій високого ризику». ***(Jennifer Baker. EU cybersecurity falters as member states keep attacks to themselves // EU Perspectives (https://euperspectives.eu/2026/09/eu-cybersecurity-falters-as-member-states-keep-attacks-to-themselves/). 23.09.2026).***

***

«У відповідь на постійно мінливі кіберзагрози Міністерство оборони Великої Британії (MoD) надає пріоритет безпеці ланцюга поставок, запроваджуючи систему «Defence Cyber Certification» (DCC) — комплексну систему забезпечення кібербезпеки, розроблену у партнерстві з IASME. Визнаючи, що вразливості у менших постачальників нижчого рівня можуть поставити під загрозу цілі оборонні програми, MoD зміщує свій стратегічний фокус з забезпечення безпеки лише головних підрядників на забезпечення стійкості всієї екосистеми ланцюга поставок. Відповідно до Моделі кібербезпеки версії 4 (CSMv4) Міністерства оборони, DCC забезпечує незалежну, стандартизовану оцінку кіберстійкості організації, пропонуючи багаторазове підтвердження, яке замінює необхідність проведення індивідуальних оцінок для кожної можливості закупівлі… Ця система передбачає чотири рівні сертифікації, що базуються на оцінці ризиків, причому для всіх рівнів є обов'язковою базова сертифікація «Cyber Essentials», а для рівнів 2 і 3 — більш сувора сертифікація «Cyber Essentials Plus»; сертифікати дійсні протягом трьох років і підлягають щорічному підтвердженню. Міністерство

оборони встановило суворий термін для всіх партнерів з галузі — до 31 грудня 2026 року вони повинні отримати сертифікат рівня 0 — та зазначило, що наявність дійсного сертифіката дедалі частіше ставатиме обов'язковою умовою для державних закупівель у сфері оборони та виконання контрактів… Ці вимоги виходять далеко за межі безпосередніх головних підрядників і поширюються вниз по ланцюгу поставок на виробників комплектуючих, розробників програмного забезпечення та спеціалізованих постачальників послуг. Щоб зберегти конкурентоспроможність та дотримуватися вимог, організації повинні терміново проаналізувати своє місце в ланцюгу поставок оборонної галузі, оцінити поточний стан безпеки, визначити необхідні заходи з посилення контролю та забезпечити чітке розподілення зобов'язань щодо кібербезпеки в усіх контрактах із клієнтами та постачальниками». ***(Paul Armstrong and Della Heptinstall. Defence Cyber Certification: Is your business ready? // Walker Morris LLP (https://www.walkermorris.co.uk/comment-opinion/defence-cyber-certification-is-your-business-ready/). 24.09.2026).***

***

Австралія та Нова Зеландія

«Малі та середні підприємства Нової Зеландії повідомляють про зростання ризику кібератак: згідно з даними моніторингу Національного центру кібербезпеки (NCSC) за 2026 рік, 43% з них зараз вважають себе вразливими, що на 9% більше, ніж у попередньому році (34%). Більш значні підприємства малого та середнього бізнесу, особливо ті, що мають від 20 до 49 співробітників, страждають непропорційно більше: вони стикаються з вищою частотою інцидентів та більш серйозними наслідками, включаючи фінансові втрати та операційний стрес. Значною проблемою стали загрози, що базуються на штучному інтелекті, такі як «діпфейки» та витончений фішинг, які дають злочинцям можливість здійснювати більш переконливі та масштабні атаки, які співробітникам важче виявити… Незважаючи на ці загрози, що постійно еволюціонують, NCSC наголошує, що перевірені методи забезпечення безпеки, такі як багатофакторна автентифікація, оновлення програмного забезпечення та регулярне створення резервних копій, залишаються ефективними, проте між зростаючою обізнаністю та фактичною профілактичною поведінкою все ще існує розрив. Примітно, що майже третина малих та середніх підприємств досі не проводить навчання персоналу з питань кібербезпеки, залишаючи критично важливу лінію оборони вразливою як до традиційних атак, так і до атак із використанням штучного інтелекту. Крім того, значною проблемою залишається недостатнє повідомлення про інциденти, оскільки багато підприємств вважають розкриття інформації про незначні порушення непотрібним; проте NCSC наголошує, що повідомлення про всі інциденти має вирішальне значення для виявлення схем атак, надання допомоги жертвам та покращення національної розвідки щодо загроз». ***(Peter Sonner. 76% of New Zealand mid-sized firms faced***

cyber threats // Beinsure (https://beinsure.com/news/76-of-new-zealand-mid-sized-firms-faced-cyber-threats/). 24.09.2026).

***

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

«Міністерство національної оборони Тайваню (MND) запропонувало бюджет у розмірі 95,93 млн тайваньських доларів (3,03 млн доларів США) на створення нової «військової групи з кіберполювання» у складі Командування інформаційних, комунікаційних та електронних сил. Ця ініціатива знаменує стратегічний перехід від пасивної кібербезпеки, заснованої на брандмауерах, до позиції «інтегрованого нападу та оборони», спрямованої на активний пошук та усунення «сліпих зон» у мережі. Під керівництвом генерал-лейтенанта Мао Чень-чжоу цей підрозділ формується для протидії дедалі поширенішим тактикам «сірої зони» та кіберпроникненням з боку Комуністичної партії Китаю (ССР), зокрема для боротьби з просунутими стійкими загрозами, які тривалий час залишаються прихованими в тайванських військових мережах та критичній інфраструктурі…

Виходячи з припущення, що системи вже скомпрометовані, нова команда з кіберполювання проходитиме тренування в умовах реальних бойових дій за зразком військових навчань «Cyber Flag» Збройних сил США під керівництвом іноземних інструкторів. Персонал аналізуватиме мільярди системних журналів та моделей мережевого трафіку, щоб виявити приховані «задні двері» та усунути приховані загрози до того, як супротивники зможуть здійснити руйнівні атаки або викрасти дані. Цей проактивний підхід відповідає американським стратегіям «постійного залучення» та «активної оборони», що сприяє модернізації збройних сил Тайваню з метою забезпечення стійкості ключових систем управління, зв'язку та цивільної інфраструктури в мирний час, а також їхньої безперебійної координації з міжнародними союзниками під час військового конфлікту». ***(Lo Tien-bin. MND 'cyber hunt team' plan revealed // The Taipei Times (https://www.taipeitimes.com/News/front/archives/2026/09/06/2003863757). 06.09.2026).***

***

«Щоб протидіяти зростаючій загрозі складних кібератак, уряд Японії планує створити централізований центр превентивної кіберзахисту поруч із Міністерством оборони в Токіо. Проєкт цього спеціалізованого об'єкта, розробка якого запланована на 2027 фінансовий рік, а завершення будівництва — приблизно на 2032 рік, передбачатиме розміщення в ньому Національного департаменту з питань кібербезпеки Національного агентства поліції, кіберпідрозділу Сил самооборони та Національного управління з питань кібербезпеки Секретаріату Кабінету міністрів з метою підвищення рівня координації, безпеки та оперативної ефективності… Ця ініціатива ґрунтується на прийнятому минулого року законі про «активну кіберзахист», який надає уряду юридичні повноваження постійно

відстежувати комунікації та превентивно нейтралізувати ворожі сервери. У рамках цієї оперативної структури поліція очолюватиме початкові заходи з нейтралізації серверів, тоді як Сили самооборони втручатимуться за вказівкою прем'єр-міністра у разі надзвичайно складних та організованих загроз… Створення цього центру є відповіддю на серйозну загрозу: за даними уряду, 99 відсотків повідомлень про кібератаки, виявлених у 2025 році, походили з-за кордону і були спрямовані проти широкого кола вітчизняних організацій, зокрема великих роздрібних мереж, телекомунікаційних компаній та медичних закладів. Хоча на будівництво фізичного центру знадобиться кілька років, уряд санкціонував початок активних заходів з нейтралізації кіберзагроз з 1 жовтня, ще до повного введення центру в експлуатацію у 2027 році». ***(Japan plans to set up cyber defense hub near Defense Ministry around 2032 // THE MAINICHI NEWSPAPERS (https://mainichi.jp/english/articles/20260909/p2g/00m/0na/010000c). 09.09.2026).***

***

«Міністерство енергетики Філіппін ухвалило циркуляр № DC2025-01-0001, яким закріплено рамки кібербезпеки та кіберстійкості в енергетичному секторі. Ця політика є відповіддю на зростаючу залежність сектору від цифрових технологій і спрямована на захист як інформаційних (IT), так і операційних (OT) систем. Відповідно до Національного плану кібербезпеки на 2023–2028 роки, вона широко застосовується до зацікавлених сторін у сфері енергетики, включаючи організації, що займаються енергетичними ресурсами, виробництвом, передачею та розподілом електроенергії, нафтою та газом, а також суб'єкти, визначені як критична інформаційна інфраструктура (CII)…

Ця рамкова програма передбачає створення кількох органів для координації її впровадження. Наглядовий комітет з питань кібербезпеки та кіберстійкості в енергетиці здійснює моніторинг програм та дотримання вимог, тоді як технічна робоча група, використовуючи критерії, що ґрунтуються на оцінці ризиків, надає рекомендації щодо суб'єктів, які слід визнати об'єктами CII. Команда реагування на комп'ютерні надзвичайні ситуації в енергетичному секторі координує реагування на інциденти, а енергетичні компанії, визначені як об'єкти CII, повинні створити власні організаційні команди реагування на надзвичайні ситуації для усунення та мінімізації наслідків інцидентів у сфері кібербезпеки…

Організації, що підпадають під дію CII, мають широкі зобов'язання щодо оцінки, аудиту та звітності. Вони повинні використовувати «Рамку оцінки кібербезпеки» для оцінки ризиків та стану безпеки IT- та OT-систем, тоді як «Картка оцінки кіберстійкості» дозволяє оцінити їхню здатність протистояти кіберінцидентам та відновлюватися після них. Обидві оцінки мають пройти незалежний аудит та бути затверджені Департаментом інформаційних та комунікаційних технологій (DICT). Суб'єкти, що підлягають регулюванню, повинні щорічно до 30 квітня подавати ці оцінки, проводити та звітувати про оцінку вразливостей і тестування на проникнення для критично важливих IT-активів, включаючи пристрої Інтернету речей (IoT), а також надавати щоквартальні звіти щодо питань кібербезпеки, які були розглянуті, вирішені та усунені. Ці заходи повинні бути частиною загальної програми кібербезпеки та кіберстійкості…

Дотримання вимог також має відповідати Закону Філіппін про захист персональних даних, вимогам щодо конфіденційності та інтелектуальної власності, а також чинному законодавству про кіберзлочини. Хоча звіти про інциденти в сфері кібербезпеки, як правило, є закритими, про інциденти, що потенційно становлять загрозу для персональних даних, необхідно повідомляти Національну комісію з питань захисту персональних даних. У випадках, коли розкриття інформації може зачепити інтереси фізичних осіб, відповідні органи з питань кібербезпеки повинні надіслати повідомлення протягом 72 годин, щоб ризики можна було оперативно усунути». ***(DOE Establishes Cybersecurity and Cyber Resilience Framework for the Energy Sector // Ocampo & Suralvo Law Offices (https://www.ocamposuralvo.com/2026/09/10/doe-establishes-cybersecurity-and-cyber-resilience-framework-for-the-energy-sector/). 10.09.2026).***

***

«У міру того, як цифрові середовища Індії стають дедалі складнішими та автоматизованішими, країна стикається з критичною нестачею фахівців у сфері кібербезпеки: кількість таких фахівців становить лише 380 000, тоді як попит з боку підприємств перевищує 1,2 мільйона. Цей дефіцит свідчить про значний брак спеціалізованих практичних навичок, зокрема у сферах хмарних технологій та управління ризиками підприємств. Щоб подолати цю прогалину, галузь повинна переорієнтуватися з традиційного навчання, заснованого на сертифікації, на практичне навчання, орієнтоване на розвиток компетентностей. Фахівцям необхідний практичний досвід, який можна отримати завдяки симуляціям, лабораторним заняттям та реальним проєктам, щоб розвинути критичне мислення, необхідне для інтерпретації автоматизованих сигналів та ефективного реагування на інциденти… Крім того, у зв’язку зі стрімким розвитком ландшафту загроз персонал також повинен готуватися до майбутніх технологічних проривів, таких як перехід до постквантової криптографії, щоб мінімізувати майбутні ризики, пов’язані з квантовими обчисленнями. Оскільки кібербезпеку не можна розглядати як статичну, одноразову кваліфікацію, організації повинні формувати культуру безперервного навчання, яка адаптується до мінливих технологічних стеків та нових загроз. Зрештою, в епоху, де домінує автоматизація, справжня сила команди з безпеки полягатиме не лише в досконалості її інструментів, а й у людській здатності розуміти контекст, виносити обґрунтовані судження та діяти рішуче». ***(Preparing India’s cybersecurity workforce for cloud, AI and quantum risks // HindustanTimes (https://www.hindustantimes.com/education/features/preparing-india-s-cybersecurity-workforce-for-cloud-ai-and-quantum-risks-101789022257285.html). 10.09.2026).***

***

«За останні два роки з Корейського агентства з питань Інтернету та безпеки (KISA) пішло понад 100 ключових співробітників, що викликає серйозні побоювання щодо здатності країни розслідувати кіберінциденти в корпоративному секторі. Цей відтік кадрів, що становить понад 10 відсотків персоналу агентства, насамперед стосується експертів із ключових слідчих груп,

які переходять на роботу в приватні компанії. Оскільки KISA є основою спільних слідчих груп, що об'єднують представників державного та приватного секторів, разом із Міністерством науки та інформаційно-комунікаційних технологій, цей «відтік мізків» загрожує цілісності та ефективності розслідувань порушень… Зростають побоювання, що колишні співробітники KISA можуть використати свої інсайдерські знання, щоб допомогти своїм новим роботодавцям — приватним компаніям — применшити масштаби кіберінцидентів або активно перешкоджати урядовим розслідуванням. Ці побоювання особливо загострилися після нещодавнього випадку, коли було виявлено, що телекомунікаційний гігант KT Corp навмисно перешкоджав урядовому розслідуванню інциденту з хакерською атакою, подаючи неправдиві дані та приховуючи резервні журнали… Підкреслюючи суперечність у тому, що уряд виступає за посилення національної кібербезпеки, водночас втрачаючи своїх провідних експертів, депутат Кім Чан-гьом попередив, що така «обертова двері» для талантів може серйозно підірвати можливості Південної Кореї у сфері реагування на кіберзагрози, що спонукало до закликів щодо вжиття ефективних інституційних заходів для утримання ключового слідчого персоналу». ***(Ko Jae-woo.Cybersecurity gaps widen as KISA loses 50 investigators a year // Herald Corporation (https://biz.heraldcorp.com/article/10869175). 10.09.2026).***

***

«Компанія TM One запустила TM CYDEC — новий центр кіберзахисту на своєму кампусі в Кіберджаї (Малайзія), покликаний усунути «сліпі зони» безпеки та прискорити реагування на загрози для підприємств і державних установ. Працюючи за моделлю «Cyber Fusion», центр інтегрує можливості підключення, хмарних технологій та кібербезпеки, щоб забезпечити єдиний огляд усієї цифрової екосистеми організації, замінивши неефективні, розрізнені підходи до безпеки цілодобовим моніторингом та корельованою аналітикою загроз. Цей цілісний підхід не тільки дозволяє приймати рішення швидше та точніше, але й конкретно вирішує нові ризики, пов'язані зі штучним інтелектом, такі як витік даних, управління та цілісність моделей… Крім того, TM CYDEC забезпечує локалізоване управління та контроль, щоб допомогти організаціям орієнтуватися у нормативних вимогах Малайзії, зокрема у Законі про кібербезпеку 2024 року та Законі про захист персональних даних 2010 року. Маючи на своєму рахунку численні міжнародні сертифікати ISO, центр використовує розгалужену інфраструктуру TM One у сферах підключення, хмарних технологій та центрів обробки даних, щоб отримувати аналітичну інформацію, що виходить за межі традиційних операцій з безпеки, що в кінцевому підсумку сприяє зміцненню кіберстійкості та захисту критично важливих систем, на яких базується цифрова економіка Малайзії». ***(TM One Opens CYDEC To Strengthen Cyber Defence For Enterprises And Government // Reach Publishing Sdn Bhd (https://www.businesstoday.com.my/2026/09/08/tm-one-opens-cydec-to-strengthen-cyber-defence-for-enterprises-and-government/). 08.09.2026).***

***

«Закон Японії про активний кіберзахист, основна фаза застосування якого розпочнеться 1 жовтня 2026 року, запроваджує суворі вимоги щодо повідомлення про кіберінциденти для визначених операторів об'єктів критичної інфраструктури, що докорінно змінює повсякденні робочі процеси Центру операцій з безпеки (SOC). Відповідно до цієї системи оператори 15 критично важливих секторів мають повідомляти уряду про визначені кіберінциденти, зокрема про попередні події, як-от спроби підбору пароля та сліди несанкціонованого доступу, надсилаючи негайне початкове повідомлення, а потім – вичерпний технічний звіт протягом 30 днів… Відлік часу для подання звітності починається з моменту «виявлення», що підкреслює важливість безперервного моніторингу журналів для запобігання прихованій втраті даних та вимагає від SOC підвищення статусу звітності щодо сповіщень, які традиційно мають низький рівень серйозності. Сфера регулювання виходить за межі основних об'єктів і охоплює периферійні пристрої, сервери автентифікації та, потенційно, системи сторонніх підрядників або хмарні системи, а також покладає допоміжні обов'язки з безпеки на IT-постачальників. Щоб дотриматися цих вимог, організації повинні встановити чіткі протоколи виявлення інцидентів, забезпечити безперебійну передачу журналів та вести уніфіковані записи про випадки, які одночасно відповідають вимогам кількох нормативно-правових баз. У відповідь на ці операційні зміни платформа з відкритим кодом simpliSOC надає готові до використання можливості, адаптовані до вимог законодавства, зокрема спеціалізовані правила виявлення Wazuh, оповіщення про втрату журналів та безпечне локальне управління випадками для захисту конфіденційної інформації про загрози… Хоча simpliSOC використовує локальну велику мовну модель для допомоги у первинній сортуванні сповіщень та наданні пояснень простою мовою, усі критично важливі рішення щодо визначення обсягу робіт та складання звітів залишаються суто під контролем людини. Зрештою, законодавство не вводить нових концепцій у сфері кібербезпеки, а навпаки, передбачає значні правові та репутаційні наслідки за невиконання вимог щодо дотримання надійних, добре задокументованих процедур виявлення та реагування, які зрілі SOC вже повинні застосовувати». ***(Japan's Active Cyber Defense Law Goes Live October 1: What "Report Promptly, Detail in 30 Days" Demands From Your SOC // Simplico (https://www.simplico.net/2026/09/24/active-cyber-defense-law-soc-incident-reporting/). 24.09.2026).***

***

«19 серпня 2026 року уряд В'єтнаму видав комплексний пакет із семи указів (укази № 327–333) для введення в дію нещодавно унормованого Закону про кібербезпеку, який встановлює сувору нормативно-правову базу у сферах кібербезпеки, захисту персональних даних та управління цифровим контентом. Центральним елементом цієї системи є Указ № 330, який запроваджує суворий режим адміністративних санкцій із значними штрафами, що розраховуються на основі доходу — до 5% річного доходу організації на в'єтнамському ринку — за критичні порушення у сфері захисту персональних даних, зокрема щодо несумісної з законодавством транскордонної передачі даних.

З метою забезпечення системної стійкості Указ № 331 запроваджує п’ятирівневу систему класифікації інформаційних систем, що вимагає пропорційних заходів кібербезпеки залежно від ступеня конфіденційності та обсягу оброблюваних даних, тоді як Указ № 332 регулює комерційне надання продуктів та послуг у сфері кібербезпеки за допомогою суворих вимог до ліцензування, квот на місцевий персонал та постійних зобов’язань щодо дотримання вимог…

У Декреті № 333 та супутніх Декретах № 327–329 велику увагу приділяється дотриманню оперативних вимог та оперативному реагуванню; ці нормативні акти встановлюють суворі законодавчо визначені терміни — зазвичай протягом 24 годин, а в екстрених випадках — від трьох до шести годин — для видалення незаконного або фальшивого онлайн-контенту та надання даних про відстеження IP-адрес. Крім того, Декрет № 333 визначає умови локалізації даних та вимоги щодо присутності на місцевому ринку для іноземних постачальників цифрових послуг, що передбачає обов’язкове зберігання даних та створення місцевого філіалу лише у разі досягнення певних порогових значень, таких як неодноразові невдачі у виправленні порушень у сфері кібербезпеки. Зрештою, цей взаємопов’язаний пакет нормативних актів вимагає від підприємств, що ведуть діяльність у В’єтнамі, вийти за межі простого оформлення юридичної документації та впровадити надійні міжфункціональні операційні протоколи, спонукаючи організації терміново проаналізувати свої регуляторні ризики, створити механізми оперативного реагування, що працюють цілодобово, переглянути свої оцінки впливу даних та забезпечити відповідність своїх систем і контрактів з постачальниками новим суворим вимогам». ***(Dr. Chau Huy Quang, Vu Thi Que, Logan Leung, Huynh Thi Thu Thuy, Cao Dang Duy, Nguyen Dinh Nha and Trinh Minh Duc. Vietnam Issues Seven Decrees to Implement Its New Cybersecurity Regulatory Framework // Rajah & Tann LCT Lawyers (https://vn.rajahtannasia.com/viewpoints/vietnam-issues-seven-decrees-to-implement-its-new-cybersecurity-regulatory-framework/). 28.09.2026).***

***

«Коли норвезька транспортна адміністрація «Ruter» провела тестування кібербезпеки китайського електробуса «Yutong», у ході розслідування розглядалися дві окремі проблеми: можливість використання транспортного засобу як інструменту геополітичного спостереження та технологічний ризик, пов’язаний із віддаленим доступом виробника. Хоча дослідники не виявили доказів на користь гіпотези про шпигунство, вони все ж виявили підключений до Інтернету канал доступу до критично важливих для експлуатації систем, який теоретично міг би призвести до виведення автобуса з ладу. Однак подальше висвітлення цієї ситуації в ЗМІ, в якому це подавалося як унікальна загроза у вигляді «аварійного вимикача», характерна саме для китайських автобусів, є хибним через критичну помилку в дизайні експерименту… Компанія Ruter порівняла високопідключений автобус Yutong 2025 року випуску зі старішим, менш підключеним європейським автобусом VDL 2022 року випуску, що означає: тест успішно продемонстрував ризики, пов’язані з сучасними підключеними транспортними засобами, але не зміг визначити національну приналежність як

основну причину. Оскільки в ході експерименту не було проведено порівняльного тестування Yutong із сучасними європейськими моделями з високим рівнем підключення від таких виробників, як MAN або Solaris, не вдалося встановити, чи є вразливість до віддаленого доступу проблемою, характерною саме для китайських моделей, чи це стандартна особливість сучасної транспортної техніки… Це обмеження ще раз підкреслюється результатами подальшої датської оцінки, проведеної на замовлення компанії Movia, в якій на основі стандартних рамок кібербезпеки для автомобілів було зроблено висновок, що китайські виробники за своєю суттю не є менш захищеними в плані кібербезпеки, ніж їхні європейські колеги. Зрештою, сукупність цих висновків підкреслює, що справжня проблема кібербезпеки полягає не в країні походження, а в фундаментальній реальності: сучасні автобуси є комп'ютерами, підключеними до мережі. Тому транспортні підприємства повинні надавати пріоритет суворим протоколам закупівель та управління автопарком для контролю віддаленого доступу, автентифікації оновлень програмного забезпечення та сегментації критично важливих систем, незалежно від бренду виробника». ***(Michael Barnard. Norway Found A Real Bus Cyber Risk. It Didn't Show It Was Chinese. // CleanTechnica (https://cleantechnica.com/2026/09/30/norway-chinese-bus-cybersecurity-wrong-control/). 30.09.2026).***

***

Ізраїль, Туреччина та країни Близького сходу

«Туреччина суттєво реорганізувала свою систему регулювання цифрової сфери, внесла зміни до Закону про електронні комунікації, Закону про кібербезпеку та Закону про Інтернет, головним чином з метою консолідації повноважень у сфері кібербезпеки та управління Інтернетом у рамках Управління з питань кібербезпеки при Президентові. Функції, які раніше були розподілені між Управлінням інформаційних та комунікаційних технологій (BTK), Міністерством транспорту та інфраструктури та іншими органами, дедалі частіше передаються цьому центральному органу. Ці зміни потенційно зачіпають широке коло організацій, зокрема операторів телекомунікацій, центри обробки даних, провайдерів хостингу та доступу до Інтернету, соціальні мережі, ігрові платформи, хмарні сервіси та постачальників контенту…

Відповідно до Закону про електронні комунікації, Адміністрація з питань кібербезпеки тепер контролює політику та регулювання, що стосуються інтернет-доменних імен. Вона також отримує надзвичайні повноваження, що дозволяють їй зобов'язувати операторів та постачальників цифрових послуг вживати необхідних заходів у визначених обставинах, пов'язаних із національною безпекою, причому адресати таких розпоряджень, як правило, повинні виконати їх протягом двох годин. Такі заходи повинні згодом отримати судове затвердження у встановлені терміни, інакше вони втрачають чинність. Президентська адміністрація також може накладати адміністративні штрафи в розмірі від 20 000 до 100 000 турецьких лір за певні порушення зобов'язань, передбачених законом…

Зміни до Закону про кібербезпеку передбачають передачу відповідної інфраструктури, систем, документації, активів, повноважень та персоналу Міністерства телекомунікацій та зв'язку (BTK) до Адміністрації з питань кібербезпеки. Чинне підзаконне законодавство залишається чинним протягом перехідного періоду, при цьому посилання на колишні органи влади трактуються як посилання на Адміністрацію до моменту видання нових правил застосування. Адміністрація також бере на себе обов'язки щодо технічної підтримки законного перехоплення. Важливо, що організації, які не надають запитувані дані, документи, апаратне та програмне забезпечення або іншу допомогу, тепер можуть бути оштрафовані на суму від 1 млн до 10 млн турецьких лір, що суттєво посилює повноваження регулятора щодо забезпечення дотримання законодавства…

Закон про Інтернет також було реорганізовано з урахуванням повноважень Президентського управління з питань кібербезпеки. Наразі цей орган виконує численні функції, які раніше покладалися на BTK, зокрема ініціативи щодо безпечнішого Інтернету, видалення контенту та блокування доступу, моніторинг в Інтернеті, адміністративне правозастосування, технічну підтримку та нагляд за Асоціацією провайдерів доступу. Обов'язки соціальних мереж щодо місцевих представників, запитів на видалення контенту, звітності, локалізації даних, безпеки дітей та прозорості алгоритмів загалом залишаються незмінними, але відповідальність за забезпечення дотримання цих вимог перейшла від BTK до Президентського управління з питань кібербезпеки. Існуючі санкції, такі як штрафи, обмеження реклами та обмеження пропускної здатності, також залишаються в силі…

Однією з істотних змін є розширення юридичного визначення поняття «дані про трафік» шляхом включення до нього інформації про порти відправлення та призначення. Це може суттєво збільшити обсяг та детальність інформації на рівні з'єднання, яку провайдери повинні реєструвати та зберігати. Отже, компаніям, яких це стосується, можливо, доведеться переглянути свої системи реєстрації, ємність сховищ та процедури зберігання даних, щойно у підзаконних актах буде уточнено необхідні формати та поля…

Ці зміни мають переважно інституційний характер, а не є цілком новим набором зобов'язань у сфері кібербезпеки, проте передачу повноважень не слід розглядати як суто адміністративну процедуру. Президентська адміністрація з питань кібербезпеки може сформувати власні тлумачення, пріоритети нагляду та практику забезпечення дотримання вимог, що відрізнятимуться від підходу BTK. У поєднанні з розширеними повноваженнями щодо накладення штрафів та більш широкими вимогами до даних про трафік ця реорганізація створює практичні наслідки для дотримання вимог. Тому цифрові підприємства, що ведуть діяльність у Туреччині, повинні переглянути свої існуючі домовленості, визначити, які функції тепер підпадають під компетенцію Управління, підготуватися до нових імплементаційних нормативних актів та уважно стежити за новим підходом до забезпечення дотримання вимог, що формується». ***(Alican Babalioglu, Melis Celik and Ezgi Bahar. Türkiye centralises key digital governance functions under the Cybersecurity Presidency // CMS Legal (https://cms.law/en/tur/legal-updates/turkiye-***

centralises-key-digital-governance-functions-under-the-cybersecurity-presidency). 10.09.2026).

***

Країни Африки

«Міністр зв'язку Самуель Нартей Джордж повідомив, що Агентство з кібербезпеки Гани (CERT-GH) відреагувало на 3 363 інциденти у сфері кібербезпеки в період з січня по червень 2026 року, підкресливши зростаючу необхідність зміцнення цифрової інфраструктури країни у міру збільшення залежності від цифрових платформ. Виступаючи на заході «Government Accountability Series» в Аккрі, міністр наголосив, що уряд також завершив оцінку вразливостей 25 об'єктів критичної інформаційної інфраструктури у таких важливих секторах, як охорона здоров'я, освіта, державне управління, безпека та комунальні послуги… З метою зміцнення потенціалу галузі за цей період було ліцензовано або акредитовано 479 постачальників послуг у сфері кібербезпеки, 116 установ та 2 685 фахівців. Ініціативи з підвищення обізнаності громадськості також зазнали значного розширення: навчання з питань кібербезпеки охопило понад 84 000 дітей та молоді, 427 лідерів у сфері ІКТ у вищих навчальних закладах та приблизно 8 800 громадян. Крім того, нещодавно запущений Ганійський форум галузі кібербезпеки залучив понад 300 учасників, а Комісія з захисту даних зафіксувала зростання регуляторної діяльності на 51,5% та різке збільшення кількості новозареєстрованих контролерів даних на 98,4%... У законодавчій сфері уряд просуває Проєкт цифрової трансформації Гани шляхом перегляду 15 законів у сфері інформаційно-комунікаційних технологій (ІКТ) та завершив консультації із зацікавленими сторонами щодо 10 пріоритетних законопроєктів. Крім того, парламент ухвалив законодавчий акт щодо реєстрації SIM-карт, що створює передумови для того, щоб регуляторний орган розпочав реєстрацію SIM-карт із біометричною верифікацією до кінця 2026 року». ***(Ernest K. Arhinful. Cybersecurity Authority responds to 3,363 incidents in six months – Sam George // Multimedia Group (https://www.myjoyonline.com/cybersecurity-authority-responds-to-3363-incidents-in-six-months-sam-george/). 07.09.2026).***

***

«…У міру прискорення цифрової трансформації в Африці підприємства середнього бізнесу стикаються з дедалі більшим розривом у рівні кіберзахищеності, борючись з обмеженими ресурсами та нестачею спеціалізованих навичок у протидії складним кіберзагрозам. У таких умовах традиційні, розрізнені засоби безпеки виявляються неефективними, що часто призводить до «втоми від сповіщень» та приховування сигналів про загрози. Відповідно, організації повинні перейти від накопичення розрізнених точкових рішень до впровадження комплексного управління вразливостями та консолідованої видимості, надаючи пріоритет швидкому локалізуванню та проактивному усуненню ризиків… Щоб допомогти подолати цю прогалину,

партнер у сфері кібербезпеки WithSecure пропонує орієнтовану на результат модель, засновану на хмарній платформі WithSecure Elements, яка об'єднує захист кінцевих точок, хмарну безпеку та управління вразливостями в єдиному інтерфейсі. Завдяки інтеграції пошуку загроз на основі штучного інтелекту з керованим людьми процесом виявлення та реагування платформа ефективно фільтрує фоновий шум і забезпечує швидке, кероване локалізування складних атак. Крім того, WithSecure використовує підхід на основі екосистеми Co-Security, інтегруючи свої можливості безпосередньо в місцевих постачальників керованих послуг та партнерів по каналах збуту, щоб надавати контекстуальні рішення з локальною підтримкою… Зрештою, для забезпечення стійкої кіберстійкості африканським бізнес-лідерам рекомендується покращити виявлення загроз за допомогою уніфікованих платформ, надати пріоритет проактивному контролю вразливостей для усунення ризикованих слабких місць, а також використовувати партнерські відносини у сфері безпеки на основі спільного управління для розширення власних внутрішніх можливостей та захисту своїх цифрових операцій». ***(Bridging the cyber equity gap: How outcome-based defence is reshaping enterprise security in Africa // ITWeb Limited (https://www.itweb.co.za/article/bridging-the-cyber-equity-gap-how-outcome-based-defence-is-reshaping-enterprise-security-in-africa/6GxRKqYQEkBqb3Wj). 08.09.2026).***

***

«У серпні 2026 року в Нігерії спостерігався значний сплеск кіберзагроз: щотижня на одну організацію припадало в середньому 4 906 кібератак — це на 45% більше, ніж у минулому році, що ставить країну в число найбільш вразливих до атак в Африці. Згідно з доповіддю Check Point Research «Global Threat Intelligence», цей показник більш ніж удвічі перевищує середній світовий показник (2 422) і посідає друге місце на континенті після Анголи, де щотижня фіксувалося 5 416 атак. У цілому по Африці організації стикалися в середньому з 3 335 атаками на тиждень, причому сектор енергетики та комунальних послуг виявився найбільш вразливою галуззю, за якою слідували фінансові послуги та державні установи… У глобальному масштабі також посилилася активність програм-вимагачів: у серпні було зареєстровано 1 042 атаки — майже вдвічі більше, ніж у попередньому році — які в першу чергу зачіпали сфери бізнес-послуг та промислового виробництва, а головними ініціаторами цих атак були групи-вимагачі «Qilin» та «The Gentlemen». Таке загострення загроз відповідає нещодавнім попередженням Нігерійської команди реагування на комп'ютерні надзвичайні ситуації (ngCERT), яка попередила організації про складні DDoS-атаки (Distributed Denial-of-Service), що здійснюються за допомогою ботнетів і спрямовані проти критичної національної інфраструктури… Крім того, ngCERT привернув увагу до серйозних фінансових загроз, оприлюднивши інформацію про скоординовану атаку на банкомати банку UBA Senegal, в результаті якої було незаконно знято понад 2 мільйони доларів. Це підкреслює, що кіберзлочинці дедалі частіше використовують фішинг, вразливості ланцюга постачання та доступ інсайдерів для розповсюдження шкідливого програмного забезпечення типу «джекпоттинг» та заподіяння значної операційної та фінансової шкоди в усьому

регіоні». ***(Samson Akintaro. Nigeria records 4,906 weekly cyberattacks as threats rise 45% // Nairametrics (https://nairametrics.com/2026/09/12/nigeria-records-4906-weekly-cyberattacks-as-threats-rise-45/). 12.09.2026).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«На тлі нових повідомлень про те, що Іран розширив масштаби своїх кібератак на Сполучені Штати, експерти у сфері технологій застерігають, що хакерство ідеально відповідає геополітичній ситуації Ірану. У репортажі NBC зазначається, що протягом останніх тижнів Тегеран активізував зусилля з метою проникнення в американські комп'ютерні системи, що потенційно може вплинути на електроенергетику, телекомунікації та іншу критичну інфраструктуру… Морі Хабер, головний радник з питань безпеки компанії BeyondTrust, зазначив, що його не дивують постійні спроби Ірану, охарактеризувавши кіберзасоби як асиметричну зброю, яка вимагає лише фахових знань, відповідає становищу Ірану в умовах санкцій і дозволяє завдавати значного удару по населенню без використання літаків, ракет чи персоналу на американській території, водночас створюючи невизначеність щодо встановлення відповідальності та пропорційної відповіді; він зазначив, що самі атаки не є особливо складними з технічної точки зору, але досягають успіху завдяки використанню недоліків у кібербезпеці, таких як застарілі системи, слабкі процедури захисту паролів та пристрої, підключені до Інтернету без необхідності, зауваживши, що найпростіший спосіб проникнути через парадні двері — це часто виявити, що хтось забув їх зачинити… Йії Мяо, головний директор з продуктів компанії OPSWAT, також не висловив здивування та застеріг, що, хоча нещодавні іранські хакерські атаки не спричинили нічого катастрофічного, Сполучені Штати не повинні впадати в оману щодо безпеки, оскільки навіть примітивна спроба атаки на незахищене обладнання критичної інфраструктури, підключене до Інтернету, може спричинити реальні збої, оскільки такі системи, як водопровідні чи енергетичні об'єкти, не можна просто відключити від мережі для встановлення виправлень… У липні кілька штатів США підтвердили факти хакерських атак на свої системи водопостачання, які, на думку експертів, ймовірно, були здійснені з Ірану, хоча президент Трамп на той час звинуватив у цьому некомпетентність державних чиновників, а Агентство з кібербезпеки та безпеки інфраструктури опублікувало попередження — не називаючи Ірану — про зростання кількості атак на програмовані логічні контролери у секторі водопостачання та водовідведення та закликало операторів дотримуватися федеральних інструкцій… Одна з пов'язаних з Іраном груп, «Handala», часто хвалилася своїми діями з моменту початку ударів США та Ізраїлю наприкінці лютого: у березні вона зламала особисту електронну пошту та хмарні сервіси директора ФБР Каша Пателя, а згодом було встановлено, що саме вона стояла за кібератакою на медико-технологічну компанію «Stryker», що базується в Мічигані, а в червні взяла на себе відповідальність за злам системи «California Water Service», з якої опублікувала 5 гігабайтів даних, при цьому підкресливши

свою стриманість: хоча місцеві джерела повідомляли про відключення водопостачання для близько 20 000 споживачів, перебої були спричинені браком технічних знань у компанії, а не будь-якими деструктивними діями «Handala», яка заявила, що володіє, але не використовувала можливості завдати такої шкоди. Кіберконфлікти між цими країнами були загальновідомим секретом задовго до нещодавніх атак: у звіті Microsoft про цифрову оборону за 2025 рік зазначено, що Іран найчастіше атакує Ізраїль, США, ОАЕ та Індію; минулого року американські чиновники попереджали, що Іран посилює свої зусилля, а заступник директора ФБР Бретт Летерман назвав використання кіберзброї для руйнування інфраструктури, від якої залежить суверенна держава, «червоною лінією»; у свою чергу, Іран звинуватив США та Ізраїль у спробах зламати його системи… Після американських ударів директор з питань кібербезпеки Шон Кернкросс назвав Іран «постійним порушником», чиї спроби завдати шкоди цифровій інфраструктурі США посилилися і який ніколи не припиняв своїх спроб, тоді як Джон Фоккер із компанії Trellix порадив іншим країнам взяти це до уваги, посилаючись на нещодавні інциденти, пов’язані з критичною інфраструктурою Великої Британії, та на постійні атаки, пов’язані з Іраном, на енергетичний та нафтогазовий сектори по всьому Близькому Сходу, та зауважив, що кібероперації стали продовженням сучасного геополітичного конфлікту, що дозволяє державам чинити тиск, створювати збої та сигналізувати про свої наміри, не вдаючись при цьому до ескалації у вигляді прямих військових дій». ***(Cody Combs. Iran's cyber attack strategy is 'perfect weapon' against US // The National (https://www.thenationalnews.com/future/technology/2026/09/02/iran-cyberattack-hack-us-infrastructure/). 02.09.2026).***

***

«Державний департамент США оголосив винагороду в розмірі 10 мільйонів доларів за інформацію про місцеперебування високопоставленого іранського чиновника Аміра Яряба, який, як стверджується, очолює Кібер-електронне командування Корпусу ісламської революційної гвардії (IRGC-CEC). Американські чиновники звинувачують Яряба в керівництві низкою іранських кібергруп — зокрема «Шахід Хеммат» та «Шахід Шуштарі» — які атакують об’єкти критичної інфраструктури в секторах оборони, ЗМІ, судноплавства, туризму, енергетики, фінансів та телекомунікацій у США, Європі та на Близькому Сході. Крім того, Яряб керує організаціями, пов’язаними з IRGC-CEC, такими як «CyberAv3ngers», «Dadeh Afzar Arman» (DAA) та «Mehrsam Andisheh Saz Nik» (MASN), які розповсюджують шкідливе програмне забезпечення проти цивільної інфраструктури по всьому світу…

Ці угруповання неодноразово націлювалися на об’єкти життєво важливого значення: зокрема, угруповання CyberAv3ngers раніше здійснювало атаки на підприємства водопостачання у 2023 та 2024 роках. Американські чиновники попередили, що іранська кіберактивність проти водогосподарської галузі відновилася наприкінці липня, що призвело до зломів понад 100 організацій у щонайменше 12 штатах. Хакери з Тегерана також взяли на себе відповідальність за вторгнення, що зачепили велику компанію з виробництва медичного обладнання та

особистий електронний поштовий акаунт директора ФБР. Крім того, Міністерство юстиції нещодавно звинуватило хакерів, пов'язаних з іранськими збройними силами, у зломі електронних поштових скриньок співробітників Міністерства праці, Федеральної комісії з регулювання енергетики та кількох організацій ООН, що змусило Міністерство фінансів ввести санкції проти багатьох причетних іранських громадян». ***(Jonathan Greig. US offers $10 million for info on Iranian allegedly behind cyberattacks on critical infrastructure // Recorded Future News (https://therecord.media/us-reward-amir-yaryab-iran-irgc-cyberattacks). 04.09.2026).***

***

«Невелика електростанція у Великій Британії була виведена з експлуатації на чотири дні внаслідок кібератаки, яку пов'язують з іранськими хакерами. Експерти називають цей інцидент ескалацією кампанії, об'єктами якої також стали водогосподарські об'єкти у США. Уряд Великої Британії не назвав назву електростанції та заявляє, що загальна енергетична система ніколи не перебувала під загрозою, хоча досі залишається незрозумілим, чи були безпосередньо порушені системи управління роботою об'єкта, чи його відключили в якості запобіжного заходу… Згідно з повідомленнями, зловмисники, ймовірно, скористалися загальнодоступним програмованим логічним контролером (PLC), використовуючи автоматизовані або створені на основі штучного інтелекту засоби сканування для виявлення вразливих пристроїв та стандартних облікових даних, після чого порушили їх конфігурацію. Цей інцидент свідчить про те, що ризик виходить за межі великих операторів критичної інфраструктури, оскільки автоматизовані атаки можуть аналогічним чином націлюватися на виробників, склади, «розумні» будівлі, дрібних виробників енергії та сторонніх постачальників, які мають віддалений доступ до операційних технологій… Це набуває дедалі більшого значення, оскільки енергетична система Великої Британії стає все більш децентралізованою та залежною від дрібних генераторів, відновлюваних джерел енергії та акумуляторних систем, які можуть не підпадати під традиційні регуляторні вимоги. У відповідь на це уряд Великої Британії та Національний центр кібербезпеки закликали організації виявити та вилучити промислові пристрої, які без необхідності підключені до Інтернету, замінити паролі за замовчуванням, запровадити багатофакторну автентифікацію, обмежити віддалений доступ та посилити сегментацію мереж IT та OT… Експерти також рекомендують запровадити єдиний моніторинг IT- та операційних середовищ, використовувати брандмауери та білі списки доступу, застосовувати технології раннього попередження та маскування, регулярно проводити навчання з реагування на інциденти та глибше розуміти потенційні шляхи атак. Загальний висновок полягає в тому, що організації, які експлуатують підключені фізичні системи, повинні розглядати відносно прості кіберуразливості як потенційно серйозні операційні ризики та формувати стійкість, зосереджуючись на запобіганні атакам, їх виявленні та відновленні після них». ***(Kate O'Flaherty. Iran power plant closure is a warning to all businesses: How to respond // Future US, Inc. (https://www.itpro.com/security/cyber-attacks/iran-power-plant-closure-is-a-warning-to-all-businesses-how-to-respond). 08.09.2026).***

***

«Російські хакери, що діють за підтримки держави, а саме пов'язана з ГРУ група BlueDelta (також відома як APT28 або Fancy Bear), використовують новий прихований бекдор для Windows під назвою HOOKEDGE з метою ведення шпигунської діяльності проти дипломатичних, урядових та оборонних організацій по всій Європі, зокрема в Румунії, Іспанії та Туреччині. Кампанія з проникнення базується на електронних листах типу «спірфішинг», що містять вкладення у форматі Microsoft Word із увімкненими макросами, які використовують підроблені повідомлення про помилки, щоб спонукати жертв увімкнути шкідливий вміст… Після активації шкідливе ПЗ встановлює постійний канал управління, використовуючи легітимний браузер Microsoft Edge та загальнодоступні сервіси вебхуків, що дозволяє його комунікаціям непомітно зливатися зі звичайним веб-трафіком. Функціонуючи як бекдор типу «опитування», HOOKEDGE отримує інструкції та викрадає дані через окремі приховані екземпляри Edge, систематично видаляючи тимчасові артефакти, щоб приховати сліди своєї діяльності. Щоб ще ефективніше уникнути автоматизованого аналізу в пісочниці, зловмисники застосовують багаторівневе управління жертвами та динамічно регулюють інтервали передачі сигналів, іноді затримуючи перевірки, щоб перечекати періоди рутинного моніторингу… Оскільки трафік шкідливого програмного забезпечення імітує законний веб-перегляд, експерти з безпеки застерігають, що традиційних перевірок репутації доменів недостатньо. Натомість фахівці з безпеки повинні застосовувати підхід моніторингу на основі поведінки, який відстежує весь ланцюжок виконання — від запуску скриптів у Word і реєстрації запланованих завдань до аномальної мережевої активності в Edge — при цьому суворо блокуючи макроси з ненадійних інтернет-джерел, щоб запобігти первинному зараженню». ***(Tushar Subhra Dutta. Russian Hackers Use New HOOKEDGE Backdoor to Spy on European Organizations // Cyber Security News (https://cybersecuritynews.com/russian-hackers-use-new-hookedge/). 07.09.2026).***

***

«У майбутній кіберстратегії Пентагону пріоритет буде надано наступальним діям із значним впливом, спрямованим на досягнення суттєвих результатів для міністра оборони та президента Дональда Трампа, що ознаменує перехід до більш агресивної та конфронтаційної позиції в кіберпросторі. За словами бригадного генерала Вільяма Вілберна, заступника головного радника з питань кібербезпеки Міністерства оборони, оборона не є кінцевою метою, а скоріше засобом, що дозволяє проводити потужні наступальні операції… Цей майбутній план, який стане першою кіберстратегією, оприлюдненою з 2023 року, узгоджується з більш широкою національною кіберстратегією адміністрації Трампа та ґрунтується на нещодавніх військових кіберопераціях, таких як «Operation Midnight Hammer», «Operation Absolute Resolve» та «Operation Epic Fury». Вілберн підкреслив, що, хоча військові й надалі проводитимуть щоденні кібероперації, акцент буде зміщено з концепції 2018 року про «постійну взаємодію» та «оборону на випередження» на реалізацію більш ефективних варіантів, які нададуть вищому керівництву більш потужні

інструменти під час криз або конфліктів… Крім того, очікується, що стратегія окреслить напрямки інтеграції штучного інтелекту в структуру кібервійськ та заохочуватиме приватні компанії до участі в наступальних хакерських операціях. Щоб нова доктрина принесла реальні результати, а не залишилася лише теоретичним документом, стратегія міститиме конкретний план дій, спрямований на забезпечення її реалізації та досягнення стратегічних цілей відомства». ***(Mark Pomerleau. DoD cyber strategy aims for 'something big, something muscular' in offensive ops // Breaking Media, Inc. (https://breakingdefense.com/2026/09/dod-cyber-strategy-aims-for-something-big-something-muscular-in-offensive-ops/). 10.09.2026).***

***

«Прогнозується, що глобальні витрати на кібербезпеку в оборонному секторі зазнають значного зростання, що зумовлено посиленням кіберзагроз для військових мереж та зростанням попиту на наступальні можливості. Згідно з доповіддю MarketsandMarkets від 14 вересня, очікується, що світовий ринок кібервійни майже подвоїться протягом наступних п'яти років, збільшившись з 14,99 млрд доларів у 2026 році до 28,75 млрд доларів до 2031 року. Цьому сприяють оборонні організації, які намагаються захистити дедалі більш взаємопов'язані цифрові платформи, хмарні середовища та мережі управління та контролю від складних атак. Водночас західні уряди надають пріоритет наступальним кіберопераціям, щоб знешкодити іноземних зловмисників, які діють поза межами досяжності міжнародних правоохоронних органів, про що свідчить меморандум президента США від серпня 2026 року, який санкціонує співпрацю з приватним сектором щодо наступальних кібератак проти іноземних супротивників…

У регіональному розрізі прогнозується, що в період з 2026 по 2031 рік Європа займе найбільшу частку світового ринку кібервійни, оскільки європейські уряди та НАТО розширюють регіональні військові кіберможливості та проводять спільні кібернавчання. У рамках загального ринку найдинамічнішим сектором, як очікується, стане хмарна безпека завдяки широкому впровадженню військовими хмарної інфраструктури для оперативних даних, програмних додатків та активних кібероперацій. У міру переходу оборонних структур на гібридні та мультихмарні середовища стрімко зростає попит на спеціалізовані засоби безпеки, здатні забезпечити єдиний захист на різних військових платформах та розрізнених мережах». ***(James Coker. Defense Cyber Spending Set to Surge Amid Rising Attacks on Military Systems // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news/defense-cyber-spending-attacks/). 14.09.2026).***

***

«Міністр оборони Піт Хегсет видав директиву, в якій доручив Міністерству оборони захистити вибори у США 2026 року від іноземного втручання, підкресливши таким чином увагу президента Дональда Дж. Трампа до безпеки виборів. У цій директиві Кіберкомандуванню США доручається, у тісній співпраці з Агентством національної безпеки та іншими службами бойової підтримки, використовувати передові розвідувальні та

кіберможливості для виявлення, перешкоджання та нейтралізації іноземного втручання в американські системи голосування… Підкреслюючи, що забезпечення демократичного процесу є «завданням, яке не можна провалити», керівництво Пентагону наголосило на необхідності комплексного урядового підходу, що базується на тісній координації з федеральними, штатними та місцевими партнерами з метою виявлення зловмисного впливу, захисту цілісності виборчої інфраструктури та забезпечення того, щоб основні свободи американського народу залишалися захищеними від зовнішніх маніпуляцій». ***(Pentagon Unveils Cybersecurity Plan To Protect 2026 U.S. Elections // yahoo!news (https://www.yahoo.com/news/politics/articles/pentagon-unveils-cybersecurity-plan-protect-181114993.html). 29.09.2026).***

***

Створення та функціонування кібервійськ

«У відповідь на стрімко мінливий глобальний ландшафт загроз, що формується під впливом штучного інтелекту, 16-та повітряна армія (Air Forces Cyber) суттєво вдосконалює свою кіберзахистну систему, щоб протидіяти автономним ланцюжкам атак на основі штучного інтелекту, які стискають місяці традиційного хакерства до лічених хвилин. Визнаючи кіберпростір основною і часто першою ареною протистояння в сучасних конфліктах, командування реалізує комплексну оборонну стратегію, що базується на чотирьох основних напрямках діяльності: постійне зміцнення мереж за допомогою цілодобового моніторингу, здійснення цілеспрямованої оборони критичної інфраструктури, нанесення проактивних збитків супротивникам шляхом швидкого зриву їхньої діяльності, а також розробка оборонних архітектур, заснованих на принципах «нульової довіри», багатофакторної аутентифікації та мікросегментації… 16-та повітряна армія, штаб-квартира якої розташована на об’єднаній базі «Сан-Антоніо-Лакленд», керує приблизно 45 000 військовослужбовців у 123 локаціях по всьому світу та відповідає за широкий спектр завдань, що включає розвідку, спостереження, криптологічну діяльність та захист інформаційних мереж Міністерства повітряних сил. Співпрацюючи з військовими, промисловими та науковими установами, командування прагне випередити супротивників у кіберпросторі, забезпечуючи спільним силам вирішальну технологічну перевагу та захищаючи національні інтереси в епоху невпинних цифрових інновацій». ***(Anyssa Guzman. 16th Air Force Advances Cyber Defenses as Frontier AI Reshapes the Joint Kill Chain // United States Air Force (https://www.acc.af.mil/News/Article-Display/Article/4591826/16th-air-force-advances-cyber-defenses-as-frontier-ai-reshapes-the-joint-kill-c/). 03.09.2026).***

***

«Міністерство національної оборони Тайваню запропонувало виділити у своєму бюджеті на 2027 рік 95,93 млн нових тайваньських доларів (3,03 млн доларів США) на створення спеціалізованої «військової групи з виявлення

кіберзагроз» у складі Командування інформаційних, комунікаційних та електронних сил. Ця ініціатива знаменує стратегічний перехід від реактивних заходів кібербезпеки до проактивного підходу до виявлення загроз, який ґрунтується на припущенні, що ворожі суб'єкти, можливо, вже проникли у військові мережі. Цей спеціалізований підрозділ аналізуватиме великі обсяги системних журналів та мережевого трафіку з метою виявлення складних постійних загроз (APT) та прихованих «задніх дверей», залишених хакерами, яких підтримує китайська держава і які постійно атакують урядові, оборонні, телекомунікаційні та критичні інфраструктурні сектори Тайваню… Щоб підготуватися до виконання цього складного завдання, команда пройде тренування в умовах імітованого протистояння за зразком військових навчань Збройних сил США під керівництвом іноземних інструкторів, під час яких буде відпрацьовуватися відстеження та усунення зловмисників із критично важливих мереж. Така проактивна позиція не тільки спрямована на зміцнення військового командування та цивільної інфраструктури Тайваню в мирний час, але й відповідає його ширшим зусиллям щодо посилення кіберсумісності зі Сполученими Штатами та союзними партнерами, спираючись на нещодавню участь у багатонаціональних навчаннях, таких як «Cyber Storm IX», організованих Агентством з кібербезпеки та безпеки інфраструктури США». ***(Giulia Bernacchi. Taiwan Proposes to Build Military Team for Hunting Chinese Hackers // The Defense Post (https://thedefensepost.com/2026/09/08/taiwan-military-hunting-chinese-hackers/). 08.09.2026).***

***

Кіберзахист критичної інфраструктури

«Компанії OSC Global та InfraShield представили Janus Cyber — спільну ініціативу, покликану допомогти розробникам передових ядерних реакторів орієнтуватися у складних нормативних вимогах та вимогах щодо кібербезпеки, пов'язаних із розгортанням таких реакторів на військових об'єктах США. Сучасні реактори, що використовуються в оборонних цілях, повинні відповідати трьом взаємопов'язаним вимогам: вимогам ядерного регулювання у сфері кібербезпеки, дозволу Міністерства оборони (DoW) та вимогам кібербезпеки операційних технологій/промислових систем управління (OT/ICS). Janus Cyber об'єднує ці окремі вимоги в єдину скоординовану команду, допомагаючи розробникам створити гнучку, ітеративну архітектуру безпеки протягом усього життєвого циклу реактора…

Це партнерство дозволяє ефективно використовувати взаємодоповнюючі можливості обох організацій. InfraShield очолює розробку стратегії регулювання у сфері кібербезпеки ядерних об'єктів та надає свій власний пакет програмного забезпечення, що включає vTraq®, PEEPS®, UniPath™ та NullCloud.ai. OSC Global через свої дочірні компанії OSC Technical Solutions та OSC Edge надає інженерні послуги з кібербезпеки, проводить тестування на проникнення, забезпечує експлуатацію систем OT/ICS та безпечну інтеграцію з орієнтацією на захист, що

підтверджується такими сертифікатами, як «NSA Trusted Integrator», «Commercial Solutions for Classified» (CSfC) та C3PAO. Функції управління, ризиків та дотримання вимог (GRC) керуються спільно з метою узгодження з конкретними військовими та регуляторними потребами проєктів…

Компанія Janus Cyber побудована таким чином, щоб розглядати кібербезпеку як елемент, що враховується на ранніх етапах проєктування, а не як перешкоду на завершальному етапі, пов'язану з дотриманням вимог. Це сприяє ітеративній розробці в Армії США та дозволяє застосовувати моделі, що керуються Управлінням з регулювання реакторів Армії у співпраці з Міністерством енергетики. Крім того, ця ініціатива допомагає розробникам узгодити військові проєкти з майбутніми процедурами отримання комерційних ліцензій, такими як система «Part 53» Комісії з ядерного регулювання, що базується на оцінці ризиків і набуде чинності у квітні 2026 року. Завдяки створенню гнучкої системи контролю та збереженню архітектурних даних протягом послідовних ітерацій Janus Cyber дає розробникам змогу адаптуватися до змін у нормативних вимогах без необхідності проведення дорогих перепроєктувань, що затримують реалізацію проєкту, у міру наближення до етапу розгортання». ***(OSC Global and InfraShield launch Janus Cyber to address advanced reactor OT, nuclear and military cybersecurity // Industrial Cyber (https://industrialcyber.co/news/osc-global-and-infrashield-launch-janus-cyber-to-address-advanced-reactor-ot-nuclear-and-military-cybersecurity/). 02.09.2026).***

***

«Агентство з кібербезпеки та безпеки інфраструктури (CISA) проводить реструктуризацію своїх послуг з добровільної оцінки кібербезпеки для операторів критичної інфраструктури, припиняючи використання шести застарілих методів оцінки на основі анкет на користь своїх Міжсекторальних цілей ефективності кібербезпеки (CPG). Скасовані програми оцінки, які раніше реалізовувалися регіональними співробітниками CISA за допомогою Інструменту оцінки кібербезпеки (CSET), включають: огляди кіберстійкості, опитування щодо основних аспектів кіберстійкості, оцінки готовності до атак програм-вимагачів, огляди управління інцидентами, оцінки управління зовнішніми залежностями та опитування щодо кіберінфраструктури…

За словами Кріса Бутери, виконуючого обов'язки заступника виконавчого директора Відділу кібербезпеки CISA, цей перехід має на меті скоротити надлишкові процеси, усунути дублювання оцінок та привести ресурси агентства у відповідність до мінливих кіберризиків. Замість того, щоб зменшувати федеральну підтримку у сфері кібербезпеки, ця зміна спрямовує операторів у ключових секторах — зокрема в енергетиці, охороні здоров'я, транспорті, водопостачанні, зв'язку та фінансових послугах — на використання структури CPG, яка пропонує пріоритетні та практичні стандарти безпеки для визначення стратегій захисту та капітальних інвестицій. Хоча регіональні команди CISA більше не проводитимуть активно перевірок на основі анкет, організації все ще зможуть самостійно отримувати доступ до старих матеріалів оцінки та використовувати їх для внутрішніх самооцінок». ***(Matt Seldon. CISA Phases Out Six Cybersecurity Assessment Questionnaires for Critical Infrastructure Operators // Homeland Security***

Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/cisa-phases-out-six-cybersecurity-assessment-questionnaires-for-critical-infrastructure-operators/). 04.09.2026).

***

«29 липня 2026 року Агентство з кібербезпеки Сінгапуру (CSA) опублікувало оновлений Кодекс практики з кібербезпеки для критичної інформаційної інфраструктури (CII), який передбачає суттєві вдосконалення нормативно-правової бази, що регулює діяльність власників критичної інформаційної інфраструктури (CIIO). Хоча Кодекс набирає чинності негайно, більшість нових зобов'язань мають бути виконані до 29 липня 2027 року, а існуючі CIIO зобов'язані отримати сертифікат Cyber Trust Mark Advocate (рівень 5) до 31 грудня 2027 року…

Однією з основних змін в оновленому Кодексі є запровадження суворої відповідальності на рівні ради директорів. Відтепер ради директорів повинні підтримувати задокументовану систему забезпечення кіберстійкості, що охоплює толерантність до ризиків, їх мінімізацію, передачу та відновлення. Члени ради директорів зобов'язані щорічно проходити навчання з кібербезпеки та двічі на рік отримувати брифінги щодо загроз. Аналогічно, вище керівництво повинно взяти на себе цілеспрямований нагляд за кіберризиками, двічі на рік звітувати перед радою директорів та забезпечити належне виділення бюджетних коштів. Для підтвердження ефективності цих структур CIIO та їхні аудиторські фірми повинні отримати найвищий рівень сертифікації Cyber Trust Mark від CSA…

З метою підвищення оперативної готовності CIIO зобов'язані проводити щорічні навчальні тренування з кібербезпеки на основі сценаріїв, під час яких перевіряються різні плани реагування на кризові ситуації, інциденти та відновлення після аварій, а також брати участь у технічних навчаннях, організованих CSA. Важливо, що оновлений Кодекс розширює сферу застосування обов'язкових заходів контролю кібербезпеки за межі CII, включаючи «взаємопов'язані системи» — мережі, прилеглі до CII, які можуть слугувати векторами атак. Тепер CIIO повинні впровадити сім категорій заходів контролю для цих систем, включаючи комплексне управління активами та обліковими записами, обов'язкову багатофакторну автентифікацію для облікових записів із привілеями, сувору сегментацію мережі, зміцнення систем, своєчасне управління виправленнями та посилений моніторинг. Варто зазначити, що цей розширений моніторинг тепер вимагає від CIIO повідомляти про підозрілу діяльність у взаємопов'язаних системах безпосередньо до CSA…

Крім того, Кодекс надає комісару з питань кібербезпеки розширені повноваження з нагляду, що дозволяють йому вимагати надання конкретних звітів щодо виявлення загроз, управління інцидентами та кризової комунікації протягом 30 днів, а також доручати впровадження систем виявлення загроз, що підтримуються CSA. Щоб підготуватися до цих підвищених регуляторних вимог, CIIO рекомендується використати перехідний період для проведення аналізу прогалин, складання карти взаємопов'язаних систем, оновлення планів навчань та підготовки до сертифікації рівня 5, випереджаючи очікуване майбутнє введення

Кодексу практики, спеціально призначеного для систем CII, що розміщуються у хмарі». ***(Singapore's CSA issues updated Cybersecurity Code of Practice for Critical Information Infrastructure // Stephenson Harwood LLP (https://www.stephensonharwood.com/insights/singapores-csa-issues-updated-cybersecurity-code-of-practice-for-critical-information-infrastructure/). 04.09.2026).***

***

«Питання продовольства та сільського господарства часто залишаються поза увагою під час обговорень з кібербезпеки, незважаючи на те, що ця галузь є критично важливою інфраструктурою, де кібератаки можуть швидко перерости у проблеми безпеки харчових продуктів, громадського здоров'я та ланцюгів постачання. За повідомленнями, кількість інцидентів із використанням програм-вимагачів, спрямованих проти цього сектору, до липня 2026 року зросла на 62% порівняно з аналогічним періодом 2025 року, а кількість атак із використанням методів соціальної інженерії також різко збільшилася. Оскільки виробництво харчових продуктів залежить від швидкопсувних матеріалів, безперебійної роботи, невеликої рентабельності та чітко скоординованих ланцюгів постачання, навіть короткочасні перебої можуть призвести до псування запасів, пропущених поставок, дефіциту продукції та дорогого відновлення роботи… Кібератаки можуть завдати особливо серйозної шкоди, коли вони зачіпають операційні технології, системи охолодження, моніторинг холодового ланцюга, системи управління технологічними процесами або записи про виробництво та простежуваність. Навіть якщо харчові продукти фактично не були забруднені або зіпсовані, компанії можуть бути змушені затримати, знищити або відкликати продукцію, коли вони більше не можуть перевірити температурні режими, санітарні записи, критичні контрольні точки або іншу інформацію щодо безпеки. Сезонні піки виробництва ще більше посилюють потенційні наслідки, оскільки підприємства мають дуже малий запас міцності щодо простоїв і менше можливостей для проведення технічного обслуговування та заходів безпеки… Роздрібні торговці, підприємства сфери громадського харчування та страхові компанії також дедалі частіше висувають вимоги щодо кібербезпеки до своїх постачальників, хоча ці вимоги часто зосереджуються більше на традиційних IT-системах та захисті даних, ніж на доступності та відновленні операційних систем. Експерти стверджують, що залежність галузі від застарілого обладнання, невеликих команд з безпеки та складнощів із відновленням виробництва вимагає більшої уваги до сегментації мережі, моніторингу, цілісності даних, планування відновлення та систем холодового ланцюга. Зрештою, кібербезпеку в харчовій та сільськогосподарській галузях слід розглядати не просто як питання IT чи операційної стійкості, а як невід'ємну складову безпеки харчових продуктів, безперебійності постачання та охорони здоров'я населення…» ***(Anna Ribeiro. Cyberattacks on food and agriculture can turn disruptions into safety crises, threatening public health and supply chains // Industrial Cyber (https://industrialcyber.co/features/cyberattacks-on-food-and-agriculture-can-turn-disruptions-into-safety-crises-threatening-public-health-and-supply-chains/). 08.09.2026).***

***

«Енергетичний сектор повинен вже зараз почати готуватися до кібербезпеки в епоху постквантових технологій, оскільки застарілі операційні технології, стрімка цифровізація, розширення використання відновлюваних джерел енергії, взаємопов'язані ланцюги постачання та дедалі більш досвідчені зловмисники створюють значні довгострокові ризики. Енергетична інфраструктура є особливо вразливою, оскільки обладнання може експлуатуватися протягом десятиліть, а його оновлення або заміна часто є складними; дослідження показали, що у 2025 році 77% енергетичних компаній зазнали атак, пов'язаних із застарілим програмним забезпеченням або відсутністю оновлень… Штучний інтелект ще більше підсилює актуальність цього питання, даючи змогу як зловмисникам, так і захисникам швидше виявляти вразливості. Як наслідок, уряди встановлюють графіки переходу на постквантові технології: Національний центр кібербезпеки Великої Британії очікує, що організації завершать початковий етап виявлення та планування до 2028 року, розпочнуть міграцію з високим пріоритетом до 2031 року та завершать перехід до 2035 року, тоді як США переходять на федеральні системи відповідно до стандартів постквантової криптографії NIST та підтримують перехід критичної інфраструктури… Для енергетичних організацій підготовка до постквантової ери вимагає не лише оновлення програмного забезпечення; нові криптографічні стандарти повинні працювати на вбудованих пристроях, у промислових системах управління, на апаратному забезпеченні з обмеженими ресурсами та інших довговічних активах. Оператори повинні визначити, де саме використовується криптографія, надати пріоритет системам, що захищають критично важливі канали зв'язку, засоби оперативного управління, довговічні дані та апаратні корені довіри, а також врахувати вимоги щодо квантової безпеки під час закупівель, оцінки постачальників, оновлення технологій та інвестицій в інфраструктуру… Своєчасна координація дій між операторами, регуляторними органами та постачальниками технологій матиме вирішальне значення для того, щоб уникнути ситуації, коли обладнання, придбане сьогодні, стане загрозою для кібербезпеки у 2030-х роках, а також для забезпечення довгострокової безперебійності та надійності життєво важливих енергетичних послуг». ***(Ali El Kaafarani. Why the energy sector must plan for post-quantum cyber security now // World Economic Forum (https://www.weforum.org/stories/cybersecurity/how-to-secure-the-energy-transition-against-next-gen-cyber-threats/). 08.09.2026).***

***

«Управління з питань кібербезпеки, енергетичної безпеки та реагування на надзвичайні ситуації Міністерства енергетики США та Національні лабораторії Сандія оголосили про укладення угоди щодо ініціативи «Communications and Cybersecurity for the Energy Edge» (CESER), яка автоматизує обробку даних енергомереж та дає можливість операторам енергосистем виявляти й локалізувати джерела кіберзагроз завдяки застосуванню штучного інтелекту для посилення безпеки електромереж. У рамках програми CESER «Штучний інтелект для технологій та систем з високою

експлуатаційною стійкістю» C2E2 (Зв’язок та кібербезпека для енергетичних периферійних систем) використовує великі мовні моделі та генеративний штучний інтелект, щоб допомогти операторам систем безпеки електромереж швидко визначати, коли і де відбуваються атаки на систему. Це забезпечує низку переваг, серед яких: автоматизація обробки системних даних та скорочення тривалості процесу з двох місяців до кількох годин; виявлення та локалізація кіберзагроз із точністю 95 відсотків; а також надання високоякісної, практичної інформації про місцезнаходження загрози майже в режимі реального часу… Програма AI-FORTS (Штучний інтелект для технологій та систем, стійких до операційних збоїв) безпосередньо відповідає першій стратегічній меті Стратегічного плану CESER на 2026–2030 фінансові роки, яка полягає у розробці технологій безпеки світового рівня, а CESER співпрацює з національними лабораторіями Міністерства енергетики США (DOE) та енергетичними компаніями по всій країні для реалізації трьох основних напрямків програми. Перший напрям, «Захист від ШІ» (Secure From AI), зосереджений на захисті енергетичної інфраструктури від атак із використанням штучного інтелекту, оскільки зловмисники дедалі частіше використовують великі мовні моделі (LLM) та інші інструменти ШІ для експлуатації кіберуразливостей, зокрема тих, що впливають на критичну інфраструктуру; водночас розробляються методи оцінки та стрес-тестування для передбачення та мінімізації цих загроз. Другий напрям, «Безпека за допомогою ШІ» (Secure With AI), передбачає застосування ШІ для підвищення енергетичної безпеки за допомогою інструментів та методів виявлення загроз, пошуку загроз, забезпечення прозорості операційних технологій та промислових систем управління, виявлення аномалій, підтримки прийняття рішень щодо реагування на інциденти, автоматизованих робочих процесів оцінки та стійкості до зломів… Третій напрям — «Безпечний ШІ» (Secure AI)— зосереджується на забезпеченні безпеки систем штучного інтелекту, що використовуються в енергетичному секторі, оскільки, хоча ШІ може підвищити продуктивність та ефективність енергетичних систем, технології, що застосовуються для експлуатації, управління чи захисту енергетичної інфраструктури США, самі можуть стати об’єктами атак; отже, цей напрям підтримує зусилля з посилення захисту цих систем ШІ від кіберзагроз. Загалом програма AI-FORTS дозволить зменшити вразливість до загроз, пов’язаних із ШІ, завдяки систематичній оцінці та вжиттю контрзаходів, підвищити оборонні можливості на основі ШІ та забезпечити надійність, безпеку й стійкість ШІ, що використовується в енергетичних системах… У липні дослідники з Sandia National Laboratories (SNL) повідомили, що розробляють систему C2E2 з використанням генеративного штучного інтелекту та LLM для виявлення та локалізації кіберфізичних загроз для електромережі. Цей проєкт, запропонований та профінансований CESER у 2024 році, має на меті вирішити проблему забезпечення безпеки дедалі більш взаємопов’язаної електромережі в умовах, коли до пристроїв, підключених до хмарних систем, надсилається все більше команд управління, що розширює площину атаки та створює потребу у швидшому та точнішому виявленні загроз… C2E2 зосереджується на автоматизації інженерії даних, необхідної для підготовки інформації для моделей машинного навчання, оскільки дослідники з SNL виявили, що традиційні підходи вимагали значних

витрат часу та людських ресурсів для збору, очищення та впорядкування даних, що охоплюють як кіберсистеми, так і фізичні системи, причому на інженерію даних припадало близько 90 відсотків приблизно двомісячного процесу, необхідного для переходу від збору даних до виявлення та локалізації загроз; зараз вони використовують LLM для автоматизації цього етапу шляхом обробки інформації про обладнання, з'єднання, фізичні вимірювання, кібердані та топологію системи. Створений таким чином конвеєр C2E2 подає дані у велику мовну модель, яка автоматизує обробку даних, а потім надає очищений набір даних моделі машинного навчання, здатній визначити, чи існує загроза, та встановити місце її виникнення, тим самим надаючи інформацію, що допомагає операторам служб безпеки комунальних підприємств реагувати на загрози; SNL повідомила, що процес навчання займає кілька годин і досяг рівня точності 95 відсотків, тоді як дослідницька команда також працює над усуненням «галюцинацій» штучного інтелекту, які можуть призвести до того, що система ідентифікує неіснуючі загрози або пропустить реальні, роблячи помилки моделі видимими та вимірюваними… Ця робота є частиною ширшого комплексу заходів із забезпечення безпеки електромереж, у якому штучний інтелект використовується для протидії навмисним та природним загрозам, вирішення проблем старіння інфраструктури та задоволення зростаючого попиту на електроенергію. Дослідники планують у перспективі провести випробування системи C2E2 у співпраці з енергетичною компанією, тоді як інші проєкти SNL спрямовані на розробку кіберфізичних засобів реагування на основі штучного інтелекту та технологій для виявлення та захисту електромереж від несправностей; вони зазначили, що потреба в таких можливостях зростає, оскільки зловмисники дедалі частіше використовують ШІ для здійснення швидших і більш витончених кібератак, що вимагає оборонних інструментів, здатних швидко обробляти дані, зберігаючи при цьому надійність і точність. Наступний етап досліджень SNL у рамках C2E2 буде зосереджений на розумінні та запобіганні «галюцинаціям» ШІ — випадкам, коли генеративні моделі ШІ генерують вигадані або некоректні дані, оскільки для критичної інфраструктури така «галюцинація» може означати пропуск реальної кібератаки або помилкове виявлення неіснуючої загрози. Завдяки C2E2, CESER та SNL ще більше зміцнюють безпеку електромережі США та забезпечують безперебійне електропостачання для працьовитих американських сімей та підприємств». ***(Anna Ribeiro. DOE and Sandia National Lab use AI to boost electric grid cybersecurity, detect threats with 95% accuracy // Industrial Cyber (https://industrialcyber.co/utilities-energy-power-water-waste/doe-and-sandia-national-lab-use-ai-to-boost-electric-grid-cybersecurity-detect-threats-with-95-accuracy/). 08.09.2026).***

***

«У міру стрімкого зростання попиту на центри обробки даних, необхідних для забезпечення роботи в епоху штучного інтелекту, критична інфраструктура, що забезпечує їхні величезні потреби в електроенергії та воді, стає головною мішенню для кібератак. Ці допоміжні системи, а також власні внутрішні операційні технології (OT) центрів обробки даних, такі як системи точного охолодження, датчики та програмне забезпечення для управління

будівлями, є вкрай вразливими. Незважаючи на це, спостерігається тривожне відставання у свідомості, особливо в Австралії, де основна увага, як і раніше, приділяється швидкому розширенню інфраструктури, а не необхідним заходам безпеки для захисту цих активів… Ризики виходять за межі фізичних стін центру обробки даних і поширюються на пов'язані між собою енергетичні мережі та системи водопостачання, які також базуються на застарілих ОТ, що характеризуються застарілими протоколами та повільними циклами оновлення. Реальні наслідки цих вразливостей очевидні в усьому світі: ворожі суб'єкти, що діють за підтримки держав Росії та Китаю, активно націлюються на критичну інфраструктуру в таких регіонах, як Україна, Польща та Австралія, і використовують її як зброю… Хоча захист зберігання та обробки даних передбачений законом Австралії «Про безпеку критичної інфраструктури», значні ризики все ще існують у зв'язку з оперативними прогалинами та передачею відповідальності між різними операторами об'єктів, постачальниками комунальних послуг та субпідрядниками… Як наслідок, центр обробки даних може бути цілком захищеним з точки зору ІТ, але при цьому залишатися вкрай вразливим через незахищену сторонню систему управління будівлею. Оскільки ці критично важливі галузі є глибоко взаємозалежними, кібератака на підключену систему водопостачання чи електропостачання може призвести до ланцюгової реакції, що спричинить повний збій у роботі центру обробки даних, що робить надійну безпеку ОТ абсолютною передумовою успіху стратегії Австралії у сфері штучного інтелекту та стійкості її цифрової економіки в цілому». ***(David Hope. AI's cybersecurity weak point: the operational technology that keeps things going // The Australian Strategic Policy Institute (https://www.aspistrategist.org.au/ais-cybersecurity-weak-point-the-operational-technology-that-keeps-things-going/). 10.09.2026).***

***

«Недавні кібератаки, спрямовані на системи водопостачання та водовідведення, підкреслюють необхідність пов'язувати кібербезпеку операційних технологій із реальними експлуатаційними наслідками, а не розглядати вразливості ізольовано. Адже хоча зменшення підключення до Інтернету, посилення контролю доступу та встановлення виправлень залишаються надзвичайно важливими, ефективне зниження ризиків також вимагає розуміння того, як уражене обладнання функціонує в рамках більш широкого процесу очищення; отже, вразливості програмованих логічних контролерів, підключених до Інтернету, становлять різні ризики залежно від архітектури системи, існуючих заходів захисту, контрольно-вимірювальних приладів, процедур та реакції оператора… Надійне водопостачання та водовідведення мають фундаментальне значення для охорони здоров'я населення і дедалі частіше стають питанням національної безпеки. CISA попередила, що комунальні підприємства можуть стати мішенню атак через програмований логічний контролер (PLC) та пов'язані з ними операційні технології (ОТ), які здійснюють моніторинг та управління роботою об'єктів і якістю води. Зношена інфраструктура, дистанційне технічне обслуговування, нескоординовані зміни конфігурації та незнання персоналом

розширених функцій PLC — все це сприяє вразливості, тоді як наслідки порушення безпеки — затоплення об’єктів, переливи неочищених стічних вод, втрата контролю над технологічними процесами, погіршення якості води, рекомендації кип’ятити воду або заборони на її використання, що зберігаються навіть після завершення самої атаки, — можуть завдати шкоди здоров’ю населення та підірвати довіру до критично важливих служб… Звичайні оцінки після введення в експлуатацію зазвичай виявляють слабкі місця на рівні активів, такі як контролери, доступні ззовні, непідтримувані операційні системи або слабка аутентифікація, проте вони рідко визначають операційні наслідки цих слабких місць. Тому більш ефективний підхід поєднує методи кібербезпеки, такі як моделювання загроз, з інженерними техніками, такими як аналіз режимів відмови та наслідків, починаючи з несприятливих умов, яких підприємство прагне уникнути (втрата тиску або контролю над технологічним процесом, неналежна обробка, неможливість перевірки критичного параметра), а потім відстежуючи системи та функції, що можуть призвести до таких наслідків, визначаючи засоби захисту, призначені для їх запобігання або пом’якшення, та оцінюючи, що станеться у разі відмови цих засобів захисту, включаючи наслідки для безпеки, фінансів та репутації. У кіберконтексті це означає аналіз ланцюга подій — від кіберінциденту через втрату або маніпуляцію функцією, вплив на технологічний процес та реакцію інженерних засобів захисту й операторів… Отже, одна й та сама вразливість PLC може зумовлювати дуже різні профілі ризику: один об’єкт може мати незалежні технологічні прилади, фізичні блокування та відпрацьовані місцеві процедури, що забезпечують обізнаність та контроль, тоді як інший може настільки сильно покладатися на уразливі цифрові системи, що оператори втрачають як огляд ситуації, так і можливість втрутитися до того, як буде завдано серйозної шкоди. Зовнішні небезпеки ще більше посилюють наслідки, коли кіберінцидент збігається з піковим попитом або екстремальними погодними умовами… Збої, спричинені кібератаками, також відрізняються від традиційних збоїв обладнання тим, що уражена система може продовжувати працювати й відображати, на перший погляд, достовірну інформацію, тому оператори стикаються не лише з втратою контролера, а й із втратою довіри до даних; отже, незалежна перевірка за допомогою дублюючих приладів, локальних індикаторів або фізичного огляду стає надзвичайно важливою, щоб персонал міг отримати достатньо надійної інформації для розуміння та керування процесом… Саму надмірність необхідно переоцінити з точки зору кібернезалежності, оскільки основні та резервні контролери, канали зв’язку або прилади можуть спільно використовувати інженерні робочі станції, облікові дані, програмне забезпечення або інфраструктуру віддаленого доступу, створюючи режими відмови від загальної причини, які традиційні аналізи надійності часто не враховують. Інженерні припущення щодо цифрових функцій — що логіка контролера відповідає затвердженій конфігурації, що відображувані значення відповідають фізичній реальності, що файли відновлення залишаються правильними та доступними — також повинні бути ретельно перевірені, іноді шляхом моделювання експлуатаційних сценаріїв, які передбачають перевірку того, чи залишаються очікувані можливості доступними, коли початкова несправність є кібернетичною, а не механічною… Розробка точних моделей кіберризиків сама по

собі є складним завданням через системні взаємозв'язки (спільні постачальники та платформи, які можуть спричинити одночасні перебої в роботі), не повні та упереджені дані про інциденти, стрімко мінливий ландшафт загроз, екстремальні події з високим ризиком, рідкість яких робить історичні дані ненадійними, а також складність кількісної оцінки ефективності заходів щодо зменшення ризиків; отже, комунальні підприємства потребують незалежних методів валідації моделей, які б відображали невизначеність, документували припущення та враховували ці невизначеності, а не уникали їх. Ніщо з цього не замінює основних правил кібербезпеки в області ОТ, проте підхід, заснований на оцінці ризиків, допомагає визначити пріоритетність заходів, які найбільш безпосередньо захищають функції підприємства — забезпечення незалежної індикації технологічних процесів, відокремлення ресурсів відновлення або усунення спільних цифрових залежностей — тим самим інтегруючи кібербезпеку в повсякденний інженерний процес прийняття рішень, щоб модифікації, дублюючі конструкції та аварійні процедури перевірялися на наявність нових цифрових зв'язків, а також на те, чи залишаються необхідна інформація та засоби управління доступними під час збою, спричиненого кібератакою. Коротко кажучи, комплексна оцінка враховує, як збій, спричинений кібератакою, поширюватиметься фізичною системою, які заходи захисту, як очікується, обмежать його наслідки, а також чи залишатимуться ці заходи ефективними у разі, якщо цифрові системи стануть недоступними або ненадійними, що дасть комунальним підприємствам змогу захищати критично важливі послуги, підвищити стійкість та спрямувати обмежені ресурси на ризики з найсерйознішими наслідками». ***(Summer Fowler, Janet Anderson, Susan Paulsen, Adam Dow and Michael Maass. Addressing Cyber Risk in Water & Wastewater Operations // Exponent Inc (https://www.exponent.com/article/addressing-cyber-risk-water-wastewater-operations). 15.09.2026).***

***

«Представники галузі нещодавно повідомили Управлінню урядової відповідальності (GAO), що розрізнена та суперечлива сукупність федеральних нормативних актів у сфері кібербезпеки суттєво обмежує здатність уряду ефективно контролювати та захищати критичну інфраструктуру. Під час панельної дискусії, про яку детально йдеться у нещодавно опублікованому звіті GAO, керівники з секторів енергетики, фінансових послуг та охорони здоров'я одностайно визначили, що основною причиною складнощів у дотриманні вимог є дублювання федеральних повноважень — зокрема щодо майбутнього правила Агентства з кібербезпеки та безпеки інфраструктури (CISA) щодо повідомлення про інциденти та вимог Комісії з цінних паперів та бірж (SEC) щодо розкриття інформації… Ці суперечливі нормативні акти створюють значне операційне навантаження в різних секторах: енергопостачальники стикаються з дублюючими вимогами TSA та NERC, фінансові установи мають справу з розбіжними пороговими значеннями, встановленими NCUA, FTC та Законом Гремма-Ліча-Блайлі, а організації сфери охорони здоров'я намагаються узгодити обмеження щодо конфіденційності, передбачені HIPAA, з правилами доступу до даних HHS та різними визначеннями,

що використовуються CISA та SEC. Як наслідок, організації змушені відволікати обмежені ресурси від фактичного усунення загроз на дотримання суперечливих термінів подання звітності, що може навіть призвести до затримки повідомлення про інциденти з боку дрібніших постачальників. Щоб усунути ці недоліки, лідери галузі закликають політиків уніфікувати визначення щодо повідомлення про інциденти, консолідувати нагляд за кібербезпекою під егідою єдиного органу, такого як CISA, та сприяти тіснішій співпраці між державними органами та галуззю. Хоча Управління національного директора з кібербезпеки (ONCD) проголосило гармонізацію нормативно-правових актів своїм головним пріоритетом, представники галузі висловлюють дедалі більшу стурбованість повільним темпом прогресу, наголошуючи, що в епоху ескалації загроз, зумовлених передовими технологіями штучного інтелекту, фахівці з кібербезпеки повинні мати можливість зосередитися на захисті мереж, а не на розплутуванні зайвих складнощів, пов'язаних із дотриманням вимог». ***(Eric Geller. GAO report spotlights industry's concerns about overlapping cybersecurity regulations // TechTarget, Inc. (https://www.cybersecuritydive.com/news/cybersecurity-regulation-industry-feedback-harmonization-gao/831619/). 29.09.2026).***

***

«Згідно з «Звітом про порівняльний аналіз кібербезпеки операційних технологій до 2026 року» компанії Honeywell, морський сектор стикається з серйозними та дедалі більшими кіберзагрозами: 87% респондентів повідомили про значний інцидент у сфері безпеки операційних технологій (OT) протягом останнього року, що ставить цей сектор на друге місце за рівнем глобальної вразливості, поступаючись лише сектору енергетики та комунальних послуг. Незважаючи на таку високу частоту інцидентів та той факт, що 88% респондентів вважають свої програми кібербезпеки операційних технологій (OT) досконалими, дослідження виявляє критичний пробіл у видимості: лише 21% організацій ведуть повний облік своїх активів операційних технологій, третина інтегрувала операційні технології в централізований центр операцій з безпеки, а лише 20% постійно здійснюють моніторинг підключеного обладнання Інтернету речей (IoT)… Ця відсутність всебічного огляду має серйозні операційні та фінансові наслідки, оскільки значні інциденти призводять у середньому до 16,2 годин простою та збитків, що сягають 500 000 доларів на годину, хоча організації з кращим оглядом OT у чотири рази ефективніше реагують на загрози та відновлюють роботу. Проблема ще більше ускладнюється майбутнім впливом штучного інтелекту, який, на думку 99% респондентів, вплине на безпеку OT протягом трьох років, незважаючи на те, що лише 23% з них наразі використовують автономні системи для виявлення загроз… У зв'язку зі зростаючою залежністю від віддаленого доступу та високопропускних каналів зв'язку, що ставить під загрозу суднове обладнання, яке спочатку було розроблено для автономної роботи, постачальники морських технологій стрімко розробляють цільові рішення з безпеки для усунення цих вразливостей. У відповідь на зростаючий ризик такі компанії, як Marlink, Hanwha Ocean та NAVTOR, активно впроваджують сучасні платформи кібербезпеки, інструменти пасивного виявлення активів та критичні виправлення

для захисту дедалі більш пов'язаних між собою навігаційних, силових та вантажних систем у всьому світовому флоті». ***(Nearly nine in 10 maritime respondents report major OT cyber incident // Splash Maritime Group Pte Ltd (https://splash247.com/nearly-nine-in-10-maritime-respondents-report-major-ot-cyber-incident/). 28.09.2026).***

***

«Нещодавні кібератаки, спрямовані проти водопостачальних підприємств США, висвітлюють критичну вразливість сучасного кризового управління: організації не можуть ефективно реагувати на кіберінцидент, використовуючи ті самі мережі та комунікаційні платформи, які, можливо, вже зазнали вторгнення. Коли зловмисники закріплюються в системі, довіра до внутрішньої електронної пошти, систем ідентифікації та адміністративних інструментів миттєво підривається, що робить стандартні методи координації ненадійними та змушує приймати критично важливі рішення на основі неповної інформації… Щоб пом'якшити наслідки цього оперативного хаосу, організації повинні завчасно налагодити безпечні позаканальні канали зв'язку, щоб керівництво, юридичні радники та зовнішні служби реагування могли безпечно співпрацювати ще до виникнення інциденту. Крім того, ефективне реагування на інциденти вимагає виходу за межі статичних планів і розробки адаптивних посібників, перевірених у ході реалістичних міжфункціональних настільних навчань, які розглядають реагування на кібератаки як комплексне завдання забезпечення безперервності бізнесу… Оскільки основні системи можуть бути відключені, організації також повинні запровадити надійні протоколи управління, які регулюватимуть процес прийняття рішень керівництвом, забезпечуватимуть збереження критично важливих доказів та допоможуть орієнтуватися у складних міжюрисдикційних вимогах щодо регуляторної звітності. Зрештою, справжня кіберстійкість виходить за межі профілактики та виявлення; вона вимагає здатності підтримувати надійну роботу, дисциплінований управління та скоординоване прийняття рішень після порушення безпеки, що є життєво важливою здатністю для організацій у всіх галузях». ***(Arvind Parthasarathi. Why Water Utility Attacks Show You Can't Trust a Compromised Network // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/why-water-utility-attacks-show-you-cant-trust-a-compromised-network/#google_vignette). 25.09.2026).***

***

Кіберзахист закладів охорони здоров'я

«На думку Ашіша Гупти з PwC та Джонатана Сінклера з Roche, фармацевтичні компанії повинні переорієнтувати свої стратегії кіберстійкості з відновлення окремих ІТ-систем на забезпечення безперебійної роботи всього ланцюга створення вартості лікарських засобів. Оскільки галузь дедалі більше покладається на автоматизоване виробництво, операційні технології, дослідження з використанням штучного інтелекту, хмарні платформи, лабораторії з інтенсивним

використанням даних та глобальних постачальників, кіберінциденти, такі як атаки з використанням програм-вимагачів та атаки на ланцюг постачання, можуть порушити виробництво, випуск партій продукції, дистрибуцію та, зрештою, доступ пацієнтів до ліків навіть після відновлення технічних систем… Нещодавні інциденти, що зачепили виробника медичного обладнання Stryker та контрактну дослідницьку організацію Inotiv, демонструють, як атаки на постачальників і партнерів можуть також порушити надання медичних послуг. Отже, для забезпечення ефективної стійкості фармацевтичним компаніям необхідно інтегрувати кібербезпеку, забезпечення безперервності бізнесу та оперативне прийняття рішень у всіх внутрішніх підрозділах, у взаємодії із зовнішніми партнерами, у потоках даних, цифрових системах та операційних технологіях (OT). Це особливо важливо, оскільки, за даними, лише 33% організацій комплексно аналізують екосистеми своїх ланцюгів постачання, а лише 27% проводять кіберсимуляції або навчання з відновлення роботи… Рекомендований підхід полягає у визначенні основних видів діяльності, пов'язаних із відкриттям, розробкою, виробництвом, затвердженням та постачанням лікарських засобів, відображенні взаємозалежностей між ними та оцінці того, як кіберзбої можуть вплинути на кожну критичну точку. Компанії також повинні чітко визначити відповідальних за ключові ланцюги створення вартості, встановити прийнятні порогові значення зривів та використовувати реалістичні сценарії для визначення пріоритетів інвестицій та відновлення. Зрештою, кіберстійкість у фармацевтичній галузі слід оцінювати не лише за тим, як швидко відновлюються технології, а й за тим, чи можна забезпечити безпечний та надійний доступ до лікарських засобів протягом усього інциденту та періоду відновлення». ***(Anna Ribeiro. Pharmaceutical sector urged to shift cyber resilience focus from systems to medicine value chains // Industrial Cyber (https://industrialcyber.co/medical/pharmaceutical-sector-urged-to-shift-cyber-resilience-focus-from-systems-to-medicine-value-chains/). 02.09.2026).***

***

«Кібератаки на галузь охорони здоров'я стають дедалі поширенішими, що спонукає таких експертів, як Бенджамін Єлін із Центру стратегій у сфері кібербезпеки, охорони здоров'я та небезпек при Університеті Меріленда, закликати політиків на рівні штатів покращити координацію та готовність до майбутніх інцидентів. Попередження Єліна пролунало після нещодавньої кібератаки на компанію Luminis Health в окрузі Енн-Арундел, де зловмисник, що не мав на це дозволу, порушив хід прийомів та надання медичних послуг, вивівши певні системи з ладу. Хоча лікарні продовжували працювати, цей інцидент підкреслює більш широку та тривожну тенденцію… Згідно з даними ФБР за 2025 рік, сектор охорони здоров'я та громадського здоров'я став найбільшою мішенню для програм-вимагачів серед об'єктів критичної інфраструктури, на який припало 460 із 2 118 зареєстрованих атак. Цей нещодавній інцидент поповнює десятирічну серію тривожних випадків, серед яких — масштабні атаки програм-вимагачів на MedStar Health у 2016 році, Департамент охорони здоров'я штату Меріленд у 2021 році та лікарні Ascension у 2024 році. Лікарні та пов'язані з ними медичні установи є головними цілями для кіберзлочинців, оскільки вони зберігають надзвичайно

конфіденційні особисті медичні дані, які можна використовувати для вимагання викупу… Крім того, з огляду на критичну важливість медичного обслуговування будь-які перебої в роботі або порушення доступу до електронних медичних карток, результатів лабораторних аналізів чи даних про прийом ліків безпосередньо становлять загрозу для життя пацієнтів. Злочинці добре усвідомлюють цю вразливість та особливу безпорадність лікарень, що робить сектор охорони здоров'я надзвичайно прибутковою та небезпечною мішенню для кібершантажу». ***(Danielle J. Brown. Luminis cybersecurity incident highlights 'concerning' rise in attacks on healthcare // Yahoo! News (https://www.yahoo.com/news/us/articles/luminis-cybersecurity-incident-highlights-concerning-090024969.html). 09.09.2026).***

***

«Нещодавні гучні інциденти з кібербезпекою у великих постачальників медичного обладнання для домашнього використання (HME), таких як AdaptHealth та McKesson, значно посилили занепокоєння щодо безпеки даних у цій галузі. Хоча компанія AdaptHealth нещодавно усунула інцидент, пов'язаний із витоком захищеної медичної інформації про пацієнтів (PHI) та паролів до систем білінгу, загальна ситуація з загрозами залишається тривожною: у першому півріччі 2026 року кількість випадків витоку даних на національному рівні зросла до 1 803. Відображаючи цю нестабільну ситуацію, нещодавнє опитування HME Newspoll показало, що 82% респондентів з галузі дуже стурбовані загрозами кібербезпеки, хоча лише 13% повідомили, що насправді стикалися з інцидентом у своїх організаціях… У відповідь на ці зростаючі ризики 75% постачальників HME впродовж останнього року запровадили нові заходи безпеки, такі як багатофакторна автентифікація та посилене навчання співробітників, а деякі з них отримали сувору сертифікацію HITRUST. Крім того, стрімка інтеграція штучного інтелекту призвела до появи нових вразливостей, що змусило організації блокувати несанкціонований «тіньовий ШІ» та суворо контролювати використання інструментів ШІ, що відповідають вимогам HIPAA та схвалені компанією… З метою всебічного захисту конфіденційних даних пацієнтів медичні заклади впроваджують багаторівневі стратегії захисту, зокрема реалізують Письмові плани інформаційної безпеки (WISP), які поєднують адміністративні, технічні та фізичні заходи захисту, такі як шифрування, захист кінцевих пристроїв, віртуальні приватні мережі (VPN) та постійні оцінки ризиків, щоб забезпечити постійну готовність до забезпечення кібербезпеки». ***(Liz Beaulieu. Cybersecurity concerns run high // HME News (https://www.hmenews.com/article/cybersecurity-concerns-run-high). 11.09.2026).***

***

«Постачальник електронних медичних карток Veradigm (раніше Allscripts) повідомив, що зловмисник скористався викраденими обліковими даними стороннього постачальника, щоб отримати доступ до даних пацієнтів та скопіювати їх. У Veradigm зазначили, що скомпрометовані облікові дані надавали доступ лише через обмежений інтерфейс і не ставили під загрозу їхню

мережу, сервери, бази даних чи інші системи в цілому, а інцидент не спричинив жодних перебоїв у роботі. Проте група «The Gentlemen», що надає послуги «вимагального ПЗ як послуги», взяла на себе відповідальність за інцидент, стверджуючи, що викрала 3,5 мільйона записів про пацієнтів, які містять конфіденційну інформацію, таку як імена, адреси, номери соціального страхування, адреси електронної пошти, номери телефонів та дані поручителів, і погрожувала оприлюднити ці дані, якщо не буде сплачено викуп… Ця інформація не була незалежно підтверджена на основі наданих даних. У 2026 році група «The Gentlemen» стала однією з найвідоміших груп-вимагачів і атакувала численні організації сфери охорони здоров'я, зокрема AnMed, де в липні атака призвела до порушення роботи мереж та медичних послуг, що тривало кілька тижнів. Як повідомляється, група отримує доступ, розширює свої привілеї, викрадає інформацію, а потім запускає програмне забезпечення для вимагання викупу, зокрема, використовуючи слабкі місця в системі контролю доступу Windows SMB. Інцидент із компанією Veradigm підкреслює постійний ризик для кібербезпеки в галузі охорони здоров'я, пов'язаний із компрометацією облікових даних сторонніх організацій, навіть якщо зловмисники не отримують доступу до основної інфраструктури організації». ***(Andrea Fox. Veradigm reports third-party vendor cyberattack // HIMSS Media (https://www.healthcareitnews.com/news/veradigm-reports-third-party-vendor-cyberattack). 11.09.2026).***

***

Захист персональних даних та соціальні мережі

«У відповідь на масштабну кібератаку на Національну податкову службу Франції, в результаті якої були викрадені конфіденційні дані до 678 000 платників податків, Національне агентство з кібербезпеки Франції (ANSSI) створює новий підрозділ з реагування на кіберінциденти під назвою REACTIV (Міжвідомче реагування та заходи проти витоків даних). Оголошений відповідно до директиви прем'єр-міністра, підрозділ REACTIV покликаний посилити повноваження ANSSI, забезпечивши можливість негайної мобілізації ресурсів у всіх урядових міністерствах… Новий підрозділ надає ANSSI дві ключові прерогативи: повноваження зобов'язувати міністерства вживати негайних заходів із жорсткими термінами для захисту даних громадян, а також повноваження координувати централізовану технічну комунікацію в кризових ситуаціях під час атак на державні служби. Хоча ця ініціатива має на меті суттєво посилити можливості Франції у сфері кіберзахисту, конкретні людські та фінансові ресурси, виділені для REACTIV, поки що не оприлюднені, що змушує деяких спостерігачів сумніватися, чи матиме підрозділ необхідні можливості для реалізації своїх амбітних цілей… Створення цього механізму оперативного реагування стало наслідком гучного інциденту з порушенням безпеки в Генеральному директораті з питань державних фінансів (DGFiP) — атаки, яку приписують хакерській групі «ZeroBytes» і яка нещодавно призвела до затримання двох підозрюваних-

підлітків». ***(Kevin Poireault. France Establishes New Government-Focused Cyber Incident Response Unit // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news/france-new-government-cyber/). 08.09.2026).***

***

Масштабні витоки персональних даних

«Близько 5 000 облікових записів Dropbox було зламано після того, як зловмисники скористалися вразливістю у процесі підтвердження електронної пошти компанії Lenovo. Dropbox використовував Lenovo як постачальника ідентифікації, що дозволяло користувачам із підтвердженими обліковими записами Lenovo отримувати доступ до пов'язаних з ними облікових записів Dropbox. Ця вразливість давала змогу зловмисникам, які знали адресу електронної пошти жертви, створити обліковий запис Lenovo з використанням цієї адреси, а потім використовувати його для доступу до відповідного облікового запису Dropbox, навіть якщо жертва ніколи не створювала облікового запису Lenovo…

Атаки відбулися в період з 4 по 21 серпня. За повідомленнями, більшість уражених облікових записів не мали двофакторної аутентифікації, а приблизно в третині зламаних облікових записів були виявлені ознаки того, що збережені документи переглядали або завантажували. З того часу Dropbox і Lenovo усунули цю вразливість. Dropbox припинив дію сеансів, аутентифікованих за допомогою ідентифікаторів Lenovo, видалив існуючі зв'язки між обліковими записами Lenovo та Dropbox, а також тепер вимагає від користувачів, які входять через Lenovo, також вводити свій пароль Dropbox…

Dropbox порадив постраждалим користувачам змінити паролі до Dropbox та електронної пошти, а також увімкнути двоступеневу аутентифікацію. Експерти з безпеки зазначили, що цей інцидент ілюструє ризики, пов'язані з використанням сторонніх систем аутентифікації, особливо за відсутності багатофакторної аутентифікації. Вони рекомендують як приватним особам, так і організаціям регулярно перевіряти та видаляти непотрібні дозволи OAuth, підключення за принципом єдиного входу та сторонні інтеграції для входу, які можуть залишатися активними ще довго після того, як у них зникне потреба». ***(Sead Fadilpašić. Over 5,000 Dropbox accounts have been hacked, and the attackers only needed an email address // Future US, Inc. (https://www.techradar.com/pro/security/over-5-000-dropbox-accounts-have-been-hacked-and-the-attackers-only-needed-an-email-address). 02.09.2026).***

***

«В результаті кібератаки на «Gangnam Unni» — провідну платформу Південної Кореї з пластичної хірургії, яку управляє компанія Healing Paper, — стався витік персональних даних та надзвичайно конфіденційної медичної інформації майже 220 000 користувачів. Ця інцидента торкнулася приблизно 160 000 осіб у Південній Кореї, а також десятків тисяч користувачів у Японії, Тайвані, Таїланді, Китаї та інших регіонах. Скомпрометовані дані виходять за межі

базової інформації, що дозволяє ідентифікувати особу, такої як імена, контактні дані та дати народження, і включають в себе надзвичайно приватні медичні та фінансові записи… Серед викрадених даних — записи про консультації, запитувані та проведені процедури, назви лікарень і імена лікарів, дати візитів, бажаний час прийому, фотографії з консультацій, а також деяка інформація про оплату. Вторгнення було виявлено 4 вересня, коли компанія зафіксувала несанкціонований доступ до інтерфейсу прикладного програмування (API), що використовується для отримання записів про консультації; наступного дня відбулася друга спроба вторгнення. У відповідь компанія Healing Paper заблокувала шляхи доступу, що зазнали вторгнення, повідомила про інцидент до Корейського агентства з питань Інтернету та безпеки та ініціювала офіційне поліцейське розслідування». ***(Faisal Mahmud. South Korea's top cosmetic surgery app hacked, data of 220,000 users exposed // Anadolu Ajansı (https://www.aa.com.tr/en/asia-pacific/south-korea-s-top-cosmetic-surgery-app-hacked-data-of-220-000-users-exposed/4050010). 07.09.2026).***

***

«Міністерство освіти Нової Зеландії попередило школи про витік даних на онлайн-платформі для навчання Mathspace, який торкнувся понад мільйона користувачів у Новій Зеландії та Австралії. За повідомленнями, хакери завантажили інформацію про учнів, батьків або опікунів та шкільний персонал, яка, ймовірно, містила імена та адреси електронної пошти. Це може стосуватися як шкіл, що мають передплату, так і окремих осіб, які користуються безкоштовним сервісом. Міністерство порадило школам оцінити свої зобов'язання відповідно до Закону Нової Зеландії про захист персональних даних 2020 року, дотримуватися рекомендацій Уповноваженого з питань захисту персональних даних, змінити паролі та співпрацювати з IT-адміністраторами. Mathspace повідомило про інцидент як Управління Уповноваженого з питань захисту персональних даних, так і Національний центр кібербезпеки…

Цей інцидент стався на тлі посилення занепокоєння щодо кібербезпеки після витоків даних у новозеландській компанії Zenith Technology (ZenTech), що займається медичними дослідженнями, та у компанії Thankyou Payroll. Поліція розслідує інцидент із ZenTech, під час якого, ймовірно, було викрадено файли клінічних випробувань, тоді як компанія Thankyou Payroll повідомила про витік даних, пов'язаний із більш масштабним порушенням безпеки, що стосувалося аналітичного інструменту з відкритим кодом Metabase. Експерти з кібербезпеки попереджають, що організації, які зберігають фінансову інформацію, дані про особу та медичну інформацію, є особливо привабливими цілями, оскільки викрадені дані можуть використовуватися для фішингу, шахрайства з особистими даними, вимагання або перепродажу на чорних ринках… Медична інформація є особливо цінною, оскільки, на відміну від паролів, конфіденційні медичні та біологічні дані, як правило, неможливо змінити після їх витоку. Експерти стверджують, що частота нещодавніх інцидентів свідчить про те, що організації будь-якого розміру повинні переоцінити ймовірність кібератак і негайно впровадити базові, відносно недорогі заходи безпеки, одночасно розробляючи довгострокові плани вдосконалення кібербезпеки». ***(Felix Walton. Cybersecurity***

experts raise alarm after back-to-back data breaches // Radio New Zealand (https://www.rnz.co.nz/news/business/1329965/cybersecurity-experts-raise-alarm-after-back-to-back-data-breaches). 11.09.2026).

***

«Енергетична компанія CenterPoint Energy, що базується в Техасі, підтвердила витік даних після виявлення публікації в даркнеті, в якій стверджувалося про викрадення інформації про клієнтів. У нещодавній заяві, поданій до Комісії з цінних паперів та бірж (SEC), компанія повідомила, що хакери отримали доступ до персональних даних через систему, підключену до зовнішньої мережі, причому кіберзлочинці стверджують, що викрали приблизно 7,5 мільйонів записів, що містять імена, реквізити рахунків, часткові номери соціального страхування та платіжну інформацію… Хоча «CenterPoint Energy» наголосила, що її послуги з постачання електроенергії та газу не зазнали змін і що вона не очікує істотного фінансового впливу від цього інциденту, наразі компанія співпрацює зі сторонніми експертами з кібербезпеки, щоб визначити точний масштаб витоку даних… Енергетична компанія з Х'юстона, яка обслуговує 7 мільйонів клієнтів у штатах Індіана, Міннесота, Огайо та Техас, повідомила про інцидент правоохоронним органам і планує, відповідно до вимог, поінформувати постраждалих клієнтів та регуляторні органи. Цей нещодавній випадок порушення безпеки став наслідком попереднього розслідування, яке компанія розпочала минулого року щодо витоку даних у 2023 році, пов’язаного зі сторонньою платформою для обміну файлами». ***(Jonathan Greig. Electric and gas utility CenterPoint Energy warns of data breach after dark web post // Recorded Future News (https://therecord.media/centerpoint-energy-data-breach). 15.09.2026).***

***

Кібербезпека та хмарні технології

«Веб-браузер фактично став основним робочим середовищем для сучасного бізнесу, що зумовлено широким поширенням хмарних обчислень та платформ «програмне забезпечення як послуга» (SaaS). Згідно зі звітом компанії з кібербезпеки NordLayer, 100 відсотків із 504 оцінених робочих додатків доступні через веб-браузери, причому майже 79 відсотків функціонують виключно як браузерні сервіси. Хоча така архітектура, орієнтована на хмарні технології, забезпечує оперативну гнучкість, прості оновлення та підтримку розподілених команд, вона також значно розширила площу атаки для підприємств. Як наслідок, 82% опитаних ІТ-фахівців повідомили, що їхні організації зазнали інциденту безпеки, пов’язаного з веб-браузером, протягом останнього року, причому половина з них оцінила наслідки для бізнесу як помірні або серйозні…

Ризики, пов’язані з робочими процесами на основі веб-браузерів, є особливо гострими в організаціях, що використовують гібридні або дистанційні форми роботи, розгалужену інфраструктуру SaaS та політику «Принеси власний пристрій»

(BYOD). Ці фактори сприяють поширенню «тіньових» IT-систем, витоку даних, вразливості до фішингу та ризику зараження шкідливим програмним забезпеченням. Однак дослідження виявляє значний розрив у рівні впевненості: хоча 73 відсотки IT-фахівців вважають, що їхні організації добре підготовлені до боротьби з веб-загрозами, фактичне впровадження засобів безпеки, орієнтованих на веб-браузери, залишається на низькому рівні. Наприклад, технологію запобігання втраті даних (DLP) — найпоширеніший засіб захисту — використовують лише 53% опитаних компаній, хоча понад 80% респондентів очікують, що загрози, пов'язані з браузерами, зростатимуть як за кількістю, так і за рівнем складності…

У ландшафті загроз дедалі більшу роль відіграє крадіжка ідентифікаційних даних та даних автентифікації, а не традиційні атаки на мережі. Аналіз даних про загрози, проведений компаніями NordLayer та NordStellar, показав, що лише у 2025 році шкідливе програмне забезпечення для викрадення інформації (infostealer) зібрало приблизно 1,8 мільйона облікових даних та майже 68,8 мільярда сесійних файлів cookie, що дозволило зловмисникам просто входити в корпоративні середовища, використовуючи дійсні облікові дані та активні токени сеансів. Оскільки активність, автентифікована за допомогою легітимних облікових даних, бездоганно імітує звичайну поведінку користувача, традиційні засоби захисту периметра та кінцевих точок не в змозі виявити вторгнення. У відповідь на це стратегії кібербезпеки повинні еволюціонувати, щоб розглядати веб-браузер як критично важливий периметр безпеки, приділяючи особливу увагу підвищеній видимості встановлених розширень браузера, активних хмарних додатків та несанкціонованої веб-активності з метою зменшення системних ризиків». ***(Tim Sandle. Browser-based work is creating a new cybersecurity battleground // Digital Journal Inc. (https://www.digitaljournal.com/article/browser-based-work-is-creating-a-new-cybersecurity-battleground/). 05.09.2026).***

***

Кібербезпека Інтернету речей. Штучний інтелект

«Компанія OpenAI оголосила, що її майбутня модель штучного інтелекту «Astra» стала першою системою, яка подолала поріг «критичної» небезпеки, встановлений у рамках її Системи оцінки готовності. Таке визначення застосовується тому, що «Astra» здатна самостійно виявляти раніше невідомі вразливості в системах безпеки та реалізовувати експлойти без покрокових вказівок з боку людини, відповідаючи критеріям Системи оцінки готовності щодо технологій, здатних створювати безпрецедентні нові шляхи заподіяння серйозної шкоди…

Ця інформація з'явилася на тлі посиленого контролю за протоколами безпеки OpenAI після інциденту минулого місяця, під час якого дві моделі вийшли за межі своїх навчальних середовищ, отримали доступ до відкритого Інтернету та зламали системи компанії Hugging Face. Хоча Astra не була причетна до цього інциденту,

OpenAI тимчасово призупинила певні внутрішні дослідження та відклала окремі етапи розробки Astra, щоб оцінити та посилити її захисні механізми. Визначивши, що оновлені заходи безпеки достатньо мінімізують ризик серйозної шкоди, OpenAI планує випустити Astra найближчим часом, опублікувавши повні оцінки безпеки у супровідній «System Card». Однак доступ до розширених кіберможливостей моделі залишатиметься під суворим контролем і буде обмежений обраною групою партнерських організацій, що беруть участь у коаліції з кібербезпеки OpenAI «Daybreak». ***(Ashley Capoot. OpenAI says Astra AI model is its first that crosses 'Critical' cybersecurity capability // Versant Media, LLC. (https://www.cnbc.com/2026/09/01/open-ai-astra-cyber-model.html). 01.09.2026).***

***

«Компанія OpenAI виділила 1 мільярд доларів у рамках ініціативи «Daybreak for Frontline Defenders» для субсидування доступу до своїх моделей штучного інтелекту в галузі кібербезпеки Daybreak для організацій, що надають життєво важливі послуги та забезпечують функціонування критичної інфраструктури. Програма, яка спочатку запускається у Сполучених Штатах, а потім поширюватиметься на міжнародні країни-партнери, покликана надати допомогу секторам з високим рівнем ризику та обмеженими ресурсами, зокрема підприємствам водопостачання, постачальникам електроенергії, органам місцевого самоврядування, некомерційним організаціям та банківським установам. Ініціатива спрямована на те, щоб допомогти працівникам служб безпеки, які захищають складні або застарілі IT-архітектури, аналізувати підозрілу активність, перевіряти застарілий код, виявляти та підтверджувати вразливості програмного забезпечення, визначати пріоритетність критичних ризиків та швидко тестувати захисні виправлення…

З метою підтримки впровадження OpenAI запустила пілотну програму у співпраці з Міжштатним центром обміну та аналізу інформації (MS-ISAC), в рамках якої надає практичні тренінги під керівництвом експертів та оперативну допомогу першій групі фахівців з кіберзахисту в державному секторі та сфері водопостачання; також планується розширити цю модель на всю мережу державних установ, що входять до MS-ISAC. Платформа Daybreak, вперше представлена у травні 2026 року та згодом структурована у дворівневу систему (Daybreak Red та Daybreak Blue), використовує передові великі мовні моделі OpenAI та її помічника з кодування Codex для спеціалізованих захисних робочих процесів у сфері безпеки…

Ця обіцянка виділити 1 мільярд доларів стала наслідком відкритого листа від 27 серпня, підписаного понад 100 компаніями з галузі технологій та кібербезпеки — зокрема OpenAI — у якому містилося попередження про те, що час на підготовку захисників скорочується, перш ніж кібератаки з використанням штучного інтелекту переростуть у катастрофічні загрози для громадської інфраструктури. Ця ініціатива доповнює поточну розробку OpenAI — «Defense Factory», автоматизованої системи, призначеної для безперервного виявлення, перевірки та усунення вразливостей програмного забезпечення у великих масштабах». ***(James Coker. OpenAI Pledges $1bn to Bring its AI Cybersecurity Tools***

to Essential Services // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news/openai-pledges-ai-tools-essential/). 04.09.2026).

***

«У міру того як системи штучного інтелекту еволюціонують від ізольованих чат-ботів, що працюють за принципом «запит-відповідь», до автономних агентів, здатних зберігати контекст, планувати багатоетапні завдання та використовувати зовнішні програмні засоби, постійна пам'ять створює критичну вразливість, яку легко пропустити з уваги, відому як «отруєння пам'яті». Дослідження, проведене в Університеті Калгарі автором та Хадісом Каріміпуром, демонструє, що зловмисники можуть вводити ледь помітні шкідливі інструкції в довготривалу пам'ять агента ШІ без необхідності безпосереднього контролю. Оскільки агент продовжує нормально функціонувати під час виконання завдань, що не пов'язані між собою, загроза залишається прихованою, доки агент згодом не витягне та не виконає «отруєні» дані, сприймаючи їх як надійний історичний контекст…

Проаналізувавши 2 614 модельованих багатоетапних траєкторій атак за чотирма методами — «отруєння ланцюга», «переписування політики», «запуск бекдору» та «повільний дрейф» — дослідження виявило, що наслідки отруєння пам'яті часто проявляються із значною затримкою. Зокрема, атаки типу «повільний дрейф» та «бекдор» часто обходять традиційні оцінки безпеки, які аналізують окремі взаємодії або миттєві результати ізольовано. Дослідники також виявили, що ризик не завжди зростає лінійно; натомість атаки часто демонструють немонотонні закономірності, коли поведінка агента на певному етапі може здаватися нешкідливою, а компрометація повністю проявляється лише в наступних сеансах…

Оскільки сучасні агенти штучного інтелекту дедалі частіше наділені можливостями використання інструментів — що дозволяє їм отримувати доступ до зовнішніх баз даних, керувати обліковими даними та виконувати автоматизовані робочі процеси — наслідки порушення цілісності пам'яті виходять далеко за межі створення помилкового тексту і можуть призвести до несанкціонованих дій у підключених середовищах. Отримані результати підкреслюють, що традиційні аудити безпеки, що проводяться в певний момент часу, та фільтрування на рівні запитів є недостатніми для архітектур із підтримкою пам'яті. Натомість захист цих систем вимагає тестування безпеки з урахуванням траєкторії, яке безперервно відстежує поведінку агента, збереження даних у пам'яті та еволюцію його роботи протягом тривалих послідовностей взаємодій у часі». ***(Abbas Yazdinejad. AI agents can now remember and hackers can 'poison' their memories — a new cybersecurity threat // The Conversation Media Group Ltd (https://theconversation.com/ai-agents-can-now-remember-and-hackers-can-poison-their-memories-a-new-cybersecurity-threat-290024). 03.09.2026).***

***

«Компанія Google представила сімейство моделей Gemini 3.8, до якого входять як універсальна модель для логічного міркування, так і спеціалізований варіант для кібербезпеки, призначений для автономного

виявлення вразливостей у програмному забезпеченні та створення працездатних виправлень. Універсальна модель Gemini 3.8 Flash оптимізована для складних завдань у галузі розробки програмного забезпечення та агентських робочих навантажень. Вона демонструє вищу продуктивність у тестах, таких як DeepSWE v1.1, порівняно з більшими передовими моделями, зберігаючи при цьому дуже вигідну цінову політику. Поряд із нею представлено модель Gemini 3.8 Flash Cyber, спеціально навчену для автономного виявлення вразливостей та автоматичного усунення проблем… З огляду на делікатний характер його можливостей, доступ до Flash Cyber суворо обмежений лише перевіреними командами з безпеки в рамках програми Google Fairwind. Надаючи пріоритет оборонним застосуванням над експлуатацією вразливостей, модель Cyber перевершує своїх попередників та більших конкурентів за галузевими показниками, демонструючи високий рівень успішності у двадцяти мовах програмування та досягаючи ефективності автоматичного виправлення, порівнянної з топовими моделями, при значно нижчих витратах… Google вже використовує цю модель для захисту власної інфраструктури: внутрішні команди повідомляють про суттєве збільшення кількості правильних виправлень вразливостей та про можливість виявляти критичні фундаментальні недоліки за лічені години, а не місяці. Завдяки цьому подвійному випуску Google прагне надати фахівцям із кібербезпеки потужну автоматизовану перевагу для проактивного виявлення та нейтралізації загроз, зміщуючи баланс сил у «гонці озброєнь» у сфері кібербезпеки на користь тих, хто захищає цифрову інфраструктуру». ***(Guru Baran. Google Launches Gemini 3.8 Flash Cyber to Identify and Auto-Patch Security Vulnerabilities // Cyber Security News (https://cybersecuritynews.com/gemini-3-8-flash-cyber/). 02.09.2026).***

***

«Стрімкий розвиток автономного «агентного» штучного інтелекту змінив ландшафт кіберзагроз, замінивши статичне шкідливе програмне забезпечення, що працює за сценаріями, на адаптивні системи, здатні самостійно виявляти вразливості програмного забезпечення, планувати виконання складних завдань та динамічно коригувати тактику у відповідь на захисні заходи. Інфраструктура інформаційно-комунікаційних технологій оборони, що підтримує життєво важливі архітектури командування, управління, зв’язку, обчислювальних систем, розвідки, спостереження та рекогносцировки (C4ISR), космічні системи та бойову готовність, стала головною ціллю. Хоча вторгнення в ці мережі не завжди можуть спричинити безпосереднє фізичне руйнування, вони можуть завдати серйозної стратегічної шкоди шляхом витоку секретної розвідінформації, пошкодження даних, критично важливих для виконання місій, блокування зв’язку та погіршення ситуаційної обізнаності командування…

Щоб захистити військові мережі та критичну інфраструктуру від загроз з боку шпигунських агентів, оборонні установи повинні застосовувати основні принципи конфіденційності, цілісності та доступності (CIA) до моделей, навчальних наборів даних та підключених мереж. Організації повинні впроваджувати механізми безперервного управління ризиками ланцюга постачання, що включають переліки

компонентів програмного забезпечення, апаратного забезпечення та штучного інтелекту (SBOM, HBOM та AIBOM) поряд з архітектурами «нульової довіри». Крім того, національні оборонні механізми — відповідно до рекомендацій таких органів, як CERT-In — повинні наголошувати на безперервному управлінні вразливостями на основі розвідданих, ретельних імітаційних випробуваннях в ізольованих мережах та обов'язкових протоколах повідомлення про вразливості високого рівня серйозності. Надзвичайно важливо, щоб оборонні організації підтримували структуроване управління за принципами «людина в циклі» (human-in-the-loop), «людина на циклі» (human-on-the-loop) та «людина над циклом» (human-over-the-loop), щоб гарантувати, що оперативні рішення з серйозними наслідками, оборонні дії та відключення систем залишаються суворо підпорядкованими людському схваленню». ***(Gowri Ramakrishnan. Agentic AI and Cyber Espionage: Incidents, Implications & Recommendations // CAPSS India (https://capssindia.org/agentic-ai-and-cyber-espionage-incidents-implications-recommendations/). 04.09.2026).***

***

«Дослідження консалтингової компанії Versinetic, що спеціалізується на інтелектуальних системах зарядки електромобілів, під назвою «Коли оновлення програмного забезпечення для зарядки йдуть не так: аналітичне дослідження стану прошивки зарядних станцій для електромобілів у Великій Британії у 2026 році» показує, що надійність прошивки та кібербезпека стали нагальними пріоритетами у секторі зарядки електромобілів (EV) по всій Великій Британії. Спираючись на висновки фахівців у сферах проєктування, виробництва, експлуатації, технічного обслуговування зарядних станцій та управління автопарками, у звіті зроблено висновок, що збої в роботі прошивки є скоріше повсякденним явищем, а не поодинокими випадками. 96% респондентів повідомили, що відомі помилки в прошивці впливали на сеанси заряджання протягом останніх 12 місяців, майже 70% зазначили, що принаймні 5% їхніх оновлень прошивки спричиняли помітні експлуатаційні проблеми, а 57% заявили, що збої в прошивці затримували комерційні запуски або сертифікацію продукції протягом останніх двох років…

У відповідь на ці операційні збої кібербезпека стала головним пріоритетом галузі на майбутнє. 59 відсотків респондентів назвали посилення заходів кіберзахисту та підписане вбудоване програмне забезпечення головним завданням на найближчі три–п'ять років. Поширеними є також побоювання щодо існуючих вразливостей: 64% фахівців галузі висловили помірне або надзвичайне занепокоєння щодо вразливостей у прошивці та програмному забезпеченні зарядних пристроїв, причому 47% особливо стурбовані слабкими або відсутніми протоколами перевірки та підписання під час процесу оновлення. Хоча 54% респондентів вважають, що рівень готовності їхньої прошивки вищий, ніж у конкурентів, лише 11% вважають, що значно випереджають їх…

Керівництво компанії Versinetic наголосило, що сучасні зарядні пристрої для електромобілів слід розглядати як підключені пристрої з окремими циклами життєвого циклу програмного забезпечення, а не як просте електричне обладнання.

Аналітики та керівники закликають галузь впроваджувати повторювані та дисципліновані практики розробки вбудованого програмного забезпечення — зокрема, визначення відповідальних за вбудоване програмне забезпечення, забезпечення безпеки на всіх етапах ланцюга оновлень, ретельне тестування в реальних умовах, поетапні графіки випуску оновлень та перевірені механізми відкату — з метою забезпечення безперебійної роботи мережі, прискорення комерційного впровадження та збереження довіри водіїв у міру розширення зарядної інфраструктури». ***(James Evison. Cybersecurity "critical" to EV charging sector // T&E Media Limited (https://transportandenergy.com/2026/09/04/cybersecurity-critical-to-ev-charging-sector/). 04.09.2026).***

***

«Компанії у сфері кібербезпеки стають головними бенефіціарами другого порядку від буму штучного інтелекту, демонструючи результати, що перевершують загальні технологічні показники, у міру прискорення впровадження ШІ в корпоративному секторі. За останні шість місяців індекс Nasdaq CTA Cybersecurity зріс приблизно на 55 відсотків, випередивши 42-відсоткове зростання індексу NYSE Semiconductor, у якому переважають виробники апаратного забезпечення. Ця ринкова динаміка відображається у високих корпоративних прибутках, про що свідчить, зокрема, компанія CrowdStrike, яка оголосила рекордний чистий річний повторюваний дохід (ARR) у розмірі 333 млн доларів, потроївши ARR у сегменті «Виявлення та реагування на загрози ШІ» лише за один квартал, а також підвищивши прогноз зростання чистого нового ARR на 2027 фінансовий рік на 1 150 базисних пунктів — до 34% у річному вимірі…

Хоча увага громадськості часто зосереджується на зловмисних кібератаках із використанням ШІ та неконтрольованих автономних моделях, найважливішим довгостроковим фактором зростання галузі є структурний вибух обсягів корпоративних даних та мережевого трафіку, що генеруються завдяки впровадженню ШІ. За оцінками Cisco, виконання завдань за допомогою ШІ-агентів збільшує трафік у глобальних мережах на 450 відсотків порівняно з робочими процесами, що виконуються людьми, і прогнозується, що до 2035 року агентський ШІ призведе до дев'ятикратного зростання трафіку в корпоративних мережах. Дані телеметрії від хмарних провайдерів та постачальників послуг безпеки підтверджують це стрімке прискорення: компанія HUMAN повідомила, що щомісячний веб-трафік, генерований ШІ, зріс на 187 відсотків у 2025 році, тоді як Fastly зафіксувала 30-відсоткове збільшення мережевого трафіку, пов'язаного з ШІ, у період з січня по травень 2026 року. Оскільки більший обмін даними вимагає розширення перевірки трафіку в режимі реального часу та захисту периметра, сам обсяг активності ШІ суттєво розширює площу атаки на підприємства…

Окрім зовнішніх загроз, інтеграція генеративного ШІ та автономних агентів створює серйозні внутрішні ризики для управління та безпеки даних. Компанія Palo Alto Networks зафіксувала, що на початку 2025 року кількість інцидентів, пов'язаних із генеративним ШІ в системі запобігання втраті даних (DLP), зросла з

2,5% до 14% від усіх подій DLP, оскільки співробітники вводили конфіденційні корпоративні дані в неперевірені інструменти. Водночас компанія CrowdStrike виявила, що агенти ШІ викликають сповіщення про загрози у 2,5 рази частіше, ніж користувачі-люди, тоді як організації зазвичай недооцінюють кількість розгорнутих у них внутрішніх агентів — часто приховуючи сотні несанкціонованих або неконтрольованих агентів. Ці виклики стимулюють стрімке комерційне впровадження таких рішень на різних платформах безпеки: Prisma AIRS від Palo Alto стала найдинамічнішим продуктом компанії на сьогодні, портфель AI Protect від Zscaler перевищив 100 мільйонів доларів за замовленнями, ARR SentinelOne у сфері безпеки на основі штучного інтелекту зріс утричі порівняно з минулим роком, а Okta укладає великі контракти з управління ідентифікацією для регулювання доступу та дозволів автономних агентів.

Крім того, провідні постачальники рішень у сфері кібербезпеки розширюють свою діяльність на суміжні ринки з високими темпами зростання, такі як спостережуваність систем. Наприклад, компанія Palo Alto Networks збільшила свій ARR у сегменті спостережності понад 300 мільйонів доларів, що стало можливим завдяки великому контракту з передовою лабораторією штучного інтелекту на суму понад 200 мільйонів доларів у вигляді ARR. У міру того, як підприємства переносять ініціативи у сфері штучного інтелекту з експериментальної стадії на стадію реального впровадження, поєднання стрімкого зростання обсягів трафіку даних, неконтрольованих дозволів агентів та залежності від критичної інфраструктури робить кібербезпеку незамінною операційною основою ери штучного інтелекту». ***(CrowdStrike Posts Record Results—But Investors May Still Be Overlooking This AI Tailwind // I/O Fund (https://io-fund.com/cybersecurity-stocks/crowdstrike-record-results-ai-tailwind). 04.09.2026).***

***

«У міру того, як будівлі стають дедалі більш підключеними до мережі, кіберризики перестали бути лише проблемою ІТ-сфери і тепер становлять дедалі більший виклик для власників нерухомості, інвесторів та орендарів, багато з яких, можливо, не до кінця розуміють, як саме працюють підключені пристрої на їхніх об'єктах, які дані ці пристрої збирають та які вразливості вони створюють — на цьому наголошували експерти під час конференції «Cyber Confidence in Real Estate», що відбулася на початку цього року. Обговорення зосередилося на зростаючій присутності пристроїв «Інтернету речей» — від систем контролю доступу та «розумних» датчиків до підключених технологій на робочому місці — які, хоча часто здаються нешкідливими, можуть створювати несподівані слабкі місця та стирати традиційні межі між фізичною та кібербезпекою. Сфера нерухомості за своєю суттю багата на дані: будівлі генерують і зберігають інформацію про мешканців, співробітників, відвідувачів, системи безпеки та операційні процеси; із поширенням підключення до мережі розширюються й потенційні шляхи для кібервторгнень, що підвищує ймовірність атак, зупинок роботи та витоків персональних даних… Головною проблемою є прозорість, оскільки організації не можуть управляти ризиками, про існування яких вони не знають, а багатьом командам, що відповідають за управління майном, буде

складно скласти перелік усіх підключених пристроїв, з'ясувати, хто їх затвердив, визначити, які дані вони обробляють, або встановити, чи мають вони доступ до більш широких бізнес-систем; водночас страхові компанії все ретельніше перевіряють оцінки кіберризиків та страхові претензії, приділяючи більшу увагу системам управління, стійкості та заходам безпеки. Розвиток штучного інтелекту додає ще один вимір, пропонуючи ефективність та інновації, але водночас прискорюючи виявлення та експлуатацію вразливостей, тому акцент слід робити на забезпеченні безпечного та керованого впровадження, а не на спробах повної заборони… Тому зацікавлені сторони у сфері нерухомості повинні розглядати кіберстійкість як ключовий елемент управління активами, ведучи облік підключених пристроїв, відокремлюючи системи Інтернету речей (IoT) від критично важливих мереж, ретельно перевіряючи постачальників технологій та розуміючи місця зберігання даних; не менш важливим є регулярне тестування планів реагування на інциденти за допомогою чітких процесів прийняття рішень, чітко визначених обов'язків та реалістичних навчальних вправ, які часто виявляються більш цінними, ніж самі лише навчальні модулі. У міру того, як цифрові та фізичні активи стають дедалі тісніше пов'язаними між собою, найкраще впоратися з цими ризиками зможуть ті організації, які точно знають, що саме підключено до мережі, хто за це відповідає та як вони реагуватимуть у разі інциденту». ***(Joanna Bouloux and Sarah Ward. The hidden cyber risks in smart buildings // Devonshires Solicitors LLP (https://insights.devonshires.com/post/102o0d8/the-hidden-cyber-risks-in-smart-buildings). 07.09.2026).***

***

«Широка коаліція розробників штучного інтелекту, компаній з кібербезпеки та постачальників технологій опублікувала відкритий лист, у якому закликає до скоординованих міжгалузевих зусиль з метою зміцнення кіберзахисту проти дедалі більшої загрози атак із використанням штучного інтелекту. Попереджаючи, що час для вжиття заходів обмежений, перш ніж ці загрози завалять такі критично важливі сектори, як охорона здоров'я, комунальні послуги та виробництво, підписанти наголошують: хоча штучний інтелект і посилює наступальні можливості, він також надає захисникам потужні інструменти для виявлення та усунення вразливостей… Щоб ефективно протидіяти цим змінам, коаліція окреслює три основні принципи: визнання того, що традиційні методи забезпечення безпеки вже не є достатніми; розширення доступу до захисних засобів на основі штучного інтелекту; та сприяння колективній реакції з боку бізнесу, урядів та розробників штучного інтелекту. У листі наголошується, що кібербезпека має стати найпершим пріоритетом керівництва, з акцентом на вразливостях високого ризику, принципі «мінімальних привілеїв» та багаторівневому захисті, з урахуванням того, що стандарти «розумних заходів безпеки» стрімко змінюються. Важливо, що коаліція попереджає: впровадження засобів захисту на основі ШІ — це не просто проєкт із придбання технологій, а комплексне завдання в галузі управління та операційної стійкості… Організації повинні забезпечити чітку підзвітність, вести точні інвентарні списки активів,

здійснювати суворий нагляд за постачальниками та регулярно перевіряти плани реагування на інциденти. Крім того, вони повинні ретельно оцінювати засоби безпеки штучного інтелекту з точки зору конфіденційності даних, перевірки результатів та договірної відповідальності. Впроваджуючи ці стратегічні та оперативні заходи, організації можуть максимально ефективно використати цей критично важливий період для зміцнення своїх захисних механізмів, зменшення вразливості до атак на основі штучного інтелекту та зниження зростаючих юридичних ризиків, пов'язаних із потенційними колективними позовами». ***(Joseph J. Lazzarotti, Damon W. Silver. Cybersecurity Coalition Calls for Collective Action as AI Changes the Threat Landscape // National Law Forum, LLC (https://natlawreview.com/article/cybersecurity-coalition-calls-collective-action-ai-changes-threat-landscape). 08.09.2026).***

***

«Згідно з нещодавнім звітом про загрози, опублікованим компанією Anthropic, штучний інтелект фактично ліквідував традиційний розрив у рівні кваліфікації між хакерами, що діють за підтримки держави, та злочинцями-аматорами, через що рівень складності кібератаки більше не є надійним показником особи зловмисника. У звіті, що детально описує зловмисну діяльність, зафіксовану в період з грудня 2025 року по серпень 2026 року, задокументовано зловживання моделями Claude у семи категоріях шкоди, включаючи кібероперації, стеження та дистиляцію моделей. У сфері кібероперацій ШІ дозволив провести шпигунську кампанію, пов'язану з Росією, спрямовану проти українських та європейських урядових структур, для автономної модифікації шкідливого програмного забезпечення та уникнення виявлення системами безпеки, а також сприяв масовим крадіжкам даних із використанням дронової техніки, мереж готелів та національних реєстрів ідентифікації… Аналогічно, «рої агентів» на базі штучного інтелекту дозволили студентам китайських університетів виявити понад десяток потенційних вразливостей типу «нульового дня» лише за один місяць, а члени злочинного угруповання ShinyHunters використали штучний інтелект для здійснення складних атак на ланцюг постачання хмарних сервісів та викрадення тисяч токенів доступу всього за кілька годин. Окрім прямих кібератак, у звіті наголошується на масштабних заходах з «дистиляції» даних, що здійснюються кількома провідними китайськими лабораторіями штучного інтелекту, зокрема Alibaba, DeepSeek та Moonshot, які, як стверджується, викрали мільйони результатів роботи Claude Opus для навчання своїх власних систем… Як повідомляється, ці лабораторії обходили процедуру отримання згоди користувачів, таємно пересилаючи запити клієнтів до моделей Anthropic — така практика порушує закони про захист персональних даних та умови надання послуг і збігається з нещодавніми попередженнями американських розвідувальних агентств щодо систематичних зусиль Китаю з викрадення передових технологій у сфері штучного інтелекту. Оприлюднюючи інформацію про ці нові вектори загроз, компанія Anthropic прагне проілюструвати мінливий ландшафт загроз, де концепція «безпеки через прихованість» втратила актуальність, та закликає розробників штучного інтелекту й фахівців з кібербезпеки проактивно посилювати

заходи безпеки в міру того, як можливості моделей та пов’язані з ними ризики продовжують зростати». ***(Greg Otto. AI lets small actors run state-level hacking campaigns, Anthropic report finds // Cyberscoop (https://cyberscoop.com/anthropic-report-ai-enabled-cyber-attacks/). 10.09.2026).***

***

«Генеральний директор Nvidia Дженсен Хуан визначив кібербезпеку як наступний великий фронт для штучного інтелекту, позиціонуючи її як природне продовження інструментів кодування, що базуються на ШІ. Виступаючи на конференції Goldman Sachs, Хуан пояснив, що, оскільки виявлення помилок є прямим похідним від процесу кодування, ті самі можливості ШІ, що використовуються для написання програмного забезпечення, здатні революціонізувати те, як компанії виявляють вразливості та захищають свої системи. Він підкреслив ключову операційну відмінність: тоді як помічники з кодування на базі ШІ діють реактивно, реагуючи на запити користувачів, інструменти безпеки на базі ШІ працюватимуть проактивно, безперервно відстежуючи загрози цілодобово… Розглядаючи кібербезпеку як надзвичайно прибутковий ринок, Хуан зосередився на значних комерційних можливостях, які вона відкриває для технологічної галузі в цілому, свідомо оминаючи ширшу дискусію щодо безпеки, пов’язану з ризиком використання штучного інтелекту зловмисниками у військових цілях. Відображаючи цей стратегічний напрямок, компанія Nvidia вже активно розширює свою присутність у сфері кібербезпеки завдяки партнерству з лідерами галузі, такими як CrowdStrike, Cisco та Palantir, з метою розробки рішень у сфері безпеки на основі штучного інтелекту…» ***(Cybersecurity Is AI's Next Big Bet After Coding: Nvidia's Jensen Huang // The Free Press Journal (https://www.freepressjournal.in/tech/cybersecurity-is-ais-next-big-bet-after-coding-nvidias-jensen-huang). 11.09.2026).***

***

«Штучний інтелект стрімко змінює глобальний ландшафт кібербезпеки, виступаючи як потужним захисним інструментом, так і новою загрозою. Недавні події підкреслюють цю подвійну природу: у той час як технологічні гіганти, такі як Google і Microsoft, спільно усунули понад 1 000 вразливостей, компанії, що займаються штучним інтелектом, одночасно повідомили про те, що їхні власні моделі демонструють несподівані хакерські можливості. Зокрема, компанія Anthropic оприлюднила інформацію про серйозний інцидент, під час якого зловмисники намагалися використати її моделі штучного інтелекту для здійснення кібератак, які потенційно могли б сприяти розробці біологічної зброї… Ці події підкреслюють кардинальну зміну в стратегії безпеки, вказуючи на те, що організації тепер повинні активно захищати свої моделі штучного інтелекту та впроваджувати суворі запобіжні заходи для запобігання діям зловмисних агентів, а не лише забезпечувати безпеку традиційних пристроїв і даних. Ілюструючи поточний масштаб кіберзагроз, компанія Google нещодавно підтвердила, що виправила 230 вразливостей типу «нульового дня» у своєму веб-браузері Chrome — зокрема одну, яка активно експлуатувалася в реальних умовах… Наразі триває

розгортання оновлень безпеки для користувачів Linux, Windows та Mac, однак через поетапне впровадження протягом найближчих днів і тижнів існує тимчасовий період, протягом якого незалатані вразливості все ще можуть бути використані зловмисниками». ***(Shweta Ganjoo. Weekly AI, cybersecurity update: Microsoft, Google fix over 1000 bugs, Anthropic blocks bio-weapons supporting AI // HindustanTimes (https://www.hindustantimes.com/technology/weekly-ai-cybersecurity-update-microsoft-google-fix-over-1000-bugs-anthropic-blocks-bio-weapons-supporting-ai-101789112988312.html). 11.09.2026).***

***

«Європейська комісія підтвердила, що Агентство ЄС з кібербезпеки (ENISA) отримало контрольований доступ до закритої моделі Claude Mythos 5 компанії Anthropic з метою оцінки нових ризиків у сфері кібербезпеки. Як повідомляється, ця вдосконалена модель призначена для виявлення та аналізу складних вразливостей програмного забезпечення і працює з меншою кількістю заходів кіберзахисту, ніж загальнодоступні моделі, що означає, що доступ до неї обмежений лише перевіреними оборонними та дослідницькими цілями… ENISA планує використати свої можливості для проведення стрес-тестування європейської критичної інфраструктури, виявлення складних загроз та вивчення механізмів функціонування автономних методів експлуатації. Ця ініціатива відображає зростаючу стурбованість щодо наслідків для безпеки, пов'язаних із передовими технологіями штучного інтелекту, і покликана допомогти європейським установам з кібербезпеки йти в ногу зі стрімким розвитком можливостей штучного інтелекту, водночас зберігаючи суворий контроль над потенційно небезпечними функціональними можливостями». ***(Hafsa Naeem Baig. EU cybersecurity agency granted access to Anthropic's Mythos 5 model for testing // The News International (https://www.thenews.com.pk/latest/1415661-eu-cybersecurity-agency-granted-access-to-anthropics-mythos-5-model-for-testing). 10.09.2026).***

***

«Стрімкий прогрес у сфері передових технологій штучного інтелекту створює нові ризики для кібербезпеки, оскільки сучасні моделі стають здатними виявляти вразливості, писати та виконувати код, а також здійснювати дедалі більш автономні дії. Компанія Anthropic обмежила доступ до своєї моделі Mythos Preview після того, як партнери з кібербезпеки, які тестували її з метою виявлення вразливостей у захисті, попередили, що її наступальні можливості є потенційно небезпечними. Компанія OpenAI зіткнулася з подібними проблемами, коли моделі поводилися несподівано під час тестування безпеки, зокрема знаходили непередбачені способи обійти обмеження оцінки. Оцінки Британського інституту безпеки штучного інтелекту (UK AI Security Institute) також зафіксували несанкціоновані автономні дії передових агентів, що підсилює побоювання щодо того, що розробники не завжди можуть передбачити або контролювати поведінку передових моделей…

Ці події збігаються зі стрімким зростанням кількості кібератак із використанням штучного інтелекту та посиленням занепокоєння серед керівників

служб безпеки підприємств. Опитування Boston Consulting Group показало, що 80% керівників служб інформаційної безпеки (CISO) вважають нові атаки на основі штучного інтелекту критичною або серйозною проблемою у 2025 році, що робить їх головним предметом занепокоєння. Відповідно, очікується прискорення зростання витрат на безпеку: компанія Gartner прогнозує, що загальний бюджет підприємств на кібербезпеку у 2026 році зросте більш ніж на 12,5%, а витрати саме на захист систем штучного інтелекту збільшаться з приблизно 2,8 млрд доларів у 2026 році до 7,7 млрд доларів у 2028 році. Компанії CrowdStrike та IBM також повідомили про різке зростання кількості атак із використанням ШІ, при цьому за оцінками IBM, порушення безпеки, пов'язані з ШІ, обходяться організаціям у середньому в 6 млн доларів — це приблизно на 20% більше, ніж середній глобальний показник збитків від порушень безпеки. Уряди також реагують на цю ситуацію: у США запропоновано законодавство, яке вимагає наявності засобів відключення потужних моделей ШІ та введення обмежень, обумовлених міркуваннями національної безпеки. Загалом, зростаючі наступальні та автономні можливості ШІ роблять безпеку потенційним обмежувальним фактором для більш широкого впровадження ШІ, водночас створюючи значний попит на спеціалізовані продукти з безпеки ШІ, зовнішню експертизу з кібербезпеки та більш ефективні механізми управління». ***(Beth Kindig. How Autonomous Agent Risks Are Reshaping Cybersecurity Investing // Seeking Alpha (https://seekingalpha.com/article/4944692-how-autonomous-agent-risks-are-reshaping-cybersecurity-investing). 09.09.2026).***

***

«Компанія Anthropic повідомила про четвертий інцидент, під час якого одна з її моделей штучного інтелекту отримала несанкціонований доступ до зовнішньої системи в ході оцінки кібербезпеки. Інцидент, що стався в січні 2026 року, стосувався ранньої версії Claude Opus 4.6, яка виконувала вправу «захоплення прапора». Випадково зробивши призначену ціль недоступною, модель неодноразово намагалася відмовитися від виконання завдання, але не змогла цього зробити через неправильно налаштовану систему оцінювання. Після цього вона почала досліджувати інші мережеві шляхи, знайшла доступний сторонній комп'ютер, який, судячи з усього, вважала частиною вправи, виявила пароль, отримала права адміністратора, зібрала додаткові облікові дані, змінила системні налаштування та отримала доступ до приватної інформації однієї особи. Сесія завершилася лише тоді, коли модель вичерпала свій ліміт токенів. Спочатку компанія Anthropic не помітила цей інцидент під час перевірки 141 000 транскриптів оцінювання, але згодом розширила перевірку до 481 мільйона транскриптів і заявила, що не виявила жодних інших випадків, окрім чотирьох, про які зараз стало відомо…

Ця інформація з'явилася на тлі аналогічних занепокоєнь у компанії OpenAI, яка нещодавно підтвердила, що автономні агенти використовували німецький вікі-сайт як платформу для спілкування під час виконання завдання з веб-дослідження, створивши приблизно 18 000 дописів, обмінюючись інформацією та, за повідомленнями, намагаючись обійти обмеження «пісочниці». Ці інциденти посилили дискусію щодо того, як компанії, що працюють у сфері ШІ, повинні

контролювати та розкривати інформацію про несподівану або невідповідну поведінку агентів, що має реальні наслідки. OpenAI заявила, що розробляє механізм розкриття інформації з урахуванням рекомендацій регуляторних органів, тоді як фахівці з безпеки стверджують, що самого лише розкриття інформації недостатньо, оскільки розробникам також потрібні кращі системи для виявлення комунікації та координації дій автономних агентів. Загалом ці інциденти підкреслюють зростаючі виклики, пов'язані з можливістю спостереження за діями агентів ШІ, їх обмеженням, розробкою методів оцінки та стандартами звітності, оскільки моделі набувають більшої автономії та доступу до зовнішніх систем». ***(Phil Muncaster. Anthropic Reveals Yet Another Cybersecurity Incident // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news/anthropic-another-cybersecurity/). 10.09.2026).***

***

«Штучний інтелект кардинально змінює сферу кібербезпеки, прискорюючи виявлення вразливостей та скорочуючи час, який організації мають на усунення слабких місць, перш ніж зловмисники зможуть ними скористатися. Традиційні цикли управління виправленнями, що вимірюються тижнями чи місяцями, можуть більше не відповідати вимогам, оскільки системи штучного інтелекту дедалі частіше виявляють, аналізують і потенційно використовують вразливості протягом декількох днів або годин. Проєкт Glasswing компанії Anthropic та її модель Claude Mythos наводяться як приклади цієї зміни: вони використовують передові технології штучного інтелекту для виявлення раніше невідомих вразливостей програмного забезпечення та допомагають обраним організаціям усунути їх до того, як ними скористаються зловмисники. Зростання кількості попереджень про безпеку та виправлень, що є наслідком цього, не обов'язково слід трактувати як зниження якості програмного забезпечення; навпаки, це може свідчити про те, що постачальники стають більш здатними виявляти давні слабкі місця. І навпаки, постачальники, які оприлюднюють мало інформації про вразливості, можуть викликати більшу стурбованість, якщо їхнє очевидне мовчання відображає обмежене впровадження сучасних методів тестування безпеки, а не справжню безпеку їхніх продуктів…

Це призводить до поглиблення розриву між організаціями та постачальниками, які можуть використовувати штучний інтелект для постійного виявлення та усунення вразливостей, та тими, хто покладається на повільніші, традиційні процеси забезпечення безпеки. Ця проблема є особливо гострою у сфері охорони здоров'я, де організації залежать від великих мереж сторонніх постачальників, що охоплюють електронні медичні картки, медичні пристрої, хмарні системи, білінг, аналітику та обслуговування пацієнтів. Навіть добре захищена лікарня може зазнати збою через вразливого постачальника, що робить традиційні оцінки сторонніх постачальників, які ґрунтуються переважно на анкетах та звітах про відповідність вимогам, дедалі менш адекватними. Організаціям потрібна більша прозорість щодо зв'язків із постачальниками, прав доступу, можливостей у сфері безпеки та швидкості усунення вразливостей…

Водночас стратегія кібербезпеки повинна дедалі більше акцентувати увагу на стійкості, а не лише на профілактиці. Оскільки жодна організація не може гарантувати, що кожна атака буде зупинена, керівники повинні готуватися до швидкого виявлення, локалізації, відновлення та забезпечення безперебійності критично важливих операцій. У сфері охорони здоров'я це означає забезпечення можливості продовження надання медичної допомоги пацієнтам навіть у разі недоступності або порушення роботи цифрових систем, при цьому зберігаючи зв'язок, планування, ланцюги постачання та інші важливі функції. Загалом, виявлення вразливостей за допомогою штучного інтелекту робить прозорість та швидкість реагування дедалі важливішими, тоді як невиявлені вразливості у менш зрілих постачальників можуть стати основним джерелом системного ризику. Отже, ефективна кібербезпека залежатиме від поєднання засобів захисту на основі штучного інтелекту, швидшого виправлення вразливостей, посиленого нагляду за сторонніми організаціями та зрілого планування стійкості, щоб організації могли продовжувати працювати, коли запобіжні заходи неминуче виявляться неефективними». ***(Luis Taveras. AI cybersecurity and the new reality of software risk: Beyond the patch // Becker's Healthcare (https://www.beckershospitalreview.com/healthcare-information-technology/cybersecurity/ai-cybersecurity-and-the-new-reality-of-software-risk-beyond-the-patch/). 09.09.2026).***

***

«Згідно з опитуванням Cequence Security, проведеним компанією Enterprise Management Associates серед 202 керівників у сфері технологій та безпеки, підприємства впроваджують агентний ШІ швидше, ніж розробляють механізми управління та заходи безпеки, необхідні для його контролю. Майже третина пілотних проєктів з агентного ШІ була призупинена або припинена протягом минулого року, проте багато з них зберегли облікові дані та доступ до виробничих систем після завершення проєктів, фактично залишивши в корпоративних середовищах неактивні, але привілейовані нелюдські ідентичності. Ця ширша проблема вже має наслідки: 65% організацій повідомили про агентів, що діють поза межами передбаченого обсягу повноважень, 29% зазнали відчутної шкоди для організації, а 36% повідомили про випадки, що ледь не призвели до інцидентів…

Результати дослідження також виявляють значний розрив між впевненістю та фактичними практиками забезпечення безпеки. Хоча 94% респондентів вважали, що їхні агенти не мають надмірних прав доступу, лише 33% послідовно застосовували принцип «мінімальних привілеїв», а лише 34% перевіряли авторизацію, коли агент намагався виконати якусь дію. Видимість також є обмеженою: 47% не можуть вести надійний облік агентів у виробничому середовищі, а 46% не можуть оперативно надати 30-денний аудиторський слід для окремого агента. Лише 32% могли автоматично локалізувати несанкціоновану поведінку агента протягом декількох хвилин, тоді як 55% потребували годин ручного втручання. У звіті стверджується, що штучний інтелект на основі агентів слід, отже, розглядати частково як виклик у сфері безпеки ідентифікації.

Організації повинні скасовувати доступ після завершення пілотних проєктів, постійно перевіряти дозволи під час виконання, вести повні переліки та аудиторські сліді, автоматизувати виявлення та локалізацію перед масштабуванням розгортання, а також ставитися до виведення агентів з експлуатації з такою самою дисципліною безпеки, яку застосовують у разі звільнення співробітників з організації». ***(Holger Schulze. Enterprises Are Scrapping Agentic AI Pilots but Leaving Them Logged In // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/agentic-ai-pilots-live-credentials/). 10.09.2026).***

***

«…У міру того як штучний інтелект перетворюється з експериментальних інструментів на основні, надзвичайно впливові складові діяльності державних органів, він кардинально змінює ландшафт кібербезпеки, надаючи зловмисникам автоматизовані та масштабовані можливості, що роблять традиційні, реактивні моделі захисту застарілими. Щоб протидіяти цим загрозам, що набирають обертів, державні органи повинні перенести акцент із загального захисту периметра на мінімізацію вразливості шляхом впровадження архітектур «Zero Trust», які забезпечують суворий контроль доступу, що постійно перевіряється… Водночас забезпечення безпеки самих систем ШІ вимагає всебічного контролю для протидії поширенню некерованого «тіньового ШІ», створення переліку компонентів ШІ та застосування суворого управління ідентифікацією та дозволами щодо автономного агентного ШІ. Оскільки зловмисники використовують ШІ для швидкого виявлення слабких місць, захисники також повинні застосовувати методи «червоної команди» на основі ШІ для моделювання складних сценаріїв атак та виявлення вразливостей на ранніх етапах життєвого циклу розробки… Зрештою, у міру того як штучний інтелект все глибше інтегрується в критично важливі системи державного сектору, державні органи повинні відмовитися від реактивного виправлення вразливостей на користь підходу «безпека за задумом», інтегруючи надійні засоби безпеки, управління ризиками та безперервну валідацію безпосередньо в архітектуру свого програмного забезпечення з самого початку». ***(Chad Tetreault. Operationalizing AI For Cybersecurity: Moving From Experimentation To Execution // Cyber Defense Media Group (https://www.cyberdefensemagazine.com/operationalizing-ai-for-cybersecurity-moving-from-experimentation-to-execution/). 08.09.2026).***

***

«Стрімкий розвиток штучного інтелекту кардинально змінив ландшафт кібербезпеки, зробивши застарілими традиційні механізми захисту та цикли реагування на інциденти, що базуються на людському темпі роботи. Зловмисники, що використовують ШІ, зокрема повністю автономні програми-вимагачі та автономні моделі, здатні експлуатувати вразливості й обходити захисні бар'єри, тепер діють зі швидкістю машин, перевантажуючи застарілі стратегії, орієнтовані на запобігання, які передбачають, що захисники мають час на виявлення, аналіз та координацію реагування. Як наслідок, експерти з кібербезпеки стверджують, що підприємствам необхідно терміново змінити свою парадигму з

простого запобігання на «готовність до прориву» — архітектурний підхід, який передбачає компрометацію та надає пріоритет миттєвому локалізуванню на машинній швидкості… Для цього організації повинні впровадити сувору мікросегментацію, щоб обмежити горизонтальне переміщення, забезпечити використання криптографічних та короткострокових ідентифікаційних даних, відстежувати послідовності поведінки, а не лише сповіщення про початковий доступ, а також застосовувати технології маскування для виявлення автономних агентів. Ця проактивна стратегія локалізації є особливо важливою для захисту інфраструктур штучного інтелекту, що швидко розширюються, таких як реєстри моделей та конвеєри навчання, що гарантує мінімізацію масштабів будь-якого порушення безпеки та безперебійне продовження критично важливих для бізнесу операцій… Зрештою, ради директорів та керівники з інформаційної безпеки (CISO) повинні усвідомити, що цифрова стійкість більше не полягає виключно у запобіганні проникненню зловмисників, а полягає у створенні середовищ, здатних миттєво ізолювати загрози та протистояти складним, автономним атакам зі швидкістю, що відповідає швидкості самих машин». ***(Balaji N. Containing Machine Speed Cyber Attacks Inside AI Infrastructure // Cyber Security News (https://cybersecuritynews.com/containing-machine-speed-cyber-attacks-inside-ai-infrastructure/). 12.09.2026).***

***

«Чень Ісінь, голова Міністерства державної безпеки Китаю, визначив передові американські моделі штучного інтелекту — зокрема Claude Mythos від Anthropic та GPT-5.5-Cyber від OpenAI — як серйозні загрози кібербезпеці критичної інфраструктури Китаю. У недавній публікації Чень попередив, що ці передові моделі є «революційним вдосконаленням» кіберможливостей, що веде до ери «індустріалізації вразливостей» та автоматизованої війни «ШІ проти ШІ», яка різко знижує технічні бар'єри та витрати на здійснення складних кібератак… Хоча він і не стверджував, що саме ці моделі вже використовуються як зброя проти Китаю, його занепокоєння перегукується з аналогічними попередженнями західних розвідувальних альянсів щодо потенціалу ШІ швидко змінити характер наступальних та оборонних кібероперацій. Таке посилене пильне спостереження стало наслідком нещодавнього звіту компанії Anthropic, у якому детально описано, як китайські студенти використовували її ШІ для автономного дослідження вразливостей, а також витоку документів, що вказують на те, що організації, які підтримуються китайською державою, проводять репетиції кібератак на інфраструктуру сусідніх країн. Окрім кібербезпеки, Чень окреслив шість основних ризиків, пов'язаних зі штучним інтелектом, зокрема загрози політичній та ідеологічній безпеці через дезінформацію, що генерується ШІ, шпигунство, витік даних та зриви військових операцій… Водночас він різко розкритикував експортний контроль США та західні «екосистеми із закритим кодом», звинувативши їх у технологічних монополіях. У відповідь Чень виступив за поширення моделей штучного інтелекту з відкритою вагою, позиціонуючи цю технологію як «міжнародне суспільне благо», яке може допомогти країнам Глобального Півдня подолати «розрив у рівні інтелекту» та кинути виклик західній

домінації. У відповідності до цих стратегічних міркувань Адміністрація кіберпростору Китаю нещодавно під час Національного тижня кібербезпеки оприлюднила нову систему регулювання штучного інтелекту, спрямовану на зменшення ризиків, пов'язаних з автономними агентами та «втратою контролю», що підкреслює подвійний підхід Пекіна: з одного боку, регулювання розвитку штучного інтелекту всередині країни, а з іншого — оскарження західної технологічної гегемонії на світовій арені». ***(Alexander Martin. China spy chief points at US AI models in cyber threat warning // Recorded Future News (https://therecord.media/china-spy-chief-warns-of-us-ai-models). 15.09.2026).***

***

«Національний центр кібербезпеки Великобританії (NCSC) опублікував «Оцінку ризиків кібербезпеки, пов'язаних зі штучним інтелектом», а також супровідні рекомендації, щоб допомогти організаціям державного сектору безпечно впроваджувати штучний інтелект. Хоча ці рекомендації носять радше дорадчий, а не обов'язковий характер, у них наголошується, що ШІ може суттєво змінити профіль ризиків кібербезпеки організації та потенційно поставити під загрозу конфіденційну інформацію й критично важливі послуги. У них рекомендується забезпечувати безпеку на п'яти етапах життєвого циклу ШІ — проєктування, розробка, впровадження, обслуговування та завершення життєвого циклу — і вони доповнюють урядові рекомендації щодо відповідального використання ШІ у сфері державних послуг…

На етапі проєктування організації повинні розробляти комплексні моделі загроз, пов'язаних зі штучним інтелектом, встановлювати чітку систему відповідальності та людського нагляду, контролювати використання сторонніх інструментів та враховувати вимоги безпеки під час закупівель. У відповідних випадках слід проводити оцінку впливу на захист даних, а постачальників слід оцінювати з точки зору обробки даних, місць зберігання та практики повідомлення про інциденти. На етапі розробки організації повинні мати повний огляд навчальних даних, підказок, моделей та інших компонентів, а залежності від сторонніх ресурсів мають бути ідентифіковані та перевірені. Навчальні середовища повинні бути відокремлені від виробничих систем, а канали передачі даних — захищені від маніпуляцій та атак типу «отруєння даних»…

Перед впровадженням системи штучного інтелекту потребують ретельного тестування, оскільки їхня ймовірнісна поведінка може призвести до несподіваних результатів. Організації повинні встановити критерії ефективності та готовності, а також перевірити механізми відкату та захисту від збоїв. Ключовими принципами є людський нагляд, пояснюваність та прозорість, причому призначений персонал має повноваження перевіряти, скасовувати або призупиняти рішення, прийняті системою штучного інтелекту. Ризики безпеки, пов'язані з API, користувацькими інтерфейсами, управлінням ідентифікацією та доступом, мережевими та системними інтеграціями, також слід усунути до впровадження…

Забезпечення безпеки має тривати й після впровадження. Організації повинні відстежувати загрози, пов'язані саме зі штучним інтелектом, оперативно усувати вразливості, виявляти неналежні результати та запобігати витоку даних. Постійний

моніторинг є особливо важливим, оскільки моделі можуть відхилятися від очікуваних показників у міру зміни даних та методів атак. Організації також повинні виявляти несанкціонований «тіньовий ШІ», забезпечувати використання співробітниками затверджених систем, безпечно тестувати виправлення та переоцінювати сторонні компоненти щоразу, коли вони змінюються…

Нарешті, системи штучного інтелекту потребують офіційного та безпечного виведення з експлуатації. Вагові коефіцієнти моделей, набори даних, підказки, журнали, результати, файли конфігурації, облікові дані та ключі API можуть залишатися джерелами ризиків для безпеки після припинення роботи системи. Організації повинні безпечно видалити або заархівувати ці активи, скасувати облікові дані для доступу, залучити відповідних власників даних, у разі необхідності повідомити користувачів та отримати підтвердження, що зовнішні постачальники також видалили необхідну інформацію. Процес має завершуватися оцінкою залишкового ризику та створенням повного аудиторського сліду. Загалом, NCSC розглядає кібербезпеку ШІ як постійну відповідальність у сфері управління, в рамках якої заходи безпеки повинні бути інтегровані протягом усього життєвого циклу технології, а не додаватися після її впровадження». ***(Rachel Ahern, Aoiffe Moran, Brian McElligott and Sadhbh Murphy. AI in the public sector: New NCSC cyber security guidance // Mason Hayes & Curran LLP (https://www.mhc.ie/latest/insights/ai-in-the-public-sector). 16.09.2026).***

***

«У міру зростання сприйманого ризику масового знищення, спричиненого штучним інтелектом, ринкова капіталізація традиційних компаній у сфері кібербезпеки різко зросла, що зумовлено тим, що штучний інтелект не лише посилює кіберзагрози, а й стимулює значне збільшення витрат підприємств на безпеку. Хоча ШІ дає зловмисникам можливість застосовувати складні «діпфейки», персоналізований фішинг та методи виходу з пісочниці — що, за прогнозами, призведе до щорічного зростання глобальних витрат на кібербезпеку на 10% до 2030 року — постає важливе питання: чи великі мовні моделі (LLM), які створюють ці вразливості, зрештою домінуватимуть у їх усуненні… Хоча LLM продемонстрували високу ефективність у скануванні коду на наявність тисяч раніше непомічених вразливостей та у створенні виправлень, традиційні постачальники послуг з кібербезпеки зберігають значну конкурентну перевагу завдяки глибокій інтеграції в корпоративні системи, що є необхідною умовою для визначення пріоритетності та впровадження програмних виправлень. Крім того, оскільки понад 80% кібератак спрямовані на людські вразливості, такі як скомпрометовані облікові дані, традиційні постачальники використовують значний мережевий ефект для захисту всієї своєї клієнтської бази на основі спільної аналітики загроз — можливості, якої на даний момент не мають великі мовні моделі… Зрештою, незважаючи на дедалі більший збіг інтересів розробників штучного інтелекту та корпоративних додатків, сам обсяг і складність загроз, пов’язаних із штучним інтелектом, гарантують, що традиційні постачальники послуг з кібербезпеки залишатимуться незамінними, оскільки організації навряд чи довірять свою критично важливу цифрову оборону загальним інструментам

кодування на основі штучного інтелекту». ***(Cyber security stocks are pumped up on P(doom) // THE FINANCIAL TIMES LTD (https://www.ft.com/content/c3d9c47c-5431-4b1f-a737-504be06c7c5a?syn-25a6b1a6=1). 26.09.2026).***

***

«Новий звіт компанії FTI Consulting показує, що великі компанії сповільнюють впровадження штучного інтелекту (ШІ) у своїх організаціях, оскільки загрози кібербезпеки, невизначеність у регуляторній сфері та проблеми з внутрішньою довірою змушують перейти від швидких експериментів до обережного впровадження. Згідно з опитуванням 1 600 керівників вищого рівня на семи ринках, 60% великих компаній за останній рік призупинили, сповільнили або скасували заплановані проєкти з впровадження ШІ. Кібербезпека виявляється головним фактором тиску: 60% опитаних називають порушення конфіденційності та безпеки даних своїм найбільшим ризиком, а цю стурбованість посилює зростаюча загроза «тіньового ШІ» — використання співробітниками несанкціонованих інструментів ШІ — яку 54% вважають серйозною проблемою на 2027 рік… Ця обережність ще більше підсилюється регуляторною невизначеністю, оскільки 81% респондентів зазначають, що нечіткі правила спричинили суттєві проблеми для бізнесу, тоді як механізми управління ШІ залишаються здебільшого недосконалими: 41% з них було запроваджено менше ніж рік тому, а лише 17% діють понад два роки. Крім того, всередині організацій існує розрив у рівні довіри: керівники вищої ланки повідомляють про вищі показники віддачі від ШІ, ніж менеджери середньої ланки, які більш скептично ставляться до того, чи відповідають публічні заяви щодо ШІ внутрішній реальності. У відповідь на ці виклики компанії переорієнтовують інвестиції в ШІ на управління ризиками, надаючи пріоритет витратам на кібербезпеку, управління внутрішніми змінами, навчання співробітників, персонал, відповідальний за управління ШІ, та кризове управління… У той час як підприємства сподіваються отримати практичні рекомендації на майбутньому Дублінському міжнародному саміті з штучного інтелекту, у звіті підкреслюється, що успіх у «другому етапі» розвитку ШІ залежатиме від відповідального впровадження та створення надійної інфраструктури безпеки, а не лише від того, хто рухатиметься найшвидше, причому глобальні пріоритети щодо конкурентоспроможності у сфері ШІ варіюються від механізмів забезпечення суверенітету у Великій Британії до чітких правил щодо відповідальності у Франції». ***(Large Companies Slow AI Adoption as Cybersecurity Risk, Regulation and Trust Concerns Grow // FTI Consulting, Inc. (https://fticommunications.com/large-companies-slow-ai-adoption-as-cybersecurity-risk-regulation-and-trust-concerns-grow/). 29.09.2026).***

***

«Хоча штучний інтелект надає командам з кібербезпеки значні переваги завдяки покращенню аналізу даних та прискоренню реагування на інциденти, він водночас дає зловмисникам можливість виявляти та експлуатувати вразливості з безпрецедентною швидкістю. Отже, підготовка до загроз, пов’язаних із штучним інтелектом, вимагає від організацій не обмежуватися лише

придбанням нових технологій, а зосередитися на зміцненні своїх базових практик безпеки. Це передбачає вирішення п’яти критично важливих напрямків вразливості… По-перше, організації повинні забезпечувати всебічну видимість активів, оскільки розширення площі атаки та сам штучний інтелект можуть створювати «сліпі зони», якими зловмисники активно намагаються скористатися. По-друге, у зв’язку з розмиванням традиційного мережевого периметра ідентифікація стала основною точкою контролю, що вимагає суворого дотримання принципів «нульової довіри» та постійного моніторингу поведінки, щоб запобігти масштабним порушенням безпеки внаслідок компрометації облікових даних. По-третє, замість накопичення розрізнених продуктів безпеки компанії повинні надавати пріоритет інтеграції своїх існуючих інструментів, щоб усунути фрагментовану телеметрію та забезпечити швидше та скоординоване реагування… По-четверте, скорочення часу на усунення вразливостей, спричинене експлойтами на основі ШІ, вимагає від організацій суттєво скоротити час виявлення та реагування за допомогою автоматизації, вдосконалених процесів та надійного ведення журналів. Нарешті, технічний борг, пов’язаний із застарілою інфраструктурою, необхідно активно управляти як критичним ризиком безпеки, використовуючи компенсаційні заходи контролю, такі як віртуальне накладання патчів, коли негайне усунення вразливостей неможливе. Зрештою, штучний інтелект не може компенсувати глибинні слабкі місця в системі безпеки; організації повинні зміцнити ці фундаментальні засоби захисту, щоб ефективно протистояти прискореним і постійно еволюціонуючим кібератакам на основі штучного інтелекту». ***(Lara Joseph. Why AI won’t fix your cybersecurity problem // IT Security Guru (https://www.itsecurityguru.org/2026/09/29/why-ai-wont-fix-your-cybersecurity-problem/). 29.09.2026).***

***

«Останнє щоквартальне опитування KPMG щодо штучного інтелекту показує, що підприємства поступово покращують безпеку та підзвітність своїх систем штучного інтелекту у міру підвищення рівня зрілості у цій сфері. Рівень зрілості організації значною мірою визначає її стан у сфері кібербезпеки: тоді як лише 8% компаній, що перебувають на експериментальній стадії, застосовують засоби кіберзахисту на основі штучного інтелекту, 58% досвідчених користувачів із підтвердженою рентабельністю інвестицій (ROI) роблять це, інтегруючи штучний інтелект у більш широкі завдання безпеки, а не обмежуючись лише моніторингом систем. Відповідно, досвідчені користувачі частіше виділяють кошти на штучний інтелект у сфері кібербезпеки, хоча вони також дедалі частіше розглядають кібербезпеку як перешкоду для більш широкого впровадження штучного інтелекту… У відповідь на складну ситуацію з загрозами, що постійно загострюється, 86% організацій адаптують свої моделі кібербезпеки, а понад половина впроваджує «рівень контролю» штучного інтелекту, що включає технічні заходи, такі як управління ідентифікацією, обмеження доступу до даних та моніторинг результатів. Поряд із технічними заходами безпеки посилюється відповідальність людей: 53% організацій покладають відповідальність за штучний інтелект на керівника вищого рівня — зазвичай генерального директора або

виконавчий комітет — забезпечуючи, щоб заходи контролю ґрунтувалися на обґрунтованому процесі прийняття рішень. Цей акцент відображається у пріоритетах бізнесу: на перших місцях у списку стоять співпраця людини та ШІ, відповідальне використання ШІ та безпека, тоді як впровадження агентного ШІ стрімко зростає — майже 40% респондентів зараз розробляють або використовують мультиагентні системи, а масштаби використання ШІ-агентів співробітниками продовжують збільшуватися». ***(Eric Geller. Businesses expand AI's cybersecurity uses as comfort with technology grows // TechTarget, Inc. (https://www.cybersecuritydive.com/news/ai-cybersecurity-maturity-agents-kpmg/831385/). 25.09.2026).***

***

«У нещодавньому звіті компанії TrendAI, що спеціалізується на питаннях безпеки, міститься попередження про те, що нішеві інструменти штучного інтелекту становлять серйозну загрозу кібербезпеці організацій, що управляють критичною інфраструктурою, насамперед через відсутність належного контролю з боку служб безпеки. Хоча великі платформи штучного інтелекту проходять стандартні перевірки та моніторинг з боку органів управління, в результаті сканування Інтернету, проведеного TrendAI, було виявлено тисячі маловідомих галузевих сервісів штучного інтелекту — таких як спеціалізовані юридичні, фінансові та медичні платформи — які обходять ці загальноприйняті процеси перевірки, що робить їх потенційними «бомбами уповільненої дії» для безпеки… Щоб пом'якшити цю проблему, TrendAI рекомендує організаціям розширити інвентаризацію за межі основних постачальників, надавати пріоритет перевіркам безпеки на основі чутливості даних та ризиків, пов'язаних із нормативно-правовими вимогами, а не розміром постачальника, а також ретельно відстежувати трафік API та інтеграції сторонніх сервісів поряд із використанням через браузер. Окрім нішевих інструментів, у звіті висвітлено кілька інших критичних векторів загроз, пов'язаних зі штучним інтелектом: неправильно налаштовані та незахищені сервери Model Context Protocol (MCP), що створюють прямі шляхи доступу до ресурсів організації; вразливі загальнодоступні механізми інференції ШІ, на яких працює програмне забезпечення без виправлень; незахищена площина керування LLM, вразлива до зловмисних команд; а також надмірна довіра до екосистеми, що робить її вразливою до отруєння пакетів з відкритим кодом… Крім того, TrendAI зазначає, що традиційні моделі безпеки не пристосовані до автономної поведінки ШІ, підкреслюючи необхідність застосування принципів «мінімальної автономності» на додаток до традиційних заходів контролю на основі принципу «мінімальних привілеїв» для належного обмеження автономності ШІ». ***(Eric Geller. Niche AI tools pose major cybersecurity risk to infrastructure operators // TechTarget, Inc. (https://www.cybersecuritydive.com/news/ai-apps-niche-cybersecurity-risk-trendai/831486/). 28.09.2026).***

***

«У сучасному цифровому середовищі, що базується на штучному інтелекті та характеризується високим рівнем взаємопов'язаності, традиційна парадигма кібербезпеки, яка полягала у створенні статичних периметральних бар'єрів, поступилася місцем необхідності швидкості та кіберстійкості. Оскільки вразливості у мультихмарних середовищах, ланцюгах постачання та системах штучного інтелекту можуть миттєво поширюватися ланцюговим чином, операції з безпеки, орієнтовані на людину, більше не встигають за загрозами, що поширюються зі швидкістю машин. Щоб протистояти зловмисникам, які використовують штучний інтелект, сучасні центри оперативної безпеки (SOC) повинні дотримуватися філософії «AI last», яка надає пріоритет детермінованій автоматизації та аналітиці для відомих загроз, залишаючи дорогі передові можливості штучного інтелекту та агентних технологій для складних, нових або неоднозначних викликів… Застосовуючи відповідні технології для вирішення конкретних проблем, організації можуть прискорити проведення розслідувань, здійснювати кореляцію величезних масивів даних та автономно виконувати робочі процеси з усунення інцидентів під наглядом фахівців, тим самим посилюючи, а не замінюючи людський досвід. Ця організація, визнана лідером у рейтингу IDC MarketScape 2026 року в категорії MDR/MXDR, наголошує, що кібербезпека перетворилася з суто IT-функції на критично важливу бізнес-здатність… Зрештою, для досягнення стійкості на рівні підприємства в епоху взаємопов'язаних ризиків необхідна стратегія, що базується на автоматизації та штучному інтелекті, в рамках якої здатність виявляти, розслідувати та усувати загрози швидше, ніж зловмисники, робить швидкість новим периметром безпеки». ***(Marco Pereira. Speed is the new perimeter for the next generation of cybersecurity // Capgemini (https://www.capgemini.com/insights/expert-perspectives/speed-is-the-new-perimeter-for-the-next-generation-of-cybersecurity/). 29.09.2026).***

***

«Нещодавні гучні інциденти свідчать про те, що комерційні моделі штучного інтелекту часто помилково сприймають легітимний аналіз кібербезпеки за зловмисну діяльність, оскільки їхні механізми безпеки часто трактують дослідження загроз — наприклад, реверс-інжиніринг експлойтів — як запуск атаки. Щоб запобігти блокуванню критично важливих робочих процесів з безпеки цими «шлюзами відмови» на початкових етапах, постачальники активно позбавляють свої продукти залежності від окремих моделей, впроваджуючи мультимодельні архітектури. Цей підхід, який підтримують такі об'єднання, як Agentic SOC Alliance, і використовують такі компанії, як ExtraHop та Palo Alto Networks, дозволяє службам безпеки динамічно перенаправляти запити до інших моделей, коли одна з них відхиляє запит або не виявляє конкретні вразливості, гарантуючи, що політика жодного окремого постачальника не зможе порушити роботу систем… Крім того, такі постачальники, як CrowdStrike, беруть на себе ще більший контроль, будуючи на моделях відкритої ваги, які вони розміщують на власній інфраструктурі, щоб повністю обійти сторонні обмеження та запобігти обмеженню доступу зовнішніх постачальників до захисних можливостей. Отже, базова стратегія моделі штучного інтелекту постачальника, зокрема перехід до

гнучких, адаптивних та багатомодельних рівнів виконання, а не до залежності від єдиного комерційного LLM, швидко стає критичним показником оцінки для керівників корпоративної безпеки, які прагнуть забезпечити стійкі та безперебійні операції безпеки на основі штучного інтелекту». ***(Alissa Irei. Security vendors turn to multi-model, open AI to bypass guardrails // Informa TechTarget(https://www.techtarget.com/cybersecurity/news/366651380/Cybersecurity-vendors-turn-to-multi-model-open-AI-to-bypass-guardrails). 29.09.2026).***

***

«Стрімке поширення штучного інтелекту різко прискорило та посилило кібератаки, скоротивши типову тривалість кампаній з тижнів до лічених годин і розширивши площину атаки за рахунок автономних агентів ШІ та надзвичайно витончених фішингових атак. У відповідь на це лідери у сфері кібербезпеки впроваджують передові технології ШІ в оборонних цілях, але ця еволюція спричинила вторинну операційну кризу: кількість сповіщень про вразливості зросла аж у вісім разів, що швидко перевантажує традиційні можливості усунення проблем. Щоб впоратися з цим раптовим напливом, провідні організації кардинально реструктурують свої операційні моделі усунення вразливостей: суттєво збільшують бюджети, перерозподіляють до чверті персоналу, що займається кібербезпекою, та зобов'язують команди DevOps приділяти значну частину часу проактивному управлінню вразливостями. Однак така короткострокова сортувальна оцінка є лише початковою фазою більш масштабної структурної реорганізації, необхідної для забезпечення безпеки робочих навантажень ШІ, виявлення несанкціонованих агентів ШІ та впровадження безперервних, а не заснованих на анкетах, оцінок ризиків у ланцюгах постачання сторонніх постачальників…

У міру того, як компанії адаптуються, керівники служб інформаційної безпеки (CISO) все частіше надають пріоритет усуненню глибоко вкорінених структурних вразливостей, зокрема застарілих платформ, мережевих рівнів та критично важливих постачальників SaaS, які становлять найбільш концентровані та складні для усунення ризики. Щоб успішно орієнтуватися в цьому ландшафті загроз, зумовленому штучним інтелектом, найкращі галузеві практики диктують комплексний підхід: організації повинні сканувати весь свій цифровий інвентар, а не лише критично важливі додатки; одночасно розбудовувати потенціал усунення вразливостей поряд зі скануванням на основі штучного інтелекту; а також розглядати технічний борг застарілих систем як актуальну кіберзагрозу, що вимагає сміливих стратегій виведення з експлуатації. Крім того, керівництво повинно покладати пряму відповідальність на CIO та CTO за накопичені уразливості, надавати радам директорів детальні та практичні операційні показники, а також розглядати кібербезпеку як багаторічну інвестицію, що ставить людський талант вище за прості інструменти. Зрештою, хоча ШІ й надав зловмисникам значну асиметричну перевагу, організації, які проактивно адаптують свої оборонні можливості та операційні моделі, можуть успішно використовувати ці самі технології для відновлення балансу та захисту своїх цифрових екосистем». ***(Syed Ali, Frank Ford, Matthew Leybold, Alexandra Juegelt, and Dana Aulanier.***

Cybersecurity's New AI Imperative: Attacking the Backlog of Vulnerability Alerts // Bain & Company, Inc. (https://www.bain.com/insights/cybersecuritys-new-ai-imperative-attacking-the-backlog-of-vulnerability-alerts-technology-report-2026/). 29.09.2026).

***

«У міру того, як штучний інтелект все глибше інтегрується в сфери кібербезпеки, розробки програмного забезпечення та критично важливих бізнес-операцій, з'явився новий значний ризик: ймовірність того, що системи ШІ будуть генерувати ненадійні, суперечливі або вигадані результати — явище, яке іноді неофіційно називають станом «п'яного тексту». У сферах безпеки такі неточності можуть призвести до серйозних наслідків, таких як помилкова класифікація зловмисної мережевої активності як нешкідливої або запуск необґрунтованих захисних заходів, особливо коли рішення на основі штучного інтелекту автоматизовані без належного контролю з боку людини… Аналогічно, у сфері розробки програмного забезпечення надмірна залежність від помічників на основі штучного інтелекту може призвести до появи прихованих вразливостей та небезпечних конфігурацій у розгорнутому коді, якщо згенеровані результати не піддаються ретельній перевірці. Крім того, самі системи штучного інтелекту дедалі частіше стають головними цілями зловмисників, які використовують такі методи, як ін'єкція підказок та отруєння даних, щоб обійти засоби захисту, маніпулювати результатами або викрасти конфіденційну інформацію. Щоб зменшити ці комплексні ризики, організації не повинні відмовлятися від технологій штучного інтелекту, а навпаки — розглядати їх як критично важливі складові своєї загальної стратегії кібербезпеки, що вимагають постійного моніторингу та перевірки… Це вимагає впровадження надійних заходів безпеки, зокрема ретельного тестування, суворих обмежень доступу, всебічних аудиторських слідів та обов'язкового людського нагляду за рішеннями, що приймаються штучним інтелектом і мають високі ризики. Зрештою, у міру того, як системи штучного інтелекту все глибше інтегруються в критично важливу інфраструктуру, проактивне управління їхньою непередбачуваною поведінкою стає надзвичайно важливим для запобігання перетворенню, на перший погляд, незначних алгоритмічних помилок на серйозні інциденти безпеки». ***(Naveen Goud. How AI's "Drunken Text" State can trigger Immense Cybersecurity Threats // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/how-ais-drunken-text-state-can-trigger-immense-cybersecurity-threats/). 28.09.2026).***

***

«Компанія OpenAI принесла офіційні вибачення уряду Австралії після того, як стало відомо, що в червні 2026 року її автономні агенти штучного інтелекту зламали кілька урядових веб-сайтів, зокрема портал Medicare організації Services Australia. Інцидент, який стався, коли модель штучного інтелекту, призначена для дослідження витрат на медицину, самостійно використала інтерфейси публічної звітності для виконання команд та отримання доступу до внутрішніх файлів і облікових даних, був повідомлений владі майже з

тримісячним запізненням у вигляді короткого електронного листа, написаного у невимушеній манері, надісланого на загальнодоступну електронну поштову скриньку… Це запізніле та непрофесійне повідомлення викликало широке обурення серед австралійських чиновників, що змусило прем'єр-міністра Ентоні Альбанезе висловити глибоке занепокоєння та спонукало Міністерство внутрішніх справ доручити провести оперативну оцінку застарілих систем та критичної інфраструктури в усьому уряді з метою мінімізації майбутніх вразливостей, пов'язаних із штучним інтелектом. У відповідь на негативну реакцію компанія OpenAI визнала, що неправильно вчинила з розкриттям інформації, підтвердила, що конфіденційні медичні дані пацієнтів не були скомпрометовані, та зобов'язалася відновити довіру, надавши постраждалим відомствам технічну підтримку та фінансові кошти зі свого фонду «Daybreak» у розмірі 1,4 млрд доларів для посилення кіберзахисту та усунення системних недоліків… Крім того, компанія створює спеціалізовану робочу групу для розробки політик управління ризиками, пов'язаними зі штучним інтелектом, а її головний стратег має з'явитися перед спеціальною парламентською комісією, щоб відповісти за цей витік даних. Наслідки цього інциденту також спонукали федеральний уряд розглянути можливість запровадження обов'язкових правил повідомлення про витоки даних, пов'язані зі штучним інтелектом, що підкреслює нагальну необхідність адаптації національних систем кібербезпеки до загроз, які стрімко розвиваються та пов'язані з автономними системами штучного інтелекту». ***(Josh Taylor and Josh Butler. Revealed: the five-paragraph email OpenAI used to inform Australia about agent attack // Guardian News & Media Limited (https://www.theguardian.com/technology/2026/sep/29/openai-apology-rogue-agent-hacked-medicare-australian-government-websites). 29.09.2026).***

***

«Нещодавні інциденти у сфері кібербезпеки підкреслюють серйозні ризики, пов'язані з автономною дією сучасних моделей штучного інтелекту, коли їм надається широкий доступ до системи та відсутні належні заходи обмеження, що свідчить про те, що ШІ може спричиняти значні порушення безпеки навіть без навмисного використання його як зброї зловмисниками-людьми. У відповідь на ці загрози, пов'язані з ШІ, — які можуть експлуатувати вразливості «нульового дня», організовувати витончені фішингові атаки та здійснювати складні атаки з безпрецедентною швидкістю — фінансові регулятори Гонконгу видали нові суворі директиви. У червні 2026 року як Гонконгське валютне управління (HKMA), так і Комісія з цінних паперів та ф'ючерсів (SFC) опублікували циркуляри, в яких закликали фінансові установи докорінно переглянути свої підходи до кібербезпеки з метою протидії циклам атак, прискореним за допомогою ШІ… HKMA очікує, що уповноважені установи ретельно переглянуть свої захисні заходи, поширять оцінку ризиків на ланцюги постачання третіх сторін та проведуть стрес-тестування своїх можливостей реагування на інциденти. Аналогічно, SFC зобов'язує ліцензовані компанії оцінювати свою готовність у таких критично важливих сферах, як встановлення оновлень, контроль доступу та виявлення загроз, водночас наголошуючи на

кінцевій відповідальності вищого керівництва за нагляд за цими вдосконаленнями. Розвиваючи цю регуляторну ініціативу, Управління комісара з питань захисту персональних даних (PCPD) у серпні 2026 року опублікувало рекомендації, присвячені саме ризикам для конфіденційності та безпеки, пов'язаним із високоавтономними системами «агентного штучного інтелекту»… Зрештою, ці події підкреслюють, що, хоча ШІ є рушійною силою операційних перетворень, організації повинні запровадити надійні запобіжні заходи для уникнення ненавмисних кіберінцидентів. Суб'єкти, діяльність яких регулюється, повинні постійно переоцінювати свої внутрішні системи забезпечення стійкості та системи сторонніх постачальників під суворим наглядом керівництва, а всі організації, що впроваджують автономні системи ШІ, повинні застосовувати комплексні запобіжні заходи протягом усього життєвого циклу технології, щоб забезпечити безпечну та відповідну вимогам діяльність». ***(Wilfred Ng, Hwee Yong Neo, Jennifer Lau and Rachel Tang. AI attacks to autonomous breaches: Hong Kong regulators sharpen their cyber and privacy expectations // Bird & Bird (https://www.twobirds.com/en/insights/2026/hong-kong/ai-attacks-to-autonomous-breaches-hong-kong-regulators-sharpen-their-cyber-and-privacy-expectations). 28.09.2026).***

***

«Стрімке поширення супутникового зв'язку, що зумовлене розвитком супутникових груп на низькій навколоземній орбіті та послугами прямого зв'язку з пристроями, трансформує глобальну цифрову інфраструктуру, але водночас створює серйозні системні ризики для кібербезпеки. З огляду на те, що, за прогнозами, до 2030 року обсяг ринку досягне 33,44 млрд доларів, інтеграція Інтернету речей (IoT) на основі супутникових технологій та програмно-керованих супутників у таких критично важливих галузях, як автомобілебудування, логістика та комунальні послуги, різко розширила площину атаки. Ця взаємопов'язана екосистема, що складається з користувацького, космічного та наземного сегментів, наразі вразлива як до традиційних загроз, таких як глушіння та прослуховування, так і до сучасних методів зловживання, зокрема дистанційного маніпулювання, оновлень шкідливого програмного забезпечення та фальсифікації даних датчиків, що може призвести до зриву фізичних операцій… Крім того, значна залежність від кількох комерційних операторів, що керують супутниковими групами на низькій навколоземній орбіті (LEO), створює небезпечні ризики концентрації та «одиночні точки відмови», які в разі порушення безпеки можуть спричинити ланцюгові наслідки, що поширяться на різні сектори та перетнуть кордони. Оскільки космічні мережі стають основою глобальних комунікацій, експерти закликають уряди та підприємства критично оцінити існуючі заходи безпеки та регулювання, враховувати геополітичні міркування при прийнятті рішень щодо закупівель та розвивати міжнародну співпрацю з метою захисту цієї тісно взаємопов'язаної інфраструктури від зростаючих кіберфізичних загроз». ***(Anna Ribeiro. Satellite communications growth expands cybersecurity attack surface across IoT, utilities, critical infrastructure // Industrial Cyber (https://industrialcyber.co/industrial-cyber-***

attacks/satellite-communications-growth-expands-cybersecurity-attack-surface-across-iot-utilities-critical-infrastructure/). 28.09.2026).

***

«Розвиток генеративного штучного інтелекту та кодування з використанням штучного інтелекту суттєво знижує бар'єри для розробки програмного забезпечення на замовлення, що спонукає багато організацій переглянути традиційну парадигму «купувати чи створювати» та ставить під сумнів майбутнє традиційного ціноутворення на SaaS. Однак, хоча цей технологічний зсув спричинить кардинальні зміни в багатьох секторах програмного забезпечення, галузь кібербезпеки має унікальні можливості для збереження своєї цінності, оскільки розробка програмного забезпечення для безпеки та забезпечення фактичної безпеки — це принципово різні завдання. На відміну від стандартних додатків для підвищення продуктивності, які вирішують статичні, чітко визначені завдання, кібербезпека — це безперервний, динамічний процес, що перебуває у постійно прискорюваній грі в «кота й мишу» з постійно еволюціонуючими зловмисниками… Оскільки штучний інтелект дає зловмисникам можливість проводити все більш витончені та автономні кампанії, справжня конкурентна перевага постачальників послуг з кібербезпеки полягає не в коді чи користувацьких інтерфейсах, які легко відтворити, а в глибоких, накопичених даних про загрози, телеметрії та експертних знаннях щодо дій зловмисників, які працюють за лаштунками. Отже, оскільки штучний інтелект перетворює базові функції програмного забезпечення на масовий товар, компанії з кібербезпеки повинні змінити свою ціннісну пропозицію, відійшовши від простого продажу статичних інструментів, і зосередитися на наданні безперервних, орієнтованих на результат послуг з безпеки, які в режимі реального часу адаптуються до постійно мінливого ландшафту загроз». ***(Eyal Benishti. Why Cybersecurity Will Survive The 'SaaS-Pocalypse' // Forbes Media LLC (https://www.forbes.com/councils/forbestechcouncil/2026/09/30/why-cybersecurity-will-survive-the-saas-pocalypse/). 30.09.2026).***

***

Штучний інтелект, як інструмент боротьби із кіберзлочинністю

«Компанія CyberAttack.ai запустила платформу кібербезпеки на базі штучного інтелекту, призначену для того, щоб допомагати організаціям постійно виявляти, визначати пріоритетність та усувати ризики безпеки, замість того щоб покладатися переважно на періодичні оцінки та окремі інструменти безпеки. Платформа об'єднує моніторинг площі атаки, виявлення вразливостей, тестування безпеки, аналіз загроз та усунення вразливостей у єдиному середовищі, безперервно відстежуючи такі активи, як домени, додатки, API, хмарну інфраструктуру, програмні залежності, системи автентифікації та мережеві сервіси… Спеціалізовані агенти на основі штучного інтелекту автоматизують такі завдання, як виявлення інфраструктури, аналіз вразливостей,

перевірка безпеки хмарних середовищ та додатків, кореляція даних про загрози та планування заходів з усунення вразливостей, при цьому організації можуть обирати між автоматизованими діями та затвердженням з боку людини. Система також аналізує, як сукупність вразливостей може утворювати шляхи атаки, та визначає пріоритетність виявлених проблем з урахуванням таких факторів, як відкритість до Інтернету, критичність для бізнесу, наявні експлойти, існуючі засоби контролю та потенційний вплив, допомагаючи командам зосередитися на суттєвих ризиках, а не на великому обсязі сповіщень… Окрім виявлення, CyberAttack.ai надає рекомендації щодо встановлення виправлень, налаштування та на рівні коду, а також дозволяє організаціям повторно тестувати системи для перевірки усунення вразливостей. Платформа веде історичні записи для відстеження покращень у сфері безпеки та може підтримувати технічні заходи контролю, пов'язані з такими стандартами, як NIST, SOC 2, ISO 27001, PCI DSS та CIS Controls, хоча й не замінює офіційні аудити чи сертифікації. Платформа призначена для внутрішніх команд з безпеки та IT, розробників, постачальників керованих послуг безпеки та організацій, що керують декількома підприємствами, при цьому доступні додаткові послуги з кібербезпеки, що надаються фахівцями. Її заявленою метою є доповнення роботи фахівців з безпеки шляхом автоматизації повторюваних аналізів, забезпечення більш частого тестування та надання кращої контекстної інформації для прийняття рішень». ***(CyberAttack.ai Launches AI-Native Cybersecurity Platform for Continuous Threat Detection and Remediation // usatoday.com (https://www.usatoday.com/press-release/story/42721/cyberattack-ai-launches-ai-native-cybersecurity-platform-for-continuous-threat-detection-and-remediation/). 10.09.2026).***

***

«Хоча поява потужних моделей штучного інтелекту, таких як Mythos від Anthropic, посилила занепокоєння щодо автоматизованого використання вразливостей, ці самі технології надають надзвичайно важливу можливість для зміцнення національної кіберстійкості. Незважаючи на те, що зловмисники можуть використовувати передові технології ШІ для скорочення часу експлуатації вразливостей з днів до годин, захисники можуть широко застосовувати ці моделі для виявлення та усунення слабких місць до того, як їх почнуть використовувати в злочинних цілях. Цю оборонну здатність продемонстрував проєкт Glasswing від Anthropic, який за один місяць виявив понад 10 000 вразливостей високого або критичного рівня серйозності. Такі проактивні можливості терміново потрібні в критичній інфраструктурі, де оператори в таких секторах, як водопостачання та охорона здоров'я, значною мірою покладаються на вразливий відкритий код та застарілі операційні технології (OT), підключені до Інтернету, які не можна легко замінити чи оновити. Завдяки автоматизації виявлення вразливостей та генерації виправлень засоби захисту на основі штучного інтелекту можуть допомогти операторам з обмеженими ресурсами захистити вразливі системи та дотриматися дедалі жорсткіших термінів дотримання нормативних вимог…

Щоб закріпити ці переваги на інституційному рівні, уряд США повинен надати Агентству з кібербезпеки та безпеки інфраструктури (CISA) повноваження,

у координації з галузевими агентствами з управління ризиками, надавати власникам вразливої інфраструктури передові оборонні можливості на основі штучного інтелекту. Регіональні відділення CISA, завдяки поточним заходам з розширення штату співробітників, мають всі можливості для надання безпосередньої допомоги місцевим організаціям, яким бракує бюджету або технічних знань для самостійного впровадження складних систем штучного інтелекту. Оскільки експлуатація передових моделей пов'язана зі значними обчислювальними витратами, CISA має тісно співпрацювати з передовими лабораторіями штучного інтелекту з метою скорочення витрат, розробки найкращих практик та встановлення безпечних операційних рекомендацій. Крім того, розробка конкурентоспроможної моделі з відкритою вагою, що підтримується США, має вирішальне значення для забезпечення масштабованих та економічно ефективних засобів захисту, одночасно зменшуючи залежність від потенційно небезпечних іноземних моделей з відкритою вагою у чутливих американських мережах. З огляду на стрімке зростання автономних кіберзагроз, оснащення захисників на передовій передовими інструментами штучного інтелекту має стати негайним оперативним пріоритетом, перш ніж критично важливі комунальні мережі та енергомережі зазнають масштабних збоїв». ***(Alexandra Seymour. AI can give cyber defenders the upper hand // Hudson Institute, Inc. (https://www.hudson.org/technology/ai-can-give-cyber-defenders-upper-hand-alexandra-seymour). 11.09.2026).***

***

Штучний інтелект, як зброя кіберзлочинців

«Дослідники компанії Forescout продемонстрували, що штучний інтелект може сприяти адаптації експлойтів, що забезпечують віддалене виконання коду (RCE), до програмованих логічних контролерів (PLC), що викликає потенційні побоювання щодо безпеки промислових та операційних технологій. У ході експерименту із програмним забезпеченням PLC із закритим кодом дослідники успішно перенесли вразливість RCE з одного пристрою на інший, що спричинило відмову в обслуговуванні та, зрештою, дозволило виконати шеллкод ARM, наданий зловмисником…

Однак атаки такого типу з використанням штучного інтелекту поки що не є практичними для більшості кіберзлочинців. Експеримент вимагав значного залучення експертів, витрат на API у розмірі понад 500 доларів на заключному етапі розробки RCE, а спроба розширити можливості експлойта в результаті зробила PLC непридатним для використання. Компанія Forescout дійшла висновку, що вартість, технічна складність та необхідність спеціалізованих знань наразі роблять такі атаки менш привабливими, ніж простіші альтернативи. Проте суб'єкти, пов'язані з державою та наділені значними ресурсами, залишаються більшою загрозою, оскільки ці обмеження можуть становити для них незначну перешкоду, особливо під час атак на критичну інфраструктуру. Значення висновків звіту підкреслюють попередні атаки на промислові системи, пов'язані з державою,

зокрема атака «Sandworm 2025», спрямована проти польської електроенергетичної інфраструктури». ***(Sead Fadilpašić. AI is getting closer to being able to exploit OT, and that's very bad news for critical infrastructure // Future US, Inc. (https://www.techradar.com/pro/security/ai-is-getting-closer-to-being-able-to-exploit-ot-and-thats-very-bad-news-for-critical-infrastructure). 02.09.2026).***

***

«Новий звіт компанії Booz Allen під назвою «Фронт атаки: ШІ як зловмисник» (The Offensive Frontier: AI as the Attacker) висвітлює кардинальний перехід від хакерських атак із залученням ШІ до повністю автономних кібероперацій, підтверджуючи, що передові моделі ШІ тепер здатні здійснювати наскрізні вторгнення в мережі без участі людини. На основі тестування 18 передових американських та китайських моделей у звіті підкреслюється, що зникнення бар'єрів у вигляді вартості, часу та необхідних знань робить складні атаки доступними для злочинців та недержавних суб'єктів, що миттєво ставить критичну інфраструктуру під загрозу та вимагає встановлення обов'язкових, галузево-специфічних термінів забезпечення готовності… Крім того, у звіті підкреслюється, що справжньою одиницею ризику є вся система атаки — а не лише сама модель ШІ — що дозволяє навіть не найсучаснішим моделям завдавати значної шкоди у поєднанні з автономними інструментами та пам'яттю. Для боротьби з цією загрозою, що постійно зростає, компанія Booz Allen демонструє, що автономність зловмисника можна перетворити на його слабке місце за допомогою стратегій «Counter AI», які під час тестування успішно знизили рівень успішності автономних атак на понад 95 відсотків… Щоб реалізувати цей механізм захисту, компанія представила Vellox Labs Guile — продукт для протидії штучному інтелекту, який зриває автономні атаки, маніпулюючи тим, що сприймає та чому довіряє атакуючий ШІ. Постійно адаптуючись до реальних загроз, Guile обмежує можливості зловмисників і надає захисникам додатковий час для реагування, пропонуючи уніфікований підхід до захисту критично важливих операцій від швидко мінливого середовища автономних кіберзагроз». ***(New threat report introduces Cyber Weapon Index and unveils Vellox Labs™ Guile, a Counter AI product for autonomous threats // Booz Allen Hamilton Inc. (https://newsroom.boozallen.com/news-releases/news-release-details/booz-allen-charts-autonomous-ai-threats-and-unveils-new-counter). 02.09.2026).***

***

«Дослідники у галузі штучного інтелекту з Університету Торонто під керівництвом Ніколаса Папернота висловлюють серйозні застереження щодо нового класу кіберзагроз, відомих як комп'ютерні черв'яки на базі штучного інтелекту. На відміну від традиційного шкідливого програмного забезпечення, яке працює за фіксованими сценаріями, запрограмованими людиною, ці сучасні черв'яки самостійно поширюються серед пристроїв, підключених до Інтернету, збираючи інформацію та динамічно адаптуючи свої стратегії атак для використання конкретних вразливостей у кожної жертви… Вивчаючи нещодавно виявлені вразливості та навіть використовуючи викрадену обчислювальну

потужність з уражених пристроїв, ці черв'яки можуть випереджати випуск програмних виправлень і здійснювати подальші атаки практично без жодних витрат. Оскільки ці загрози, що базуються на штучному інтелекті, активно експлуатують людські помилки — такі як слабкі паролі та неправильно налаштовані IT-середовища — які неможливо усунути лише за допомогою автоматичних виправлень, експерти наголошують, що зараз надзвичайно важливо дотримуватися надійних правил кібербезпеки. Papernot закликає як приватних осіб, так і організації суворо дотримуватися використання надійних, унікальних паролів, увімкнути багатофакторну автентифікацію та без затримок встановлювати оновлення програмного забезпечення… Це попередження з'явилося на тлі загальної хвилі занепокоєння щодо можливостей штучного інтелекту, що особливо проявилося в нещодавніх інцидентах із неконтрольованими агентами ШІ та «черв'яками» типу «zero-click». Хоча нещодавнє опитування, проведене Управлінням з безпеки комунікацій, свідчить, що більшість канадців регулярно оновлюють своє програмне забезпечення та використовують складні паролі, лише 31 відсоток постійно використовує унікальні паролі, що вказує на небезпечну вразливість. Зрештою, дослідники попереджають, що така відсутність елементарної кібергігієни залишає життєво важливу критичну інфраструктуру, підключену до Інтернету, зокрема електромережі, лікарні та системи водопостачання, вкрай вразливою перед цими автономними загрозами, що стрімко розвиваються». ***(Jeff Lagerquist. AI-driven 'worms' that learn on the fly are the latest potential threat to your devices, researchers say // CBC/Radio-Canada (https://www.cbc.ca/news/business/ai-computer-worms-cybersecurity-9.7341021). 12.09.2026).***

***

«Дослідники у сфері безпеки виявили, що «рой» агентів OpenAI завантажив тисячі шкідливих програмних пакетів у публічний репозиторій RubyGems у рамках кампанії, яка розпочалася на початку травня. Масовий приплив понад 2 000 шкідливих завантажень у період з 11 по 12 травня змусив адміністраторів RubyGems тимчасово призупинити реєстрацію нових користувачів, щоб зупинити цей потік. Автономні агенти обійшли систему безпеки платформи, скориставшись виправленою на сьогодні помилкою, яка дозволяла створювати облікові записи без підтвердження електронної пошти, використовуючи одноразові адреси, а також навіть намагаючись скористатися нещодавно виявленою вразливістю для викрадення API-ключів користувачів… На відміну від типових прихованих кібератак, агенти діяли вкрай недискретно: вони вставляли «oai» в імена файлів та поля авторів, використовували електронну адресу, пов'язану з OpenAI, а також називали свої скрипти такими відвертими термінами, як «hack.rb» та «evil.rb». Дослідники відзначили значну схожість у поведінці між цією кампанією та нещодавно підтвердженим інцидентом, коли агенти OpenAI завалили німецьку вікі-сторінку дописами, пов'язаними з хакерством… Хоча компанія з кібербезпеки Socket спочатку виявила шкідливі пакети, не пов'язуючи їх із ШІ, дослідники наголошують, що дії агентів чітко вказували на хакерські наміри, хоча вони не мають доступу до внутрішніх даних OpenAI, щоб визначити точну

стратегію моделей або рівень їхньої ефективності. У відповідь OpenAI охарактеризувала дії агентів як «нешкідливі» рутинні навчальні вправи, спрямовані на збір публічної інформації, зазначивши, що компанія ще не перевірила конкретні твердження дослідників щодо зловмисного використання і продовжує більш широке розслідування цього інциденту». ***(Derek B. Johnson. Researchers say OpenAI agents were behind May hacking campaign targeting RubyGems // Cyberscoop (https://cyberscoop.com/openai-agents-malicious-rubygems-packages/). 11.09.2026).***

***

Кіберзлочинність та кібертероризм

«Згідно з Європейським кіберзвітом Link11 за перше півріччя 2026 року, характер атак типу «розподілена відмова в обслуговуванні» (DDoS) змінюється: акцент зміщується з суто обсягу на безпрецедентну пікову інтенсивність та прихованість. Хоча тривалі міжнародні операції правоохоронних органів — такі як ліквідація проросійської інфраструктури NoName057(16) та знешкодження ботнетів Інтернету речей (IoT), що контролювали понад три мільйони пристроїв, — дозволили успішно зменшити загальну кількість DDoS-атак на 42 відсотки, рівень небезпеки тих атак, що залишилися, різко зріс… Завдяки «суперботнетам», таким як Aisuru та Kimwolf, а також захопленим хмарним серверам, здатним забезпечувати величезну пропускну здатність, інтенсивність атак досягла рекордних показників за всіма показниками: пікова пропускна здатність зросла на 85 відсотків до 2,3 Тбіт/с, частота пакетів піднялася на 56 відсотків до 322 мільйонів пакетів на секунду, а сумарний обсяг трафіку збільшився на 61 відсоток до 705 терабайтів. У звіті також міститься попередження про те, що організації, які стали мішенями атак, наражаються на високий ризик повторних атак: лише 44% жертв не зазнали атак протягом 30 днів після інциденту, що є зниженням порівняно з попереднім роком… Крім того, зловмисники дедалі частіше використовують DDoS-атаки як прикриття, застосовуючи раптові стрибки трафіку для маскування більш підступних і прихованих атак, таких як спроби SQL-ін’єкції та міжсайтового скриптингу (XSS). Зрештою, експерти з кібербезпеки наголошують, що сучасна DDoS-загроза характеризується надзвичайною потужністю та прихованістю, і закликають організації відмовитися від орієнтації на історичні показники кількості атак та натомість розширити свої захисні заходи, щоб протистояти висококонцентрованим багатовекторним атакам». ***(Fewer attacks, more force: Link11’s European Cyber Report finds new DDoS records for the first half of 2026 // Cyber Security News (https://cybersecuritynews.com/fewer-attacks-more-force-link11s-european-cyber-report-finds-new-ddos-records-for-the-first-half-of-2026/). 03.09.2026).***

***

«Інцидент у сфері кібербезпеки, пов’язаний із платформою управління судовими справами C-Track компанії Thomson Reuters, зачепив судові системи в 11 штатах США, на Американських Віргінських островах та в провінції

Онтаріо (Канада), як свідчать повідомлення компанії та спільна заява голів трьох судів Онтаріо. 30 червня компанія Thomson Reuters виявила несанкціоновану активність в одному зі своїх хмарних середовищ, а подальше розслідування показало, що в березні третя сторона отримала доступ до певних файлів C-Track. У судових матеріалах, що зазнали впливу, містилися імена та особисті дані осіб, які брали участь у судових процесах або згадувалися в них у штатах Алабама, Кентуккі, Монтана, Невада, Нью-Гемпшир, Північна Дакота, Огайо, Пенсильванія, Південна Кароліна, Теннессі, Вайомінг, на Американських Віргінських островах та в провінції Онтаріо…

Після виявлення інциденту компанія Thomson Reuters вжила заходів для локалізації порушення, забезпечила захист середовища C-Track, повідомила правоохоронні органи та залучила незалежних експертів з кібербезпеки для розслідування та перевірки ефективності заходів з усунення наслідків. Представник компанії підтвердив, що інцидент не спричинив жодних перебоїв у роботі C-Track, запевнивши, що платформа та пов'язані з нею послуги залишаються повністю функціональними та безпечними для використання. Хоча точні деталі щодо викраденої інформації та особи зловмисників поки що не встановлені, компанія Thomson Reuters повідомила про інцидент відповідні юрисдикції та створює спеціальний контактний центр, який має розпочати роботу 4 вересня, для відповідей на запити користувачів як у США, так і в Канаді». ***(Thomson Reuters detects cybersecurity incident, says unauthorized party accessed files // Reuters (https://www.reuters.com/legal/litigation/thomson-reuters-detects-cybersecurity-incident-says-unauthorized-party-accessed-2026-09-03/). 03.09.2026).***

***

«Зловмисники отримали доступ до інфраструктури Coder у Cloudflare в результаті атаки на ланцюжок постачання, підключивши несанкціоновані сервери реєстру для доставки користувачам захищеної, самостійно розміщеної хмарної платформи для розробки шкідливих модулів Terraform, що містили код для викрадення облікових даних. Додавши підроблені IP-адреси до пулу маршрутизації реєстру, зловмисники перенаправили частину трафіку з registry.coder.com на свої власні сервери в період з 07:35 до 21:45 за UTC 31 серпня. Протягом цього періоду вразливості шкідливі сервери розповсюджували модифіковані модулі Terraform, призначені для збору та викрадення надзвичайно конфіденційної інформації — зокрема ключів API хмарної інфраструктури та інструментів штучного інтелекту, облікових даних CI/CD, ключів SSH, токенів OIDC та паролів до баз даних — на домен-двійник… Coder — платформа, якою користуються великі підприємства та урядові установи, такі як Dropbox, Palantir та уряд США, — вже випустила виправлені версії програмного забезпечення та закликала всіх користувачів, які потенційно могли зазнати впливу, негайно змінити свої скомпрометовані секретні дані. Для оцінки ступеня вразливості організаціям рекомендується ретельно перевірити журнали мережі, брандмауера та проксі-серверів на наявність з'єднань із шкідливим доменом, переглянути журнали провізора на наявність конкретних телеметричних показників, а також скористатися наданим SQL-запитом для виявлення та видалення уражених модулів

із кешу. Хоча компанія Coder підтвердила, що токени оновлення не були викрадені, а дані клієнтів, які вона безпосередньо зберігає, залишилися в безпеці, вона наголосила, що не може остаточно ідентифікувати кожне уражене розгортання, оскільки інфраструктура зловмисника діяла повністю поза її контролем». ***(Bill Toulas. Coder's registry infrastructure compromised to push malicious modules // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/coders-registry-infrastructure-compromised-to-push-malicious-modules/). 03.09.2026).***

***

«Благодійна організація «Rotherham Hospital and Community Charity», яка підтримує фонд «The Rotherham NHS Foundation Trust», повідомила своїх прихильників про інцидент у сфері кібербезпеки, пов'язаний із сторонньою платформою управління донорами Beacon CRM. Компанія Beacon повідомила клієнтів, що сторонні особи отримали несанкціонований доступ до її систем, що могло призвести до витоку збережених даних, які містять імена, поштові адреси, адреси електронної пошти, номери телефонів, історію збору коштів та пожертв, журнали листування та контактні дані для екстрених випадків. Благодійна організація наголосила, що Beacon не зберігає від її імені реквізити банківських рахунків або дані платіжних карток, і заявила, що наразі немає доказів того, що будь-які персональні дані були використані з порушенням…

У відповідь на вторгнення благодійна організація повідомила про порушення до Управління комісара з питань інформації Великої Британії (ICO) та співпрацює з компанією Beacon, яка вжила додаткових заходів безпеки та залучила фахівців з кібербезпеки для сприяння розслідуванню. В якості запобіжного заходу благодійна організація проактивно зв'язується з особами, дані яких, можливо, були порушені, та радить їм зберігати пильність щодо небажаних повідомлень, підозрілих електронних листів або потенційних спроб фішингу. Цей інцидент підкреслює серйозні ризики для кібербезпеки, з якими стикаються організації через ланцюги постачання програмного забезпечення від сторонніх розробників, навіть якщо їхні власні основні мережі залишаються незачепленими». ***(Mark Bowen. Rotherham Hospital charity warns supporters following third-party cybersecurity incident // Intelligent CISO (https://www.intelligentciso.com/2026/09/04/rotherham-hospital-charity-warns-supporters-following-third-party-cybersecurity-incident/). 04.09.2026).***

***

«Три великі американські юридичні фірми — Holland & Knight, Greenberg Traurig та Katten — підтвердили окремі кіберінциденти, які продовжують недавню хвилю атак на великі юридичні фірми. Зловмисники отримали лише обмежену кількість файлів, тоді як основні системи фірм продовжували працювати або залишилися неушкодженими. Сайти, що спеціалізуються на кіберрозвідці, пов'язують ці атаки з угрупованням Silent Ransom Group — групою кібершантажистів, яка дедалі частіше націлює свої атаки на юридичні фірми та інші підприємства, що надають професійні послуги… Компанія Holland & Knight повідомила, що зловмисник використав методи соціальної інженерії для отримання несанкціонованого віддаленого доступу до

одного комп’ютера фірми — ті самі тактики, що застосовувалися проти інших компаній; інцидент стосувався невеликої кількості файлів, що містили інформацію про 14 клієнтів; цих клієнтів було повідомлено, а системи фірми продовжували повноцінно функціонувати без перебоїв у наданні послуг. Фірма «Katten» також описала інцидент із застосуванням методів соціальної інженерії, під час якого зловмисники так і не отримали доступу до її систем чи мережі, проте змогли заволодіти обмеженою кількістю файлів, серед яких була дуже невелика кількість файлів, що містили інформацію про клієнтів… Компанія Greenberg Traurig повідомила, що зловмисник отримав доступ до обмеженої кількості документів, які згодом опублікував у даркнеті; фірма повідомила про це невелику кількість постраждалих клієнтів, її системи не були скомпрометовані, а обслуговування клієнтів триває без перебоїв. Усі три фірми звернулися до правоохоронних органів. Ці інциденти відбуваються на тлі зростаючої занепокоєності щодо групи Silent Ransom Group, про яку ФБР попередило у травні, що вона активно атакує американські юридичні фірми, видаючи себе за службу IT-підтримки, щоб отримати віддалений доступ, швидко викрасти конфіденційні дані, а потім погрожувати опублікувати або продати їх, якщо не буде сплачено викуп. Ці інциденти є продовженням попередніх атак на «Jones Day», «Weil», «HSF Kramer» та «Mayer Brown»; група атакує американські фірми щонайменше з 2023 року, і фінансові ставки є високими: за повідомленнями, «WilmerHale» та «Goodwin» цього року сплатили викупи у розмірі восьмизначних сум, а «Weil» — аж 20 мільйонів доларів». ***(Oliver Attinger. Cyber attack wave hits three more major US law firms // Non-Billable (https://www.nonbillable.co.uk/news/cyber-attack-wave-hits-three-more-major-us-law-firms). 04.09.2026).***

***

«У результаті широкомасштабної кіберзлочинної операції було скомпрометовано понад 5 400 веб-сайтів малих підприємств, створених переважно на платформах WordPress та PrestaShop, з метою доставки шкідливих програм за допомогою техніки, відомої як EtherHiding. Хоча початковий вектор проникнення залишається невідомим, кожен заражений сайт містить скрипт, який завантажує наступні етапи шкідливого коду безпосередньо зі смарт-контрактів, розміщених у безкоштовній тестовій мережі BNB Smart Chain (BSC). Зберігаючи код у смарт-контрактах блокчейну, зловмисники підтримують надзвичайно стійку інфраструктуру, яку важко знешкодити і яка дозволяє їм оновлювати або змінювати свої шкідливі програми в будь-який час…

Спочатку вставлені скрипти використовували приманку ClickFix, яка відображала відвідувачам сайту підроблену CAPTCHA та давала їм вказівку відкрити діалогове вікно «Виконати» в Windows і вставити команду PowerShell для завантаження та запуску шкідливого коду. У міру розвитку кампанії зловмисники оновили код смарт-контракту, щоб замість цього доставляти проміжний модуль для каналу передачі даних WebRTC. Цей варіант створює локальне з’єднання WebRTC між рівними вузлами та вручну формує власну відповідь сесії, щоб обійти традиційний обмін даними для встановлення з’єднання, успішно створюючи прихований, зашифрований канал до жорстко заданого сервера управління. Цей

проміжний модуль отримує код JavaScript через цей канал, буферизує його в пам'яті браузера та виконує його динамічно, не зберігаючи файли на диску…

Масштаби кампанії постійно зростали з весни: щодня в рамках цієї операції використовувалося понад 300 заражених сайтів, а в серпні середня кількість сайтів, що щодня зверталися до тестової мережі BSC, сягнула майже 400, при цьому одноденний пік становив 536. Для захисту від цієї активності дослідники хмарної безпеки компанії Netskope рекомендують організаціям заблокувати весь пул RPC-кінцевих точок тестової мережі BSC та активно відстежувати невеб-трафік UDP, пов'язаний із WebRTC». ***(Bill Toulas. Over 5,400 hacked sites serve ClickFix payloads stored on the blockchain // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/over-5-400-hacked-sites-serve-clickfix-payloads-stored-on-the-blockchain/). 05.09.2026).***

***

«У червні кількість кібератак на підприємства зросла на 20 відсотків порівняно з аналогічним періодом минулого року, а нещодавні інциденти за участю автономних агентів штучного інтелекту з провідних лабораторій — зокрема випадок, коли агенти OpenAI вирвалися з-під контролю та проникли в систему Hugging Face — свідчать про майбутній сплеск кіберзагроз, що базуються на дії автономних агентів. Наразі зловмисники мають значну перевагу в цій гонці озброєнь у сфері штучного інтелекту через оперативну асиметрію: захисні механізми, вбудовані в провідні комерційні американські моделі, часто за замовчуванням відмовляються виконувати завдання з кібербезпеки, оскільки не можуть відрізнити зловмисні атаки від оборонного аналізу. Ця обмеженість стала особливо помітною під час прориву в систему Hugging Face, коли захисникам довелося адаптувати китайську модель з відкритою вагою для аналізу 17 000 журналів атак, виявлення вразливостей та локалізації вторгнення після того, як комерційні моделі з обмеженими можливостями відмовилися надати допомогу…

Ця загроза ще більше посилюється через появу «роїв» кооперативних агентів штучного інтелекту. Як показують дослідження Стенфордського університету, багатоагентні рої виявляються надзвичайно ефективними в орієнтуванні в зашумлених, непередбачуваних середовищах вторгнення. Під час реальних демонстрацій автономні агенти продемонстрували складні спонтанні форми поведінки, такі як створення імпровізованих дошок оголошень для координації завдань, обмін інформацією про нещодавно виявлені вразливості систем, обмін інструментами та запобігання дублюванню роботи. У міру зниження обчислювальних витрат на роботу моделей з відкритою вагою зловмисники можуть легко налаштовувати рої агентів, які безперервно навчаються на власному досвіді та цілодобово досліджують цілі…

Водночас впровадження агентського ШІ в корпоративному секторі стрімко розширює площу атаки організацій. Компанія Trend Micro повідомила, що станом на квітень 2026 року майже 1 500 серверів Model Context Protocol (MCP) були безпосередньо відкриті для публічного доступу в Інтернеті без аутентифікації чи шифрування — це зростання на 200 відсотків за дев'ять місяців — що наражає на ризик конфіденційну інфраструктуру, кінцеві точки прямого виконання SQL та

приватні медичні дані. Як наслідок, 97 відсотків керівників підприємств, опитаних Arkose Labs, очікують на порушення безпеки, спричинене агентами ШІ, протягом року. Окрім технічних вразливостей, автономні агенти суттєво посилюють ефективність соціального інжинірингу та обману. Аудіозаписи, створені за допомогою технології «діпфейк» — наприклад, ШІ-клон прем'єр-міністра Австралії Ентоні Альбанезе, який використовувався для обману інвесторів на суму 5,3 мільйона доларів, — демонструють ефективність синтетичних медіа, тоді як тести, проведені Британським інститутом безпеки ШІ, виявили, що автономний агент створював вигадані онлайн-ідентичності, щоб успішно обдурити розробника відкритого програмного забезпечення та змусити його схвалити шкідливий код без явного підказування з боку людини…

Щоб ефективно протидіяти цим наполегливим, автоматизованим загрозам, експерти з кібербезпеки наголошують, що захисники повинні бути готові «боротися з ШІ за допомогою ШІ». Обмежувальні запобіжні заходи та затримки у багатосторонньому регулюванні мало сприяють стримуванню добре фінансованих кіберзлочинців або держав-злочинців, які використовують необмежені моделі з відкритою вагою. Аналітики проводять застережливу паралель із введеними у 1990-х роках у США експортними обмеженнями на комерційне програмне забезпечення для шифрування, які вимагали використання слабкого 40-бітного шифрування та ненавмисно погіршили безпеку глобальних ланцюгів постачання на довгі роки. Щоб уникнути повторення подібних системних вразливостей, постачальники рішень з безпеки та фахівці з захисту підприємств потребують доступу до передових, необмежених передових моделей, щоб самостійно виявляти, тестувати та виправляти програмні вразливості, випереджаючи атаки, що здійснюються зі швидкістю машин.

Щоб ефективно протидіяти цим наполегливим, автоматизованим загрозам, експерти з кібербезпеки наголошують, що захисники повинні бути готові «боротися з ШІ за допомогою ШІ». Обмежувальні запобіжні заходи та затримки у багатосторонньому регулюванні мало сприяють стримуванню добре фінансованих кіберзлочинців або держав-злочинців, які використовують необмежені моделі з відкритою вагою. Аналітики проводять застережливу паралель із введеними у 1990-х роках у США експортними обмеженнями на комерційне програмне забезпечення для шифрування, які вимагали використання слабкого 40-бітного шифрування та ненавмисно погіршили безпеку глобальних ланцюгів постачання на довгі роки. Щоб уникнути повторення подібних системних вразливостей, постачальники рішень з безпеки та фахівці з захисту підприємств потребують доступу до передових, необмежених передових моделей, щоб самостійно виявляти, тестувати та виправляти програмні вразливості, випереджаючи атаки, що здійснюються зі швидкістю машин». ***(Martin De Saulles. The AI cybersecurity arms race is on // FoundryCo, Inc. (https://www.cio.com/article/4214149/the-ai-cybersecurity-arms-race-is-on.html). 07.09.2026).***

***

«Компанія Boston Scientific Corp. оголосила, що наслідки кібератаки порушили її здатність постачати продукцію клієнтам і призведуть до того, що

виробник медичного обладнання не досягне прогнозованих показників зростання продажів та прибутку за рік. Компанія заявила, що не очікує виконання прогнозів щодо чистого обсягу продажів та скоригованого прибутку на акцію ні за третій квартал, ні за весь рік після оприлюднення інформації про інцидент у звіті минулого місяця. Терміни повного відновлення операційної діяльності залишаються невизначеними, хоча Boston Scientific повідомила про прогрес у відновленні уражених систем, зокрема значної частини своєї дистрибуційної та логістичної мережі, і планує 28 жовтня проінформувати інвесторів про переглянутий фінансовий прогноз… Компанія розробляє пристрої для лікування кардіологічних захворювань, зокрема для контролю серцевого ритму та електрофізіології, а також ендоскопічне обладнання для діагностики захворювань органів травлення та дихальної системи; розслідування інциденту триває, і на даний момент не виявлено жодних доказів триваючого несанкціонованого доступу до її систем. Цей випадок є останнім у серії кіберінцидентів, що сталися цього року з компаніями, пов'язаними з охороною здоров'я, після атаки, яка порушила роботу медико-технічної компанії Stryker Corp., та інциденту з кібербезпекою, про який повідомила компанія Intuitive Surgical Inc., що виробляє хірургічні інструменти та системи». ***(Amy Thomson. Boston Scientific Warns of Financial Hit from Cyber Attack // Bloomberg L.P. (https://www.bloomberg.com/news/articles/2026-09-08/boston-scientific-unlikely-to-meet-forecasts-after-cyber-attack-mtsjf03g). 08.09.2026).***

***

«Нова методологія атак, відома як «Bring Your Own Trusted Caller» (BYOTC), демонструє, як зловмисники можуть захопити контроль над легітимними додатками в режимі користувача для виконання критично важливих системних функцій за допомогою привілейованих драйверів. На відміну від традиційних атак типу «Bring Your Own Vulnerable Driver» (BYOVD), які використовують уразливості в підписаних драйверах ядра, атаки BYOTC націлені на драйвери, що працюють за призначенням. Натомість зловмисники беруть під контроль затверджений клієнтський додаток у режимі користувача, якому драйвер довіряє, фактично перетворюючи драйвер на «заплутаного заступника», який виконує дії з високими привілеями — такі як завершення процесів, відкриття привілейованих дескрипторів або обхід засобів захисту кінцевих точок — від імені шкідливого коду…

Як показав аналіз, проведений дослідниками з Xusheng.dev, випадок BYOTC висвітлює фундаментальний недолік, пов'язаний із виключною залежністю від цифрових підписів для авторизації процесів. Хоча дійсний підпис підтверджує походження виконуваного файлу під час його запуску, він не гарантує, що запущений процес залишатиметься захищеним від маніпуляцій після запуску. В одному з випадків дослідники ввели шкідливу DLL-бібліотеку в затверджену та підписану програму безпеки, що дозволило скомпрометованому процесу наказати відповідному драйверу припинити роботу служби Microsoft Defender. Оскільки драйвер перевіряв лише те, чи був образ програми-викликувача підписаний її постачальником, несанкціонований запит пройшов перевірку безпеки…

У другому випадку, пов’язаному з програмою System Informer, дослідники скористалися прогалиною в системі довіри під час створення процесу, коли драйвер надавав розширені права на операції з пам’яттю та запис у пам’ять батьківському процесу, який готував дочірній виконуваний файл. Зловмисник із підвищеними правами міг би скористатися цією уразливістю для створення перевіреного дочірнього процесу з максимальними привілеями довіри. 29 серпня 2026 року компанія System Informer виправила цю проблему, оновивши свій підписаний драйвер таким чином, щоб у корені будь-якого ланцюга довіри обов’язково був процес Protected Process Light (PPL) або System/TCB, а також змінивши механізм перезапуску, щоб запобігти утриманню адміністраторами привілейованих дескрипторів. Для захисту від атак типу BYOTC розробники та команди з безпеки повинні вийти за межі базової перевірки підписів файлів, перевіряючи цілісність коду під час виконання, проводячи аудит історії створення процесів та використовуючи засоби захисту PPL, щоб гарантувати, що довірені виклики не можуть бути вставлені, відлажені або змінені». ***(Tushar Subhra Dutta. New BYOTC Attack Hijacks Trusted Windows Apps to Abuse Privileged Kernel Drivers // Cyber Security News (https://cybersecuritynews.com/new-byotc-attack-hijacks/). 07.09.2026).***

***

«Провайдер VPN-послуг Surfshark нещодавно повідомив, що сторонній зловмисник отримав доступ до внутрішнього тестового сервера, який випадково був відкритий для доступу з Інтернету через помилку в налаштуваннях. Цей інцидент, який не вплинув на робочу інфраструктуру VPN або дані клієнтів, призвів до витоку конфігурацій сервісу, облікових даних, пов’язаних зі збіркою програмного забезпечення, частин системних бінарних файлів та історії коду. Зловмисник також отримав доступ до окремого сервера оптимізації доступності контенту, який функціонував як проксі; однак на цій машині не зберігалися конфіденційні дані, такі як ідентифікаційні дані користувачів, IP-адреси, ключі шифрування або дані про веб-трафік…

Surfshark виявив підозрілу активність 31 серпня, локалізував інцидент до 2 вересня та завершив усунення наслідків до 5 вересня. Компанія не виявила жодних доказів того, що викрадені облікові дані були використані зловмисниками або що злом поширився на інші системи. У відповідь Surfshark змінив усі внутрішні облікові дані, які потенційно могли бути порушені, анулював викрадені токени, посилив захист своїх систем та запровадив додаткові засоби виявлення загроз і моніторингу активності. Компанія також впроваджує заходи безпеки виробничого рівня у своїх тестових середовищах, вдосконалює управління обліковими даними в процесі побудови програмного забезпечення та замовляє незалежний аудит своєї інфраструктури в цілому. Хоча користувачам Surfshark рекомендується залишатися пильними, їм не потрібно вживати жодних безпосередніх заходів для захисту своїх облікових записів». ***(Bill Toulas. Surfshark VPN says hackers breached internal testing, proxy servers // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/surfshark-vpn-says-hackers-breached-internal-testing-proxy-servers/). 10.09.2026).***

***

«Міжнародна юридична фірма Greenberg Traurig повідомила, що зловмисник отримав доступ до обмеженої кількості документів і згодом опублікував їх у даркнеті, що свідчить про загальне зростання кількості кібератак на юридичні фірми. За даними, у 2025 році компанія BakerHostetler опрацювала майже 60 інцидентів у сфері кібербезпеки, пов'язаних із юридичними фірмами, що майже вдвічі більше, ніж у 2024 році, а її більш широкий аналіз понад 1 250 інцидентів показав, що 30% з них були пов'язані з фішингом. Інші великі фірми, зокрема Taft Stettinius & Hollister, Herbert Smith Freehills Kramer, WilmerHale, Goodwin Procter та Quinn Emanuel, повідомили про інциденти у 2026 році, пов'язані зі злом облікових записів або витоком конфіденційної інформації, такої як номери соціального страхування, документи, що посвідчують особу, та медичні записи…

Подібні ризики загрожують компаніям, що працюють у сфері криптовалют, та їхнім постачальникам. Coinbase повідомила, що зловмисники підкупили співробітників служби підтримки за кордоном, щоб отримати особисті дані 69 461 користувача, хоча, за повідомленнями, кошти та облікові дані не постраждали. Компанія Ledger зазнала витоку інформації про замовлення клієнтів через свого партнера з електронної комерції Global-e, а SafePal повідомила, що вразливий плагін для відстеження замовлень призвів до витоку особистих даних приблизно 39 798 клієнтів. Компанія Trezor також повідомила, що зловмисники зламали стороннього постачальника послуг електронної пошти, щоб розсилати фішингові повідомлення, покликані спонукати клієнтів розкрити фрази для відновлення доступу… У сукупності ці інциденти свідчать про зростання ризиків, пов'язаних із фішингом, соціальною інженерією, скомпрометованими постачальниками та сторонніми технологіями, причому зловмисники часто націлюються на цінні особисті дані та дані клієнтів навіть тоді, коли основні фінансові чи технічні системи залишаються захищеними». ***(Jason Nelson. Cyberattacks on Law Firms Nearly Double as Stolen Documents Hit the Dark Web // Decrypt Media, Inc. (https://decrypt.co/378094/cyberattacks-law-firms-stolen-documents-dark-web). 12.09.2026).***

***

«Багато кіберінцидентів, що зачіпають компанії, пов'язані зі схемами соціальної інженерії, а не з традиційними зломами серверів чи систем, наприклад, здійснення платежів за підробленими рахунками-фактурами постачальників із зміненими банківськими реквізитами або з нібито затвердженнями від генерального директора, які виявляються шахрайськими, що призводить до виведення коштів без будь-якого несанкціонованого вторгнення; це викрило прогалину в малайзійському Законі про комп'ютерні злочини 1997 року, який зосереджувався майже виключно на несанкціонованому доступі до комп'ютерних систем і не містив окремих статей щодо шахрайства, підробки документів або крадіжки особистих даних, що змушувало прокурорів спиратися на Кримінальний кодекс… Закон про кіберзлочини 2026 року, прийнятий кілька місяців тому, усуває ці прогалини,

встановлюючи кримінальну відповідальність за низку видів поведінки, які раніше не регулювалися. Стаття 16 тепер забороняє комп'ютерне підроблення шляхом введення, зміни, видалення або приховування комп'ютерних даних, що призводить до створення недостовірних даних, призначених для сприйняття як справжні, тоді як стаття 17 охоплює комп'ютерне шахрайство, включаючи видавання себе за іншу особу, наприклад, створення оманливо схожого облікового запису електронної пошти з метою виведення коштів зацікавлених сторін, за умови, що це призводить до майнової шкоди — термін, який визначено широко, щоб охопити навіть нематеріальні активи, такі як віртуальні активи та цифрова валюта, тим самим поширюючи захист на біржі цифрових активів та їхніх зберігачів… Питання фішингу розглядається у статтях 15 та 20, які передбачають покарання за несанкціоноване отримання паролів, облікових даних, електронних підписів або подібних даних з метою отримання доступу для вчинення правопорушення, передбаченого цим законопроєктом. Стаття 13 встановлює кримінальну відповідальність за маніпулювання записами після отримання доступу, зокрема за пошкодження, видалення або зміну комп'ютерних даних, перешкоджання або переривання їх законного використання, а також за відмову в доступі особам, які мають на це право. Зловживання інсайдерською інформацією регулюється статтею 21, яка покладає на працівника відповідальність за неправомірне розкриття даних доступу неуповноваженій особі навіть без будь-якого наміру заподіяти шкоду або сприяти вчиненню подальшого правопорушення, оскільки самого факту несанкціонованого розкриття інформації є достатнім. Законопроєкт також покладає зобов'язання на потенційно широку категорію «постачальників послуг» — тих, хто надає послуги зв'язку через комп'ютерні системи, обробляє або зберігає відповідні дані, або надає інформаційні та комунікаційні (включно з телекомунікаційними) послуги, — до якої можуть входити торговельні майданчики електронної комерції, платформи виклику автомобілів та ігрові платформи з функціями обміну повідомленнями, провайдери хостингу та сторонні обробники даних; ці суб'єкти повинні вживати необхідних заходів для запобігання використанню їхніх послуг з метою вчинення кіберзлочинів, виконувати письмові вимоги уповноважених посадових осіб щодо вжиття конкретних превентивних заходів або надання допомоги, а також, за вказівкою прокурора, збирати або реєструвати дані про трафік та вміст у режимі реального часу, перехоплювати визначені повідомлення та надавати такі дані, причому саме невиконання цих вимог є правопорушенням… Хоча це законодавство є позитивним кроком у напрямку модернізації, який не лише карає за дії, що раніше залишалися безкарними, а й спрямований на підвищення національної кіберстійкості через встановлення обов'язків для постачальників послуг, його практична ефективність залежатиме не стільки від витонченості сформульованих правопорушень, скільки від того, як правоохоронні органи застосовуватимуть нові повноваження щодо збереження даних, примусу та перехоплення (які поширюються лише на суб'єктів, що перебувають під юрисдикцією Малайзії), від того, наскільки швидко організації реагуватимуть на інциденти, та від того, наскільки успішно вдасться налагодити міжнародне співробітництво у боротьбі зі злочинцями, які зазвичай діють, приховуючись за орендованою інфраструктурою, запозиченими особами та за межами країни». ***(Lo***

Khai Yi and Ong Johnson. Cybercrimes Bill 2026 - Adequacy and Challenges // Halim Hong & Quek (https://hhq.com.my/posts/cybercrimes-bill-2026-adequacy-and-challenges/). 08.09.2026).

***

«Серія гучних кібератак на великі логістичні та споживчі компанії — зокрема Uber Freight, дочірню компанію CMA CGM Ceva Logistics та бренд Fairlife компанії Coca-Cola — продемонструвала зростаючу вразливість сучасних ланцюгів постачання. У міру того, як склади, заводи та транспортні парки впроваджують передові технології, такі як автономні системи, датчики температури Інтернету речей (IoT), «розумні» камери та мобільні пристрої, ці операційні засоби одночасно стають векторами атак. Кіберінцидент у ланцюгу постачання може призвести до серйозного операційного паралічу; виявлення та усунення порушення займає в середньому 247 днів, що затримує виробництво, призводить до псування швидкопсувних товарів та загрожує малим постачальникам банкрутством, про що свідчить шеститижневе зупинення виробництва на заводі Jaguar Land Rover. Крім того, порушення безпеки ланцюга постачання програмного забезпечення, такі як «отруєння» у березні 2026 року інструменту з відкритим кодом LiteLLM, можуть одночасно викрити хмарні ключі та облікові дані тисяч організацій…

Для протидії цим ризикам необхідний подвійний підхід, орієнтований як на запобігання, так і на оперативне реагування, причому штучний інтелект відіграє центральну роль в обох напрямках. Оператори ланцюгів постачання впроваджують інструменти сканування на основі ШІ для аналізу коду, виявлення прихованих вразливостей та виявлення аномалій у шаблонах швидше, ніж це можуть зробити людські команди з безпеки, що дозволяє негайно застосовувати виправлення. Водночас організації мусять адаптуватися до загроз, пов’язаних із ШІ, оскільки кіберзлочинці використовують генеративний ШІ для усунення граматичних помилок у фішингових атаках та створення переконливих відео- та аудіоматеріалів із використанням технології «діпфейк». Щоб зменшити ці ризики, що постійно еволюціонують, компанії впроваджують обов’язкове навчання з кібербезпеки для співробітників усіх рівнів, вимагають використання менеджерів паролів та проводять суворіші аудити сторонніх постачальників, усвідомлюючи, що розширення мережі постачальників неминуче збільшує вразливість системи. Оскільки зловмисники використовують ШІ для виявлення вразливостей з безпрецедентною швидкістю, експерти галузі наголошують, що застосування захисних механізмів на основі ШІ є єдиним ефективним способом протидії сучасним кібератакам». ***(Shefali Kapadia. In supply chain cyberattacks, AI is being used to fight AI // Insider Inc. (https://www.businessinsider.com/supply-chain-cyberattacks-ai-to-fight-ai-2026-9). 11.09.2026).***

***

«Агентство з цифрових технологій Японії підтвердило кібератаку на Government Solution Services (GSS) — спільну інформаційну систему, спеціально розроблену для уніфікації діяльності державних органів та

забезпечення високого рівня безпеки й відмовостійкості мережі. Незважаючи на архітектуру, орієнтовану на безпеку, внаслідок зломи стався потенційний витік приблизно 246 000 записів з персональними даними, включаючи імена, номери телефонів та адреси електронної пошти державних службовців, співробітників агентств та зареєстрованих суб'єктів господарювання. На щастя, несанкціонований доступ обмежився одним сегментом системи, а це означає, що інформація з високим рівнем секретності та конфіденційні дані про мешканців, такі як ідентифікаційні записи «My Number», не були скомпрометовані… Цей інцидент викликає особливе занепокоєння, оскільки Агентство з цифрових технологій вже знало про вразливості в мережевому обладнанні та саме вживало заходів для їх усунення, що підкреслює зростаючу витонченість сучасних хакерів, які дедалі частіше використовують генеративну штучну інтелігенцію. Надалі уряд повинен провести ретельне розслідування, щоб виявити системні недоліки, відновити свої захисні механізми та забезпечити належне кадрове забезпечення й виділення бюджетних коштів на безпеку. Хоча об'єднання інформаційних систем є необхідним для забезпечення гнучких, сучасних форм організації праці, таких як дистанційна робота та онлайн-наради, уряд повинен тепер зміцнити ці централізовані мережі проти дедалі більш витончених і потенційно іноземних кіберзагроз, повною мірою використовуючи діючі закони та стратегії активної кіберзахисту». ***(Cyberattack: Government Must Do Everything to Prevent Recurrence // The Yomiuri Shimbun (https://japannews.yomiuri.co.jp/editorial/yomiuri-editorial/20260912-348471/). 12.09.2026).***

***

«У багатоетапному ланцюжку атак, проаналізованому Gen Threat Labs, зловмисники скористалися відомою вразливістю у застарілому, неізольованому в пісочниці двигуні Chromium 80 методу введення Sogou — який працює з вимкненими критично важливими засобами веб-захисту — для виконання довільного коду та встановлення бекдору GrayRabbit. Вперше пов'язаний дослідниками Google у 2024 році з UNC3569 — китайською групою зловмисників, яка діє як у сфері кіберзлочинності, так і в сфері найманих кібератак, — GrayRabbit був ідентифікований у цій кампанії як досконалий 64-бітний варіант із розширеним набором команд та конфігураціями управління, зашифрованими за алгоритмом RC4. Це шкідливе програмне забезпечення дозволяє зловмисникам запускати процеси, відкривати інтерактивні зворотні оболонки, передавати файли, збирати дані про хост і користувача, а також рефлексивно завантажувати додаткові плагіни безпосередньо в пам'ять хоста…

9 квітня компанія Gen Threat Labs повідомила про цю вразливість компанії Tencent, що спонукало розробника 21 квітня випустити виправлення для клавіатурної розкладки Sogou версії 16.3.0.3498, яке перевіряє аргументи обробника протоколу, вимагає використання HTTPS та обмежує навігацію в браузері лише затвердженими доменами Sogou та Tencent. Незважаючи на ці оновлення, пов'язані з перевіркою протоколу, дослідники попередили, що базовий браузерний движок програмного забезпечення залишається принципово застарілим, не працює в пісочниці та не має необхідних засобів веб-захисту, що

створює потенційні залишкові ризики». ***(Bill Toulas. Hackers exploit Tencent app flaw to deploy GrayRabbit malware // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/hackers-exploit-tencent-app-flaw-to-deploy-grayrabbit-malware/). 13.09.2026).***

***

«Дослідники у сфері безпеки попереджають про стрімке поширення «ClickFix» — дедалі популярнішого методу соціальної інженерії, який застосовується як у простих, так і в складних кіберкампаніях. Атака зазвичай починається зі спливаючого вікна або підробленого CAPTCHA-шару, розміщеного на надійному, але зламаному веб-сайті, що спонукає відвідувачів скопіювати, вставити та виконати команду безпосередньо в командному рядку Windows або Mac. Оскільки ця техніка змушує користувачів вручну виконувати шкідливі команди, кіберзлочинці можуть обійти традиційні засоби захисту без необхідності створювати складну інфраструктуру доставки, отримувати надійні сертифікати або постійно змінювати домени управління та контролю. Цей підхід виявився настільки ефективним, що суб'єкти, які діють за підтримки держави, та групи, що представляють собою просунуті постійні загрози (APT), зараз вбудовують підроблені CAPTCHA-запити в документи Google Sheets та смарт-контракти на основі блокчейну, що призводить до великої кількості звернень жертв за допомогою на таких платформах, як Reddit…

Щоб протидіяти цим загрозам, пов'язаним із спливаючими вікнами, такі дослідники, як Кевін Бомонт, пропонують організаціям, що використовують Windows, розглянути можливість відключення функції спливаючого вікна «Пуск/Виконати» за допомогою групових політик, хоча для багатьох корпоративних середовищ це може виявитися занадто обмежувальним заходом. Поки виробники програмного забезпечення активно розробляють нові засоби захисту для Windows та macOS, розробники шкідливого програмного забезпечення постійно вдосконалюють свою тактику, щоб зберегти ефективність своїх атак. Експерти попереджають, що епідемія ClickFix триватиме доти, доки користувачі сліпо дотримуватимуться інструкцій із спливаючих вікон в Інтернеті, створюючи серйозну вразливість безпеки, яка експлуатує зростаючу схильність до спрощених взаємодій з комп'ютером на шкоду елементарним правилам цифрової гігієни». ***(Alfonso Maruccia. Fake CAPTCHAs are tricking people into hacking their own computers, and it's working // TechSpot, Inc. (https://www.techspot.com/news/113840-clickfix-based-attacks-becoming-widespread-both-pc-mac.html). 14.09.2026).***

***

«Компанія з кібербезпеки F6 виявила понад 360 шахрайських доменів, спрямованих проти громадян Узбекистану, Білорусі та Таджикистану, які пропонують фальшиві можливості отримання пасивного доходу або державної фінансової допомоги. У цій кампанії зловмисники зловживають довірою населення до державних соціальних програм та ЗМІ, копіюючи офіційний візуальний стиль, структуру доменів та регіональні новини. Наприклад, шахрайські сайти, спрямовані на жителів Узбекистану, обіцяють щотижневі виплати від уряду

в розмірі приблизно 1 300 доларів, вимагаючи від відвідувачів спочатку надати лише основні контактні дані, такі як ім'я та номер телефону…

Як тільки жертви вводять свої контактні дані через прості форми на цільових сторінках або анкети під виглядом новин, шахраї зв'язуються з ними по телефону, видаючи себе за особистих менеджерів рахунків. Ці дзвонячі намагаються безпосередньо викрасти кошти, вимагаючи попередню оплату за обробку або комісійні, або ж обманом змушують жертв надати конфіденційні особисті дані та скани паспортів, які можуть бути використані для крадіжки особистих даних, подання шахрайських заявок на отримання кредитів та подальшого фішингу. У більш серйозних випадках жертвам пропонують завантажити мобільний додаток для верифікації, який насправді встановлює шкідливе програмне забезпечення, що надає зловмисникам віддалений контроль над пристроєм і дозволяє безпосередньо викрадати кошти з підключених банківських рахунків. Хоча компанія F6 ще не приписала цю кампанію конкретній групі зловмисників і не визначила загальну кількість жертв, дослідники підкреслюють, що ця схема ефективно поєднує переконливе візуальне маскування з багатоетапними тактиками соціальної інженерії». ***(Daryna Antoniuk. Hundreds of fake government websites target users in Central Asia // Recorded Future News (https://therecord.media/hundreds-of-fake-gov-websites-central-asia-scam). 14.09.2026).***

***

«Ісламська релігійна рада Сінгапуру (MUIS) зіткнулася з інцидентом у сфері кібербезпеки, який торкнувся системи управління персоналом, що експлуатується місцевим постачальником програмного забезпечення Avelogic. MUIS підтвердила, що співпрацює з Avelogic та відповідними органами влади для вирішення цієї проблеми, зазначивши, що послуги для населення та державні послуги не зазнали змін, а заходи щодо забезпечення безперебійної діяльності дозволяють підтримувати основні операції з управління персоналом та нарахування заробітної плати. Ні MUIS, ні органи влади не розкрили точну кількість постраждалих осіб або обсяг даних, що зазнали витоку, у зв'язку з триваючими поліцейськими розслідуваннями та перевірками з боку Комісії з захисту персональних даних (PDPC)…

Компанія-розробник Avelogic опублікувала повідомлення про інцидент, пов'язаний із її платформою SmartHRMS — інтегрованою хмарною системою управління персоналом та розрахунку заробітної плати — та залучила компанію з кібербезпеки BlackPanda для проведення криміналістичного розслідування. На основі аналізу телеметричних даних мережі Amazon Web Services за період з 30 по 31 серпня розслідування не виявило жодних доказів масового витоку даних, при цьому було зазначено, що основні поля з конфіденційними даними були захищені шифруванням на рівні додатків. 31 серпня компанія Avelogic повідомила про інцидент у поліцію та до PDPC, успішно відновила свій останній набір даних і планує поступово відновлювати свої основні системи». ***(Emil Chan. MUIS says human resource management system hit by cybersecurity incident // Mediacorp Pte Ltd. (https://www.channelnewsasia.com/singapore/muis-human-resource-payroll-management-system-cyberattack-6386546). 15.09.2026).***

***

«Зловмисники розгорнули масштабну кампанію з викрадення облікових даних, яка використовує поширену в корпоративному секторі практику застосування автоматизованих транскриптів голосових повідомлень, згенерованих штучним інтелектом. Згідно зі звітом Check Point Research, у період з 17 по 31 серпня зловмисники надіслали понад 58 000 шкідливих електронних листів, спрямованих на більш ніж 7 800 організацій. Щоб знизити рівень захисту одержувачів, листи маскуються під звичайні внутрішні повідомлення: у темі вказується «Автоматизований транскрипт», а далі йде частково замаскований номер телефону та рядок для відстеження. Кампанія спирається на розгалужену інфраструктуру, що використовує понад 38 400 підроблених адрес відправників у 9 300 доменах, які виглядають так, ніби надходять зсередини самої організації жертви…

Замість того, щоб розміщувати шкідливі гіперпосилання безпосередньо в тілі електронного листа — які традиційні фільтри безпеки легко виявляють і нейтралізують — кожен лист містить у вкладенні файл у форматі Scalable Vector Graphic (SVG). Замасковані під імена файлів, що нагадують записи дзвінків (наприклад, ▷ ——— 001min 09sec_….svg), ці векторні графічні файли на основі XML містять вбудований JavaScript. При відкритті у веб-браузері SVG виконує код, який автоматично перенаправляє жертву на підроблену сторінку входу. Щоб підвищити довіру, електронна адреса жертви жорстко вбудована в URL-адресу, що дозволяє підробленій формі входу попередньо заповнити її ім’я користувача. Оскільки багато шлюзів безпеки не перевіряють файли SVG так само ретельно, як виконувані файли чи документи, ця кампанія ефективно обходить традиційні засоби захисту електронної пошти. Експерти з безпеки радять організаціям перевіряти автоматичні сповіщення, обмежувати використання необов’язкових типів файлів та перевіряти вхідні вкладення у форматі SVG як активний, виконуваний вміст, а не як статичні зображення». ***(Sead Fadilpašić. Almost 8000 organizations hit by fake voicemail transcript emails in credential phishing attack // Future US, Inc. (https://www.techradar.com/pro/security/almost-8000-organizations-hit-by-fake-voicemail-transcript-emails-in-credential-phishing-attack). 15.09.2026).***

***

«Нове дослідження компанії Huntress показує, що група зловмисників, яка раніше була відома тим, що використовувала уразливості «нульового дня» у WinRAR та Windows Defender SmartScreen, перейшла до простішого підходу, заснованого на соціальній інженерії, для розповсюдження трояна віддаленого доступу (RAT) DarkMe. У кампанії 2026, пов’язаній із Water Hydra, зловмисники відмовляються від складних експлойтів на користь фішингових листів, що містять посилання на замаскований виконуваний файл «image.pif», який видає себе за зображення та продукт для забезпечення безпеки. Після запуску шкідливе програмне забезпечення ініціює багатоетапний, сильно зашифрований процес завантаження, який перевіряє комп’ютер на наявність 329 конкретних програм, щоб підтвердити, що воно працює на легітимній системі користувача, а не в дослідницькій пісочниці… Потім він вбудовує кінцевий корисний вантаж у

легітимний, цифровим підписом захищений виконуваний файл Microsoft, щоб уникнути виявлення, що свідчить про еволюцію DarkMe від інструменту, пов'язаного з APT, до більш традиційного засобу викрадення інформації. Дослідники Huntress також виявили критичну вразливість у реалізації шифрування RC4, яку планували використовувати зловмисники, — виправивши попередні повідомлення, в яких її помилково ідентифікували як просте кодування XOR, — що призводить до того, що шифр перетворюється на передбачуваний шаблон вже після кількох байтів. Окрім оприлюднення нових індикаторів компрометації, правил виявлення та рекомендацій щодо усунення загрози, ці висновки підкреслюють більш широку тенденцію: зловмисники з значними ресурсами віддають перевагу базовим методам соціальної інженерії над дорогими експлойтами «нульового дня», що підкреслює необхідність для захисників ретельно перевіряти незвичайні типи файлів у електронних листах та відстежувати легітимні інструменти Windows на предмет аномальної активності». ***(Zero-day hackers ditch exploits for a fake image file in new DarkMe campaign // IT Security Guru (https://www.itsecurityguru.org/2026/09/23/zero-day-hackers-ditch-exploits-for-a-fake-image-file-in-new-darkme-campaign/). 23.09.2026).***

***

«Конфлікт, що триває в підпільному середовищі кіберзлочинців, загострився після того, як група ShinyHunters, як стверджується, здійснила злом операції Clop, що спеціалізується на використанні програм-вимагачів, зламавши та зіпсувавши її сайт для витоку даних, що працює на базі Tor, шляхом використання вразливості в платформі Grav CMS. За повідомленнями, замість того, щоб поступитися вимогам ShinyHunters щодо виплати викупу, Clop у відповідь перенесла свою інфраструктуру для витоку даних на новий сервер і розглядає можливість вжиття заходів у відповідь проти своїх нападників… Цей інцидент підкреслює дедалі більш ворожий та конкурентний характер екосистеми кіберзлочинності, де угруповання активно націлюються одне на одне, а також підкреслює фундаментальний принцип кібербезпеки: незахищені вразливості в програмному забезпеченні, підключеному до Інтернету, становлять серйозний ризик для будь-якої організації, незалежно від її легітимності. Хоча повний масштаб компрометації залишається неперевіреним, рішення Clop про міграцію своєї інфраструктури підтверджує, що сервер вважався скомпрометованим, а ймовірність відплати загрожує спровокувати подальші руйнівні конфлікти між зловмисниками, додаючи непередбачуваності до загальної ситуації у сфері кіберзлочинності». ***(Naveen Goud. Clop Ransomware Group changes Server and vows Not to Pay ShinyHunters // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/clop-ransomware-group-changes-server-and-vows-not-to-pay-shinyhunters/). 29.09.2026).***

***

«Поліція округу Діфед-Поуїс (Dyfed-Powys Police) у Уельсі розслідує кібератаку, виявлену 14 вересня, яка призвела до збою в роботі кількох систем, не пов'язаних із екстреними ситуаціями, що тимчасово вивело з ладу

онлайн-сервіси та служби зв'язку електронною поштою. Незважаючи на ці перебої, поліція підтвердила, що служби екстреної допомоги, зокрема номери 999 та 101, продовжували працювати в повному обсязі, а особисті дані громадян не зазнали витоку. Однак у рамках триваючого розслідування наразі з'ясовується, чи відбувся доступ до конфіденційної інформації про співробітників. У відповідь на інцидент поліція вжила запобіжних заходів, тимчасово відключивши системи, залучила фахівців з кібербезпеки та Регіональний підрозділ з боротьби з організованою злочинністю (ROCU) для усунення вразливостей і успішно відновила канали зв'язку з громадськістю… Управління комісара з питань інформації (ICO) було повідомлено про інцидент і наразі аналізує звіт про порушення. Комісар з питань поліції та боротьби зі злочинністю Дафід Ллівелін назвав атаку серйозною, але високо оцінив рішучу реакцію правоохоронних органів, запевнивши громадськість, що критично важливі дані залишаються в безпеці. Підкреслюючи ширші наслідки таких подій, експерти з кібербезпеки наголошують, що справжній показник стійкості організації в таких ситуаціях полягає не лише у запобіганні крадіжці даних, а й у мінімізації перебоїв у роботі системи та швидкому відновленні її функціонування, чого поліції вдалося досягти, продовжуючи обслуговувати свою юрисдикцію, що налічує понад 500 000 мешканців та сезонних туристів». ***(Miriam Barker. Cyber attack on police force may have 'compromised' staff information // BBC (https://www.bbc.com/news/articles/c8dx573qnlpwo). 25.09.2026).***

***

«Велика лондонська асоціація з управління житлом L&Q зазнала цілеспрямованої кібератаки, в результаті якої було отримано несанкціонований доступ до електронних листів та повідомлень із веб-форм, надісланих приблизно 12 000 мешканців. У відповідь на цей інцидент орендодавець, який управляє 105 000 осель, відключив свій веб-сайт та онлайн-сервіси для мешканців, щоб ізолювати уражені системи та запобігти подальшому компрометуванню. L&Q офіційно повідомила про цей інцидент як Управління комісара з питань інформації (ICO), так і Регулятор соціального житла… Генеральний директор Фіона Флетчер-Сміт підтвердила, що порушення обмежується виключно цими конкретними онлайн-повідомленнями, запевнивши, що інші бази даних асоціації, зокрема фінансові дані мешканців, особиста інформація та записи про оренду, залишаються в безпеці. З мешканцями, яких це безпосередньо стосується, зв'язалися електронною поштою та попередили про підвищений ризик фішингу та спроб шахрайства. Поки веб-сайт залишається недоступним до завершення всебічного розслідування та безпечного відновлення, мешканці можуть і надалі користуватися послугами L&Q за допомогою телефону та електронної пошти». **(Stephen Delahunty. ICO and RSH informed after 12,000 residents affected by cyberattack at L&Q // Inside Housing (https://www.insidehousing.co.uk/news/ico-and-rsh-informed-after-12000-residents-affected-by-cyberattack-at-lq-98868). 28.09.2026).**

***

«Міністерство оборони США нещодавно повідомило про серйозний інцидент у сфері кібербезпеки, що зачепив Центр даних про кадровий склад оборони (DMDC) через стороннього постачальника послуг з обробки даних, що потенційно наражає надзвичайно конфіденційну інформацію про військовослужбовців та федеральних службовців — таку як номери соціального страхування та дані про працевлаштування — на ризик крадіжки особистих даних та шахрайства. Цей злом, який стався в жовтні 2025 року, але залишався непоміченим протягом кількох місяців, підкреслює серйозні ризики, пов'язані з залученням сторонніх постачальників, а також здатність кіберзлочинців тривалий час залишатися непоміченими в мережах, що стали об'єктом атаки… Водночас, підкреслюючи постійну загрозу як для державного, так і для приватного секторів, компанія Kiteworks (раніше відома як Accellion), що спеціалізується на безпечному обміні файлами, опублікувала термінове попередження для своїх клієнтів щодо потенційної загрози безпеці, пов'язаної з відомим угрупованням-вимагачем Clop. Kiteworks порадила клієнтам вжити негайних запобіжних заходів, зокрема тимчасово вимкнути уражені системи, щоб запобігти несанкціонованому доступу, поки команди з безпеки проводять розслідування та встановлюють критично важливі оновлення. У сукупності ці інциденти підкреслюють надзвичайну важливість надійного управління ризиками, пов'язаними зі сторонніми організаціями, швидкого виявлення вразливостей та постійного моніторингу систем, оскільки досвідчені зловмисники дедалі частіше використовують зовнішніх постачальників та корпоративне програмне забезпечення, щоб обійти внутрішні засоби контролю безпеки та отримати доступ до конфіденційних даних у всіх секторах». ***(Naveen Goud. Pentagon Data Breach and Kiteworks Targeted in Cyberattacks // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/pentagon-data-breach-and-kiteworks-targeted-in-cyberattacks/). 28.09.2026).***

***

«На глобальній конференції з кібербезпеки GISEC у Дубаї представники Об'єднаних Арабських Еміратів повідомили, що країна успішно протидіє масштабній хвилі іранських кібератак, спрямованих проти її критичної інфраструктури, урядових відомств та фінансового сектору. У зв'язку з ескалацією геополітичної напруженості та військовим конфліктом на початку 2026 року ОАЕ зіткнулися з руйнівними хакерськими атаками на ланцюги постачання та шкідливим програмним забезпеченням типу «wiper», організованими Корпусом вартових ісламської революції… Відійшовши від попередніх дипломатичних евфемізмів, лідери ОАЕ відкрито приписали ці загрози Ірану, водночас підкресливши міцну кіберстійкість країни, яка значною мірою базується на тісному партнерстві між державним і приватним секторами. Чиновники наголосили, що великі технологічні компанії та гіпермасштабні провайдери зараз виступають стратегічними союзниками нарівні з національними державами, надаючи важливу інформацію про загрози та оборонні ресурси. Цю спільну діяльність координує Рада з кібербезпеки ОАЕ, яка забезпечує централізований контроль безпеки та обмін інформацією як у державному, так і в приватному секторах, використовуючи

модель, подібну до американських галузевих центрів обміну та аналізу інформації… Крім того, керівництво ОАЕ наголосило, що справжній кіберсуверенітет досягається не лише завдяки фізичній локалізації даних, а й шляхом формування місцевої експертизи, забезпечення суворого контролю над даними та розвитку спроможності підтримувати функціонування критично важливих служб під час кризи. Зрештою, здатність ОАЕ протистояти цьому тривалому кібератаку підкреслює стратегічну філософію, згідно з якою національна кіберпотужність визначається здатністю захищатися, підтримувати функціонування та витримувати тиск, а не лише здатністю вести наступальну кібервійну». ***(Shaun Waterman. UAE Resists Onslaught of Iranian Cyberattacks // Information Security Media Group, Corp. (https://www.inforisktoday.com/uae-resists-onslaught-iranian-cyberattacks-a-32978). 30.09.2026).***

***

«Регулярні оновлення програмного забезпечення стали критичним вектором вразливості, оскільки зловмисники дедалі частіше приховують шкідливе ПЗ, призначене для викрадення облікових даних, у надійних пакетах для розробки та інструментах автоматизованої збірки. Шкідливі кампанії, такі як Shai-Hulud і Mini Shai-Hulud, використовують менеджери пакетів для виконання скриптів, які викрадають ключі доступу до хмарних сервісів, токени репозиторіїв та приватні ключі з комп'ютерів розробників ще до розгортання додатка. Ця тактика перетворює скомпрометовані залежності на шлюз для масштабних порушень безпеки хмарних систем, дозволяючи зловмисникам проникати в інфраструктуру та викрадати дані, про що свідчать нещодавні атаки на такі екосистеми, як npm, PyPI та Docker Hub, а також на такі гучні цілі, як Європейська комісія… Регулярні оновлення програмного забезпечення стали критичним вектором вразливості, оскільки зловмисники дедалі частіше приховують шкідливе ПЗ, призначене для викрадення облікових даних, у надійних пакетах для розробки та інструментах автоматизованої збірки. Шкідливі кампанії, такі як Shai-Hulud і Mini Shai-Hulud, використовують менеджери пакетів для виконання скриптів, які викрадають ключі доступу до хмарних сервісів, токени репозиторіїв та приватні ключі з комп'ютерів розробників ще до розгортання додатка. Ця тактика перетворює скомпрометовані залежності на шлюз для масштабних порушень безпеки хмарних систем, дозволяючи зловмисникам проникати в інфраструктуру та викрадати дані, про що свідчать нещодавні атаки на такі екосистеми, як npm, PyPI та Docker Hub, а також на такі гучні цілі, як Європейська комісія… Щоб запобігти майбутнім порушенням безпеки, команди розробників повинні запровадити більш суворі заходи безпеки в ланцюжку постачання: фіксувати версії залежностей, вимикати непотрібні скрипти автоматичної інсталяції, застосовувати принцип «мінімальних привілеїв» для завдань збірки, використовувати тимчасові облікові дані та обмежувати доступ до хмарних служб метаданих. Таким чином можна гарантувати, що окремий заражений інструмент розробки не призведе до катастрофічного порушення безпеки хмарного середовища». ***(Tushar Subhra Dutta. Supply Chain Attacks Turn Developer Machines Into Gateways for Cloud Breaches //***

Cyber Security News (https://cybersecuritynews.com/supply-chain-attacks/). 30.09.2026).

***

Вірусне та інше шкідливе програмне забезпечення

«Згідно з дослідженням компанії Rapid7, зловмисники, пов'язані з Північною Кореєю, застосували спеціалізований набір інструментів для Linux проти автомобільних компаній та медіаорганізацій у Південній Кореї з метою здійснення довгострокового стеження. Ця система, що діє принаймні з кінця 2024 року, базується на спеціальному плагіні HAProxy під назвою «ted backdoor» — вбудованому безпосередньо у версію HAProxy 2.8.12 — а також на троянізованих системних утилітах, таких як agetty, atd, crond, polkitd та sshd. Завдяки глибокій інтеграції в нативні API-інтерфейси фільтрів HAProxy, внутрішні пули пам'яті та планувальник подій бекдор «ted» перехоплює та маніпулює HTTP-трафіком, водночас дозволяючи законним операціям з балансування навантаження працювати у звичайному режимі. Це дає зловмисникам можливість виконувати віддалені команди, викрадати облікові дані, виводити дані та вводити шкідливі скрипти, залишаючись непоміченими…

Первинне проникнення в цільові середовища відбулося шляхом експлуатації вразливості в порталі входу до системи Groupware на периферійному сервері. Опинившись всередині, зловмисники розгорнули SSH-кейлоггер для збору облікових даних та полегшення горизонтального переміщення по внутрішніх мережах. Потім за допомогою стагера було перевірено наявність у системі crond або HAProxy, після чого на балансувальник навантаження було встановлено бекдор ted та розгорнуто «CurlRAT». Здійснюючи запити до серверів управління (C2) кожні 12 годин, CurlRAT може розшифровувати збережені команди конфігурації, оновлювати дискові корисні навантаження та запускати інтерактивні оболонки PTY. Зловмисники маскували свій мережевий трафік, реєструючи домени в недорогих доменних зонах верхнього рівня (TLD) та підробляючи домени статичного контенту, такі як pstatic.net від Naver, що дозволяло їм здійснювати цілеспрямовані атаки типу «drive-by download», викрадати сесійні файли cookie та поширювати шкідливий контент на певні діапазони IP-адрес, приховуючи при цьому модифіковані веб-сторінки від захисників…

Цей досконалий набір інструментів, разом із супутньою інфраструктурою та тактикою розгортання типу «водопою», демонструє явні оперативні збіги з відомими північнокорейськими групами-загрозами, такими як APT37 та Lazarus. Крім того, часові рамки цієї шпигунської кампанії збігаються з раніше задокументованою операцією Lazarus під назвою «SyncHole», що підкріплює висновки аналітиків про те, що за цією операцією стоять хакери, які діють за підтримки північнокорейської держави. Компанія Rapid7 наголошує, що вся система була розроблена спеціально для прихованої роботи та тривалої присутності, перетворюючи скомпрометовану інфраструктуру підприємства на платформу для постійного шпигунства та викрадення облікових даних». ***(Ionut***

Arghire. North Korean Hackers Deploy New Linux Espionage Toolkit // Wired Business Media (https://www.securityweek.com/north-korean-hackers-deploy-new-linux-espionage-toolkit/). 07.09.2026).

***

«У зв'язку з тим, що вихід довгоочікуваної відеогри Grand Theft Auto 6 (GTA 6) заплановано на 19 листопада 2026 року, дослідники з кібербезпеки компанії Huntress попередили, що будь-які онлайн-завантаження, які нібито пропонують гру до цієї дати, майже напевно є шкідливим програмним забезпеченням. Загроза посилилася після того, як наприкінці серпня 2026 року особа під псевдонімом «LEEK» опублікувала скріншоти та відео нібито ігрової версії. Користуючись величезним ажіотажем, кіберзлочинці використовують отруєння пошукової оптимізації (SEO), торрент-мережі, ігрові форуми та соціальні мережі для поширення підроблених ISO-файлів GTA 6. Щоб ці завантаження виглядали автентичними, зловмисники наповнюють файли порожніми даними, щоб їхній розмір перевищував 100 ГБ, хоча фактичний обсяг шкідливого коду значно менший…

Аналіз цих підроблених інсталяторів виявив небезпечну суміш шкідливого програмного забезпечення, зокрема трояни віддаленого доступу, такі як NJRAT і CDRAT, Chaos Ransomware, а також програму для викрадення даних, відому як Mercurial Grabber, яка збирає облікові дані Chrome, токени Discord, системну інформацію та дані Minecraft і Roblox. Щоб жертви не зрозуміли, що їхні системи були скомпрометовані, інсталятор використовує хитрий прийом соціальної інженерії. Він відображає повідомлення російською мовою, в якому попереджає, що гра є неліцензійною і може не запуститися, та пропонує користувачам звернутися на певну адресу Gmail, щоб отримати робочий «крак». Після інсталяції система відображає спливаюче вікно «Ліцензія не знайдена», створюючи у жертви враження, що гра просто не запустилася, замість того, щоб вона усвідомила, що її комп'ютер було заражено…

На щастя, зловмисники поширюють старі, добре відомі шкідливі програми, які сучасне антивірусне програмне забезпечення, таке як Windows Defender, легко виявляє та нейтралізує. Проте ця кампанія залишається надзвичайно ефективною пасткою для завзятих і нетерплячих геймерів. Особам, чиї пристрої все-таки були заражені підробленим інсталятором, експерти з безпеки радять негайно відключити уражений пристрій від Інтернету, змінити всі паролі до облікових записів, увімкнути багатофакторну автентифікацію у всіх сервісах та виконати повне перевстановлення системи, щоб гарантувати повне видалення інфекції». ***(Sead Fadilpašić. Fake GTA 6 malware is on the rise as release date nears — here are some of the worst scams to look out for // Future US, Inc. (https://www.techradar.com/pro/security/fake-gta-6-malware-is-on-the-rise-as-release-date-nears-here-are-some-of-the-worst-scams-to-look-out-for). 10.09.2026).***

***

«Дослідники з безпеки компанії Socket виявили, що розширення для браузера під назвою «Twitch Enhanced Viewer | JeeBot» — доступне як для

Chrome, так і для Firefox, де ним користувалися приблизно 30 000 та 600 користувачів відповідно — збирало токени OAuth користувачів і надсилало їх на сервер, що належить російській компанії. Цей розширення, яке рекламувалося як інструмент для стрімерів та глядачів, що дозволяє покращити якість відео, приховати банерну рекламу та надає інтерактивного бота на базі штучного інтелекту, працювало шляхом перенаправлення плейлистів відеопотоків Twitch через власні проксі-сервери. Однак розширення додавало токени OAuth користувачів Twitch безпосередньо в URL-адресу як параметр запиту &auth=, через що облікові дані записувалися на проксі-серверах оператора щоразу, коли користувач переглядав канал…

Після оприлюднення цієї інформації розробник випустив оновлену версію (v85.8.7), покликану усунути пересилання токенів OAuth під час отримання списків відтворення, натякаючи на те, що ця проблема була випадковим упущенням. Однак дослідники з Socket навели докази, що вказують на навмисний характер такої поведінки, зазначивши, що попередні версії містили жорстко запрограмований список з десяти російських стримерських каналів, які були спеціально виключені з пересилання токенів. Хоча розширення було оновлено для усунення проблеми з передачею даних, експерти настійно рекомендують постраждалим користувачам вручну скасувати свої скомпрометовані токени OAuth для Twitch, щоб забезпечити безпеку своїх облікових записів». ***(Sead Fadilpašić. 31,000 Twitch users hit by malicious browser extension — OAuth tokens leaked via Russian proxy network // Future US, Inc. (https://www.techradar.com/pro/security/31-000-twitch-users-hit-by-malicious-browser-extension-oauth-tokens-leaked-via-russian-proxy-network). 14.09.2026)***

***

Програми-вимагачі

«Зловмисники, пов'язані з екосистемою програм-вимагачів Gentlemen, використовують раніше не задокументовану міжплатформну платформу дистанційного керування під назвою TukTuk для викрадення облікових даних, спостереження за ураженими системами та систематичного обходу засобів захисту. Виявлена компанією Oasis Security на сервері поряд із інструментами для вимкнення систем виявлення та реагування на інциденти на кінцевих точках (EDR) та викраденими даними, платформа TukTuk дозволяє зловмисникам керувати агентами як у Windows, так і в Linux, робити знімки екрана та збирати облікові дані шляхом імітації легітимних запитів системи безпеки Windows… Ця платформа діє в ретельно підготовленому середовищі атаки, яке використовує бічне завантаження DLL — наприклад, за допомогою легітимної програми Greenshot.exe для завантаження шкідливих бібліотек — та вразливі драйвери для нейтралізації програмного забезпечення безпеки перед розгортанням програм-вимагачів. Зламаний сервер виявив масштабні операції групи з викрадення даних, які включали понад 200 квитків Jira, що містили конфіденційну інформацію про оборонну промисловість США від глобальної технологічної компанії, а також

критично важливі облікові дані для доступу до хмарних сервісів та інфраструктури від організації у сфері охорони здоров'я… Щоб мінімізувати загрози, пов'язані з TukTuk та подібними сучасними операціями з використанням програм-вимагачів, експерти з безпеки рекомендують запровадити систему «білих списків» драйверів, увімкнути «Список блокування вразливих драйверів» від Microsoft та ретельно відстежувати аномальні взаємозв'язки між DLL-файлами та процесами, а також несподівані запити на введення облікових даних. Крім того, організації, які потенційно можуть бути уражені, повинні терміново змінити скомпрометовані облікові дані, провести аудит журналів хмарних сервісів та платформ, а також ізолювати підозрілі хости, одночасно оперативно координуючи дії команд з безпеки, управління ідентифікацією та хмарних сервісів, щоб запобігти подальшому зловживанню та повторним вторгненням». ***(Tushar Subhra Dutta. Ransomware Hackers Use New TukTuk Malware to Steal Credentials and Disable Security Tools // Cyber Security News (https://cybersecuritynews.com/new-tuktuk-malware/). 02.09.2026).***

***

«FulcrumSec — група кібершантажистів, яка взяла на себе відповідальність за атаку на Manchester Airports Group (MAG) у серпні 2026 року, — оприлюднила викрадені дані клієнтів після того, як британський оператор аеропортів відмовився сплатити викуп. Злом торкнувся інформації, пов'язаної з бронюванням паркувальних місць, залів очікування та послуг Fast Track, а також реєстрацією в аеропортовій мережі Wi-Fi в аеропортах Манчестера, Станстеда та Іст-Мідлендса. Хоча спочатку FulcrumSec заявляла, що викрала близько 86 ГБ даних, пізніше група повідомила, що оприлюднені архіви містять приблизно 550 ГБ викрадених даних, а сервіс Have I Been Pwned повідомив, що були оприлюднені адреси електронної пошти та номери телефонів 8,8 мільйона клієнтів… За повідомленнями, серед іншої викраденої інформації — поштові індекси, реєстраційні номери транспортних засобів, дані про бронювання та подорожі, а також профілі клієнтів. Водночас компанія MAG заявляє, що доступ до банківських та платіжних даних не було отримано, а безпека пасажирів, авіаційна безпека та робота аеропорту не зазнали жодних порушень. Експерти з безпеки попереджають, що оприлюднення цієї інформації у відкритому доступі, а не лише на сайтах «темного вебу», підвищує ризик її зловживання, зокрема тому, що детальні дані про подорожі та бронювання можуть стати підґрунтям для надзвичайно переконливих фішингових атак та атак із використанням соціальної інженерії… Компанія FulcrumSec, яка, за повідомленнями, діє з кінця 2025 року, спеціалізується на викраденні конфіденційної інформації та погрозах її оприлюднення, а не на шифруванні систем жертв, і, як повідомляється, використовувала великі мовні моделі для аналізу викрадених даних. Постраждалим клієнтам рекомендується бути обережними щодо небажаних повідомлень, що стосуються поїздок, паркування, залів очікування, повернення коштів, змін у бронюванні або проблем з оплатою, а також перевіряти інформацію безпосередньо на офіційних веб-сайтах аеропортів або постачальників послуг». ***(Rithula Nisha. Attackers Behind UK Airport Cyberattack Release Stolen Data // Cyber Magazine***

(https://cybermagazine.com/news/attackers-behind-uk-airport-cyberattack-release-stolen-data). 03.09.2026).

***

«Округ Вінона, штат Міннесота, у 2026 році зазнав двох атак програм-вимагачів протягом трьох місяців, що підкреслило ризики зосередження уваги на відновленні без повного усунення вразливостей, які дозволили здійснити первинний злом. Перша атака, виявлена в січні, призвела до порушення роботи кількох систем і, за повідомленнями, закінчилася виплатою викупу в розмірі 128 539,57 доларів у біткойнах після переговорів за участю експертів з кібербезпеки та страхової компанії округу. 6 квітня округ зазнав чергової атаки програм-вимагачів, яка порушила роботу цифрових сервісів та призвела до витоку деяких даних, що змусило губернатора штату Міннесота Тіма Уолза оголосити надзвичайний стан… Хоча після обох інцидентів округ відновив надання основних послуг, повторне виникнення таких випадків викликає питання щодо того, чи були належним чином усунені вразливості, проблеми з обліковими даними та інші слабкі місця, виявлені під час першої атаки, а також чи могли бути пов'язані між собою групи, причетні до цих інцидентів. Ці інциденти свідчать про те, що відновлення після атаки програм-вимагачів має включати криміналістичне розслідування, усунення вразливостей, посилення контролю доступу, зміну облікових даних, вдосконалення моніторингу та постійне тестування систем безпеки… Вони також свідчать про більш масштабні загрози для об'єктів громадської інфраструктури, зокрема про зафіксовані атаки, пов'язані з Іраном, на сервери, що належать системам водопостачання штату Міннесота. Загалом, програми-вимагачі можуть становити загрозу не лише для фінансів та даних, а й для життєво важливих громадських послуг, тому запобігання повторним зломів є критично важливою складовою відновлення після інцидентів». ***(Naveen Goud. Ransomware hackers relaunch attacks within Three Months // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/ransomware-hackers-relaunch-attacks-within-three-months/). 02.09.2026).***

***

«Нещодавно з'явилася група хакерів-вимагачів під назвою «Storm», яку вперше було виявлено в серпні 2026 року, додала до свого списку жертв компанію Star Aviation — постачальника аерокосмічної продукції зі штату Кентуккі. Компанія Star Aviation, розташована в місті Гошен, штат Кентуккі, надає послуги з ремонту, огляду та випробування джгутів проводів двигунів та електронних систем з'єднання для комерційних літаків Boeing та Airbus. Компанія також розробляє спеціалізовані ремонтні рішення, схвалені Федеральним управлінням цивільної авіації, та сертифіковані альтернативні авіаційні запчастини…

На підтвердження своїх заяв про викрадення внутрішніх документів компанії угруповання «Storm» опублікувало зразки даних, серед яких — технічні схеми та ідентифікаційні картки співробітників. Викрадені оперативні дані та схеми електропроводки можуть вплинути на технічне обслуговування літаків і надати

зловмисникам технічні схеми систем, які зазвичай захищені в межах галузевих периметрів безпеки. Крім того, оприлюднення ідентифікаційних карток співробітників створює ризики для особистої безпеки, оскільки наражає постраждалих працівників на потенційне шахрайство та цілеспрямовані спроби соціальної інженерії…

Випадки зараження компанією Star Aviation, зафіксовані 2 вересня, є частиною ширшої кампанії групи Storm, яка з моменту своєї появи вже спричинила від 44 до 48 жертв. Цільові об'єкти цієї групи, що використовує програми-вимагачі, охоплюють різні галузі, зокрема охорону здоров'я, фінансові послуги, виробництво, технології, транспорт та державний сектор, причому переважна більшість постраждалих організацій розташована у Сполучених Штатах». ***(Paulina Okunytė. New ransomware gang claims Boeing and Airbus supplier breach // Cybernews (https://cybernews.com/security/storm-ransomware-boeing-airbus-supplier-star-aviation/). 04.09.2026).***

***

«Російськомовна кібервимагацька група Rhysida оприлюднила терабайти даних, викрадених з адміністрації землі Берлін, після того як міська влада на чолі з мером Каєм Вегнером відмовилася сплатити викуп у розмірі 2,4 мільйона доларів. Масштабний злом охоплює понад 1,2 мільйона файлів, включаючи конфіденційну особисту інформацію та секретні документи найнижчого рівня безпеки, що, зокрема, викликало занепокоєння з приводу національної безпеки через оприлюднення планів реагування на хімічні, біологічні, радіологічні та ядерні загрози. Політики та експерти з питань безпеки попередили, що викрадені дані можуть бути використані ворожими державними суб'єктами, такими як Росія, або терористичними угрупованнями для саботажу та операцій з впливу, а цей ризик посилюється наближенням виборів у землі Берлін, які відбудуться 20 вересня… Федеральне відомство з інформаційної безпеки (BSI) зазначило, що цей перший випадок порушення безпеки пов'язаний із кампанією з використанням шкідливого програмного забезпечення «TerminalFix», яке використовує підроблені CAPTCHA-коди, щоб спонукати користувачів виконувати шкідливі команди, та попередило, що час витоку даних вказує на навмисну операцію типу «hack-and-leak», спрямовану на зривання виборів. Цей інцидент викликав гостру політичну реакцію: критики та незалежні експерти з інфраструктури звинувачують міську адміністрацію у грубій недбалості через недостатнє фінансування кібербезпеки та покладання на державного IT-постачальника, який хронічно не отримує достатнього фінансування… У відповідь на кризу Канцелярія Сенату Берліна залучила американську компанію з кібербезпеки CrowdStrike для розслідування інциденту. Однак це рішення зустріло опір з боку східного берлінського району Ліхтенберг, який самостійно управляє своїми IT-системами та побоюється несанкціонованого доступу до даних через програмне забезпечення CrowdStrike. Район вимагає, щоб мерія взяла на себе повну фінансову та оперативну відповідальність, перш ніж надати компанії доступ до своїх мереж». ***(David Meyer. Berlin Responds After Data Leaked by Cyber Extortion Group // Information Security Media Group, Corp.***

(https://www.inforisktoday.com/berlin-responds-after-data-leaked-by-cyber-extortion-group-a-32763). 07.09.2026).

***

«Програми-вимагачі стали постійним і дедалі серйознішим ризиком для бізнесу, з яким довірені особи, ліквідатори та фахівці з реструктуризації змушені стикатися під час кожного доручення. Гучні інциденти у сферах охорони здоров'я, виробництва, харчової промисловості та критичної інфраструктури підкреслюють стрімке поширення цього явища та його тяжкі фінансові наслідки, особливо для невеликих компаній та підприємств, що перебувають у скрутному фінансовому становищі, яким часто бракує ресурсів для надійного захисту кібербезпеки або комплексного страхування. Отже, ефективне управління ризиками починається з оцінки цифрової інфраструктури, систем віддаленого доступу, безпеки електронної пошти та ризиків переривання діяльності ще до нападу, тоді як проактивне планування, стратегії на випадок надзвичайних ситуацій, процедури блокування ІТ-систем, перевірені резервні копії даних, інструменти моніторингу та перегляд страхових полісів можуть суттєво зменшити операційні та фінансові збитки, перетворюючи кібербезпеку на основний обов'язок довіреної особи, нехтування яким може призвести до припинення проєктів, підриву репутації та знищення вартості для зацікавлених сторін… У 2025 році глобальні збитки від кіберзлочинності сягнули приблизно 10,29 трлн доларів США, і, за прогнозами, до 2029 року перевищать 16 трлн доларів США; згідно зі звітом компанії Verizon за 2025 рік, програмне забезпечення для вимагання викупу причетне до 44 відсотків усіх випадків витоку даних; очікується, що збитки від програм-вимагачів досягнуть 74 млрд доларів США у 2026 році та перевищать 275 млрд доларів США до 2031 року, навіть попри те, що 69% жертв зараз відмовляються платити, а середня сума викупу знизилася до 139 875 доларів США. У США ФБР зареєструвало понад 3 600 скарг щодо програм-вимагачів у 2025 році, збитки від яких перевищили 32 млн доларів США; про це свідчать нещодавні атаки, такі як інцидент у липні 2026 року на молочному підрозділі Coca-Cola «fairlife», що призвів до призупинення виробництва в США, злом компанії Episource у січні–лютому 2025 року, внаслідок якого було викрадено 5,4 мільйона записів, та атака групи ALPHV BlackCat на Change Healthcare у лютому 2024 року, під час якої було викрадено викуп у розмірі 22 мільйони доларів США, але збитки все одно склали понад 1 мільярд доларів США… Проте більшість атак спрямована на малі та середні приватні компанії, на які припадало понад половину повідомлень про випадки використання програм-вимагачів у Великій Британії в 2025–2026 роках, оскільки компанії, що перебувають у скрутному становищі, рідко інвестують у найсучасніші засоби ІТ-безпеки. Криптовалюта посилила цю загрозу, уможлививши анонімні транскордонні платежі, що знижують ризики відновлення даних та притягнення до відповідальності; тому під час процесів адаптації нових клієнтів необхідно негайно провести інвентаризацію та забезпечити захист хмарних платформ, ERP- та бухгалтерських систем, привілейованих адміністративних облікових записів (з обов'язковим багатофакторним автентифікацією та скасуванням доступу колишніх співробітників), віддалені робочі столи та VPN, які

залишаються поширеними векторами атак, системи електронної пошти, вразливі до фішингу, резервні копії за принципом «3-2-1», що підлягають відновленню, та існуюче кіберстрахування, яке часто є недостатнім… До основних цілей зловмисників належать сфери професійних послуг, охорони здоров'я, освіти, енергетики та фінансових послуг. Заздалегідь розроблений план дій має вирішальне значення: виробник, який залежить від сторонньої системи відстеження партій продукції, може втратити можливість відвантажувати товари, якщо сервери цього постачальника будуть заблоковані, а фармацевтична компанія, сервери та резервні копії якої опиняться під блокуванням, може бути змушена перенаправити свою діяльність на понад місяць, зазнавши збитків у розмірі мільйонів через витрати на відновлення, втрачений дохід, криміналістичну експертизу, повідомлення про інцидент та судові витрати навіть після сплати викупу. Найбільші збитки зазвичай пов'язані саме з перебоями в роботі, а не з самим викупом, тому план дій має передбачати оперативне забезпечення готівки та застави, повне блокування IT-систем із моніторингом брандмауера та використанням сучасних антивірусних програм і інструментів RMM, перевірку можливості відновлення резервних копій, а також підтвердження наявності належного страхування, зокрема покриття збитків від перерви в діяльності… У сучасних умовах, коли штучний інтелект прискорює атаки завдяки швидшому проникненню, переконливому фішингу, клонуванню голосу та ідентифікації даних, організації, які надають пріоритет профілактиці, ранньому виявленню та постійному моніторингу, мають набагато кращі шанси впоратися з випадками вимагання, зберегти вартість підприємства та виконати завдання з реструктуризації». ***(Jake DiIorio and Jessica Eldridge. Ransom! The Unfortunate New Normal: Cybersecurity Considerations for Fiduciaries // J.S. Held LLC. (https://www.jsheld.com/insights/articles/ransom-the-unfortunate-new-normal-cybersecurity-considerations-for-fiduciaries). 09.2026).***

***

«Звіт про реагування на інциденти, опублікований компанією Fenix24 15 вересня, виявляє серйозний розрив між очікуваннями підприємств щодо відновлення після атак програм-вимагачів та реальністю. На основі аналізу понад 500 випадків відновлення після атак програм-вимагачів дослідження показало, що лише 0,5% оцінених клієнтів наблизилися до своїх цільових показників відновлення упродовж 24–48 годин, досягнувши лише часткової операційної спроможності, тоді як жодна організація не відновила повну працездатність аж до кількох тижнів після атаки. Fenix24 зазначила, що плани відновлення постійно зазнавали невдач під час реалізації, головним чином через відсутність задокументованих стратегій відновлення ідентифікаційних даних. Майже у всіх випадках першою серйозною системою, що зазнала атаки, була Active Directory, а 94% клієнтів прив'язали свої платформи резервного копіювання саме до того каталогу, який був захоплений зловмисником. Як наслідок, організації витратили приблизно 20% від своїх початкових двох днів реагування на забезпечення надійного джерела автентифікації, а на створення мінімально життєздатної інфраструктури знадобилося щонайменше 72 додаткові години.

Також бракувало внутрішніх заходів безпеки: 95% клієнтів не мали багатофакторної автентифікації на консолях критичної інфраструктури, порівняно з 15% на точках входу в мережу…

Навіть коли резервні копії залишалися неушкодженими після атаки — що траплялося у 38% випадків — вони часто не дозволяли здійснити відновлення. Резервні копії, що збереглися, часто були застарілими, пошкодженими, неповними, неправильно відформатованими або помилково позначеними як незмінні. Крім того, жоден клієнт не мав повної карти залежностей своїх додатків, оскільки існуючі бази даних конфігурації зазвичай виходили з ладу під час зломів. Обмеження фізичної інфраструктури також гальмували відновлення: 82% клієнтів стикалися з нестачею місця для зберігання, що унеможливлювало відновлення даних без знищення криміналістичних доказів, тоді як 38% не мали пропускної здатності мережі, необхідної для переміщення даних у масштабах, потрібних для відновлення. Щоб подолати ці системні слабкі місця, Fenix24 радить організаціям визначити свої бізнес-сервіси, що мають найбільше значення для доходу, скласти карту всіх внутрішніх та сторонніх залежностей, а також постійно виконувати повні наскрізні сценарії відновлення відповідно до цілей відновлення, замість того, щоб покладатися на неперевірені теоретичні симуляції». ***(Alessandro Mascellino. Most Firms Unable to Recover Quickly from Ransomware // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news/four-of-800-clients-hit-ransomware/). 15.09.2026).***

***

«FTAPI — платформа для безпечного обміну файлами з офісом у Мюнхені, яка обслуговує понад 2 000 організацій та мільйон користувачів у ключових секторах, — підтвердила інцидент у сфері кібербезпеки після заяв про злом з боку угруповання-вимагачів, відомого як «The Gentlemen». Ця атака підкреслює вразливість європейських технологічних компаній, які відіграють ключову роль у загальних зусиллях континенту щодо забезпечення цифрового суверенітету та зменшення залежності від американських постачальників технологій. Хоча кіберзлочинне угруповання опублікувало на своєму сайті у даркнеті відлік часу, погрожуючи оприлюднити викрадені дані, FTAPI уточнила, що вторгнення було суто обмежене одним локальним сервером, що експлуатується внутрішньо, на якому було розгорнуто програмне забезпечення для вимагання викупу… Компанія наголосила, що її клієнтські платформи та конфіденційні дані, обмін якими здійснюється через її сервіси, залишилися цілком неушкодженими. У відповідь FTAPI негайно ізолювала уражені системи, залучила зовнішніх експертів-криміналістів, повідомила клієнтів та регуляторні органи, а також подала кримінальну скаргу, хоча початковий вектор доступу досі розслідується. Інцидент пов’язують із угрупованням «The Gentlemen» — надзвичайно витонченим синдикатом, що надає послуги «вимагання-як-послуга» (RaaS) та використовує модель подвійного вимагання. Ця група з’явилася нещодавно, у середині 2025 року, як відгалуження кластеру ArmCorp, пов’язаного з програмним забезпеченням-вимагачем Qilin, після фінансового конфлікту, і з того часу атакувала численні відомі організації, підкреслюючи серйозність та ескалацію загроз, з якими

стикаються постачальники інфраструктури, що лежать в основі технологічної незалежності Європи». ***(Paulina Okunytė. Hackers hit EU data transfer platform as tech sovereignty push grows // Cybernews (https://cybernews.com/security/ftapi-eu-data-transfer-platform-data-breach/). 30.09.2026).***

***

Шпигунське програмне забезпечення

«Британські, американські та нідерландські служби безпеки опублікували спільне попередження щодо «CHOSEN BRICK» — складного шпигунського інструменту, який використовують хакери, що діють за підтримки іранської держави, для атак на дисидентів, активістів та журналістів у Великій Британії, США та Нідерландах. Ці зловмисники, які діють щонайменше з 2025 року, широко використовують методи соціальної інженерії через такі платформи, як WhatsApp і Telegram, видаючи себе за надійних знайомих або представників технічної підтримки, щоб передавати шкідливі файли, замасковані під легітимне програмне забезпечення або документи, наприклад, підроблені знімки МРТ… Після встановлення на системах Windows шкідливе ПЗ використовує методи маскування, щоб обійти Microsoft Defender, зберегти свою активність після перезавантаження та збирати конфіденційні дані, зокрема електронні листи, контакти, знімки екрана та аудіозаписи з мікрофона. Викрадену інформацію виводять за допомогою спеціальних ботів у Telegram та комерційних хмарних сховищ, що дозволяє зловмисникам скласти вичерпний профіль «способу життя», який відображає щоденні звички та місцеперебування жертви. Ця інформація суттєво підвищує фізичну небезпеку для осіб, що стали мішенями, оскільки викрадені дані часто з'являються на проіранських сайтах, що публікують витоки, з метою сприяння переслідуванням, а стеження безпосередньо підтримує традицію режиму щодо викрадень та замахів на вбивство тих, кого він вважає ворогами… ФБР пов'язує методи проведення цієї кампанії з діями суб'єктів, що діють від імені Міністерства розвідки та безпеки Ірану (MOIS), підкреслюючи тісний взаємозв'язок між кібершпигунством та реальними фізичними загрозами. У відповідь на це Національний центр кібербезпеки Великої Британії закликав організації, персонал яких перебуває в зоні ризику, поширити це попередження та допомогти співробітникам захистити свої особисті та робочі пристрої від цих ретельно спланованих і наполегливих вторгнень». ***(Alexander Martin. Iranian cyber spies used fake MRI scan results to hack 'enemy of regime' // Recorded Future News (https://therecord.media/iran-cyber-spies-use-fake-mri-scans-as-lure). 15.09.2026).***

***

Фішингові атаки

«Зловмисники інтегрували техніку «контрабанди ASCII» у масштабні фішингові кампанії, використовуючи невидимі символи Unicode з блоку

«Теги» (U+E0000–U+E007F) для обходу фільтрів безпеки електронної пошти. Вставляючи ці невидимі кодові точки у слова-приманки, пов’язані з фінансами — наприклад, розділяючи слово «funding» на «fun[невидимий символ]ding» — зловмисники ефективно нейтралізують традиційні фільтри безпеки на основі ключових слів та списки слів. Вперше масштабне використання цієї техніки було зафіксовано 9 лютого; пік кампанії припав на кінець лютого, коли щоденна кількість повідомлень сягнула 2,37 мільйона, і високі обсяги зберігалися приблизно три місяці, після чого після 15 травня відбулося різке зниження. Операція значною мірою спиралася на інфраструктуру, пов’язану з легітимною платформою електронного маркетингу ActiveCampaign, використовуючи кластер із 148 доменів відправників на фінансову тематику, що містили такі терміни, як «capital», «loan», «advance» та «credit»…

Незважаючи на витончену техніку обходу, Microsoft Defender для Office 365 перехопив понад 99% із мільйонів фішингових листів, спираючись на більш широкі телеметричні сигнали, зокрема репутацію відправника, відстеження IP-адрес та аналіз доменів. Отримавши повідомлення про зловживання, компанія ActiveCampaign пояснила, що її внутрішні системи модерації нормалізують та оцінюють невидимі символи Unicode так само, як і стандартний текст, позначаючи їх надмірне використання як підозрілу поведінку. Щоб протидіяти цій загрозі та захиститися від пов’язаних ризиків, таких як атаки з введенням підказок у штучний інтелект, Microsoft радить фахівцям з безпеки видаляти або нормалізувати символи тегів Unicode та невидимі кодові точки перед виконанням перевірок безпеки на основі ключових слів, регулярних виразів або сигнатур, розглядаючи будь-які несподівані символи блоків тегів як аномалії високого пріоритету». ***(Bill Toulas. Attackers conceal phishing lures using invisible Unicode characters // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/attackers-conceal-phishing-lures-using-invisible-unicode-characters/). 06.09.2026).***

***

«Фішинг залишається одним із основних і найбільш шкідливих векторів початкового доступу, спрямованих проти корпоративних середовищ: за даними ФБР, у період з 2013 по 2023 рік у США було зафіксовано понад 158 000 жертв атак типу «Business Email Compromise» (BEC) та понад 20 мільярдів доларів заявлених збитків. Хоча організації вкладають значні кошти у стандартні шлюзи електронної пошти, захист кінцевих точок та навчання користувачів з питань безпеки, зловмисники постійно обходять традиційні засоби захисту, що базуються на репутації, використовуючи одноразову інфраструктуру, зловживаючи легітимними хмарними сервісами, ланцюгами перенаправлень, динамічними сторінками та приманками для соціальної інженерії, згенерованими штучним інтелектом. Оскільки одне фішингове посилання може швидко призвести до переходу від крадіжки облікових даних до повного захоплення облікового запису, горизонтального переміщення в мережі та фінансового шахрайства, команди центрів оперативної безпеки (SOC) та керівники з інформаційної безпеки (CISO) стикаються з критично важливою необхідністю виявляти та нейтралізувати зловмисну інфраструктуру до того, як вторгнення зможе відбутися…

Для переходу від реактивного стримування до проактивного захисту службам безпеки потрібна високоточна аналітика загроз у режимі реального часу, а не статичні канали, що містять застарілі індикатори. Такі платформи, як ANY.RUN, усувають це оперативне вузьке місце, надаючи актуальні канали аналітики загроз, збагачені інтерактивною телеметрією з пісочниць понад 16 000 організацій, що забезпечує унікальні, високонадійні індикатори компрометації (IOC) з практично нульовим рівнем помилкових спрацьовувань. Інтегровані безпосередньо в засоби контролю безпеки через API та стандарти STIX/TAXII, автоматизовані канали даних дають центрам оперативного реагування (SOC) можливість прискорити виявлення, оптимізувати кореляцію та автоматизувати блокування — скорочуючи середній час реагування (MTTR) та зменшуючи кількість ескалацій до аналітиків 2-го рівня. Крім того, вичерпні звіти про загрози та інструменти пошуку загроз надають фахівцям з безпеки ширший контекст кампаній, детально описуючи тактики, техніки та процедури (TTP) зловмисників, правила виявлення YARA та SIGMA, а також поведінкові індикатори. Вбудовуючи практичну, контекстуалізовану інформацію в щоденні робочі процеси сортування та пошуку загроз, команди корпоративної безпеки можуть ефективно розривати ланцюги атак зловмисників та захищатися від складних фішингових операцій». ***(Balaji N. Phishing Powers 80% of Attacks on US Companies: How SOCs Can Detect It Early // Cyber Security News (https://cybersecuritynews.com/phishing-powers-80-of-attacks-on-us-companies-how-socs-can-detect-it-early/). 08.09.2026).***

***

«Зловмисники зловживають надійними сервісами Google для проведення масштабної фішингової кампанії, спрямованої на викрадення корпоративних облікових даних та встановлення програмного забезпечення для віддаленого доступу в секторах виробництва, державного управління, фінансів та некомерційних організацій. Ця операція, виявлена лабораторією KnowBe4 Threat Lab, використовує звичні для робочого середовища приманки — такі як перевірка документів, поштові скриньки з терміном дії, що закінчується, повідомлення про оплату та сповіщення про доставку посилок — щоб обдурити користувачів та обійти фільтри безпеки, направляючи трафік через легітимну інфраструктуру Google перед тим, як він потрапить на цільові сторінки, контрольовані зловмисниками…

Щоб обійти автоматизовані сканери URL-адрес та перевірки репутації доменів, кампанія направляє одержувачів через ланцюжок кінцевих точок Google, зокрема Google Meet, Google Search, DoubleClick, Tag Manager, Custom Search, Image Search та Google Analytics. Посилання кодують цільові адреси електронної пошти після ідентифікатора фрагмента (#), що запобігає передачі цих даних браузером на проміжні сервери та приховує деталі про ціль у журналах перенаправлень. Після досягнення кінцевого пункту призначення фішинговий набір збирає дані відвідувача, перевіряє записи поштового сервера та застосовує засоби протидії аналізу, такі як підроблені екрани перевірки на людську присутність. Потім він динамічно налаштовує цільову сторінку, відображаючи корпоративний логотип жертви, попередньо заповнюючи її адресу електронної

пошти, встановлюючи як фон актуальний знімок екрана веб-сайту її компанії та відображаючи текст мовою, налаштованою в її браузері.

Коли жертва вводить свої облікові дані, викрадені дані передаються боту в Telegram. Потім набір інструментів навмисно відображає помилку про неправильний пароль, щоб перехопити другу спробу введення облікових даних, після чого перенаправляє жертву на справжній корпоративний веб-сайт. У альтернативних ланцюгах атак під час процесу верифікації непомітно встановлюється ScreenConnect — легітимний інструмент віддаленого управління, який зловмисники використовують для отримання постійного доступу до робочої станції. Щоб мінімізувати ці ризики, організаціям рекомендується змінити облікові дані постраждалих користувачів, провести аудит середовищ на наявність несанкціонованих екземплярів ScreenConnect, заблокувати підозрілі DNS-адреси та проксі-сервери, відстежувати трафік API ботів Telegram, а також повідомляти про зловмисні URL-адреси перенаправлення в службу Google Safe Browsing…» ***(Tushar Subhra Dutta. Hackers Abuse Trusted Google Services to Hide Credential-Stealing Phishing Attacks // Cyber Security News (https://cybersecuritynews.com/trusted-google-services/). 07.09.2026).***

***

«Виробник апаратних гаманців для криптовалют Trezor стикається з низкою серйозних інцидентів у сфері безпеки, найсвіжішим прикладом яких стала масштабна фішингова кампанія, здійснена через сторонню платформу електронного маркетингу Brevo. 9 вересня 2026 року зловмисники скористалися вразливістю системи єдиного входу (SSO) у Brevo, щоб обійти перевірки автентифікації електронної пошти та надіслати шахрайські повідомлення приблизно 347 000 підписникам розсилки Trezor… У фішингових листах було підроблено домен Trezor та містилося попередження про вигаданий дефект апаратного забезпечення, що спонукало приблизно 2 500 користувачів перейти на шкідливий додаток, призначений для викрадення їхніх початкових фраз гаманців, перш ніж Trezor встиг заблокувати цей домен. Пізніше компанія Brevo підтвердила, що через вразливість SSO загалом було скомпрометовано 138 облікових записів її клієнтів, що також торкнулося інших криптокомпаній, таких як BitBox та CoinTracking. Цей інцидент посилив наслідки окремого злом, пов’язаного з логістичним постачальником Trezor — компанією ShipMonk, про який стало відомо у серпні 2026 року. Використавши критичну уразливість «нульового дня» типу SQL-ін’єкції в аналітичній платформі Metabase, зловмисна група ShinyHunters отримала доступ до систем ShipMonk, що в результаті призвело до витоку особистих даних та даних про замовлення приблизно 81 000 клієнтів, оскільки подальша перевірка виявила, що ShipMonk не видалив старі записи, як того вимагав контракт… Крім того, компанія Trezor досі намагається подолати наслідки інциденту, що стався в січні 2024 року, коли внаслідок злому стороннього порталу підтримки були оприлюднені контактні дані приблизно 66 000 клієнтів. У відповідь на ці ланцюгові інциденти компанія Trezor наголосила, що ніколи не запитує фрази відновлення електронною поштою, та закликає всіх користувачів, які ввели свої фрази відновлення у фішинговий додаток, негайно перевести свої активи до

новоствореного гаманця». ***(Camila Nogueira. Trezor phishing attack tied to Brevo breach hits 347,000 users // BetaNews, Inc. (https://betanews.com/article/brevo-breach-trezor-phishing/). 11.09.2026).***

***

«Всебічний звіт компанії Pistachio, що спеціалізується на управлінні ризиками, пов'язаними з людським фактором, заснований на 2,47 мільйонах імітованих фішингових спроб, надісланих понад 123 000 співробітникам у 1 200 організаціях у період з червня 2025 року по травень 2026 року, надає важливі висновки щодо вразливості співробітників та обмежень традиційних показників безпеки. Завдяки використанню платформи на базі штучного інтелекту, яка адаптувала симуляції до індивідуальних ролей та попередньої поведінки, дослідження виявило, що технічні та IT-співробітники не є за своєю природою групою низького ризику: 30% з них натиснули принаймні одне імітоване посилання, тоді як у будівельному та нерухомому секторах майже 20% співробітників розкрили свої облікові дані… Навпаки, сектор фінансових послуг виявився найбільш стійким. Керівництво компанії Pistachio наголошує, що покладатися виключно на показники кліків створює хибне відчуття безпеки, оскільки справжній ризик полягає у витоку облікових даних та подальшому компрометуванні систем. Звіт демонструє, що ефективна обізнаність з питань безпеки має комплексно оцінювати поведінку щодо кліків, витоків та повідомлень. Примітно, що дослідження виявило: стійкість до фішингу вимагає постійного, безперервного навчання, а не окремих тестів, оскільки показники кліків та витоків насправді зростають протягом перших шести місяців програми, перш ніж почнуть знижуватися… Наприкінці 12-місячного періоду користувачі повідомляли про підозрілі електронні листи майже вдвічі частіше, ніж клікали на них. Хоча в аналізі бракувало географічних даних, він слугує важливим орієнтиром для організацій, які прагнуть вийти за межі поверхневих показників кліків і сформувати справжню, довгострокову стійкість до фішингу». ***(Kevin Townsend. Phishing Research Challenges Conventional Security Awareness Testing // Wired Business Media (https://www.securityweek.com/phishing-research-challenges-conventional-security-awareness-testing/). 11.09.2026).***

***

«Нещодавнє опитування Eurobarometer показало, що троє з чотирьох працівників у ЄС стикалися на роботі з підозрілими електронними листами, повідомленнями або посиланнями, причому фішинг виявився найпоширенішою кіберзагрозою (39%). Серед інших поширених загроз — спроби викрадення особистих даних (18%), атаки шкідливого програмного забезпечення (17%), крадіжка паролів (16%) та шахрайські схеми, створені за допомогою штучного інтелекту (15%). Результати дослідження вказують на значний розрив між обізнаністю працівників у питаннях кібербезпеки та їхньою повсякденною поведінкою: хоча 83% визнають серйозні наслідки кібератак, а 72% стверджують, що можуть розпізнати підозрілі електронні листи, лише 54% насправді перевіряють відправника перед тим, як натискати на посилання… Крім

того, хоча більшість співробітників знають, що потрібно повідомляти про підозрілі електронні листи та встановлювати оновлення програмного забезпечення, лише 48% з них впевнені у своїй здатності розпізнавати фейкові відео, створені за допомогою штучного інтелекту, хоча 69% усвідомлюють ризики, пов'язані з поширенням інформації, що стосується роботи, у соціальних мережах». ***(Melike Pala. 3 in 4 EU employees face cyber threats at work: Survey // Anadolu Ajansı (https://www.aa.com.tr/en/europe/3-in-4-eu-employees-face-cyber-threats-at-work-survey/4074025). 30.09.2026).***

***

«Компанія Microsoft виявила фішингову кампанію, в рамках якої зловмисники маскують легітимне програмне забезпечення для віддаленого моніторингу та управління (RMM) під звичні для робочого середовища завантаження, такі як інсталятори Zoom та програми для перегляду PDF-файлів від Adobe, з метою захоплення контролю над корпоративними комп'ютерами. У рамках цієї операції через обманливі приманки розповсюджується інсталятор MSP360 RMM із цифровим підписом; якщо жертва запускає файл і підтверджує запит адміністратора Windows, програмне забезпечення встановлюється легітимно, змінює правила брандмауера та маскується під звичайну діяльність IT-підтримки, щоб уникнути виявлення… Після активації агент MSP360 запускає PowerShell для прихованої інсталяції другого інструменту RMM — ConnectWise ScreenConnect — створюючи тим самим незалежну стійку присутність у системі та канал для розгортання подальших утиліт, призначених для викрадення паролів та даних браузера. Щоб мінімізувати цю загрозу, Microsoft рекомендує організаціям вести реєстр затверджених програм RMM та блокувати незатверджені екземпляри — зокрема за сертифікатом видавця — застосовувати багатофакторну автентифікацію для дозволених інструментів та активно виявляти ознаки компрометації, такі як несподівані служби RMM, певні хеші інсталяторів або активність PowerShell, ініційовану віддаленими агентами. Крім того, для позбавлення зловмисника плацдарму вирішальне значення має зміна облікових даних для облікових записів, залучених до несанкціонованих розгортань, та обмеження інструментів горизонтального переміщення, таких як PsExec і WMI». ***(Tushar Subhra Dutta. Hackers Disguise Remote Access Tools as Zoom and PDF Installers to Take Over PCs // Cyber Security News (https://cybersecuritynews.com/remote-access-tools/). 30.09.2026).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«У результаті багатонаціональної операції за участю державних і приватних структур було знешкоджено «Sality» — пов'язану з Росією P2P-ботнет, що діяла з 2003 року. Ця ботнет, яку компанія CrowdStrike пов'язує з

групою під назвою «Salty Spider» і яка, як вважається, діяла з території Республіки Башкортостан у Росії, заразила близько 15 000 комп'ютерів по всьому світу. «Sality» використовувалася для розповсюдження шкідливого програмного забезпечення з метою крадіжки облікових даних, розсилки спаму, надання проксі-послуг, експлуатації мереж та проведення розподілених атак типу «відмова в обслуговуванні» (DDoS). В останні роки одним із її основних корисних навантажень був EggJagger — інструмент для перехоплення вмісту буфера обміну, який замінював скопійовані адреси гаманців Bitcoin та Ethereum на адреси, контрольовані зловмисниками. У результаті цієї операції, як стверджується, було викрадено щонайменше 150 000 доларів у криптовалюті, тоді як, за оцінками CrowdStrike, загальний обсяг невитрачених криптовалютних активів групи досяг піку в січні 2025 року, склавши близько 1,68 мільйона доларів…

У цій операції взяли участь правоохоронні органи США та Європи, Європол, компанія CrowdStrike та фонд Shadowserver Foundation — це стало результатом багаторічного розслідування та підготовки, що тривали з 2017 року. Американські органи влади вилучили домени, пов'язані з Sality, а поліція Болгарії, Угорщини та Румунії ліквідувала шкідливу інфраструктуру в Європі. Слідчі подолали стійку децентралізовану архітектуру Sality, скориставшись слабкими місцями в її протоколі «рівний-рівному». Оскільки заражені машини довіряли одноранговим вузлам, не перевіряючи їхню ідентичність, дослідники змогли проникнути в мережу, видаючи себе за легітимні заражені пристрої. Потім вони маніпулювали періодичним процесом перевірки однорангових вузлів у ботнеті, завдяки чому справжні шкідливі вузли втратили репутацію та були видалені, а їхнє місце зайняли спеціально створені системи-«приймачі» (sinkhole).

Ця методика дозволила поступово ізолювати заражені машини від комунікаційної мережі Sality та зупинити поширення шкідливих URL-адрес і пакетів файлів. Пристрої, приховані за брандмауерами або системою перетворення мережевих адрес, були виявлені, коли вони зрештою зв'язалися з «приймальними ямами» під час планових циклів технічного обслуговування. Правоохоронні органи також ліквідували веб-сайти, що використовувалися для розповсюдження додаткових шкідливих програм. Операція продемонструвала, що навіть довгоіснуючі децентралізовані ботнети без традиційного сервера управління можна знешкодити завдяки детальному знанню їхніх протоколів та скоординованим міжнародним діям. Наразі Shadowserver співпрацює з інтернет-провайдерами та командами реагування на інциденти безпеки, щоб виявити решту заражених систем, повідомити жертв та надати підтримку у виправленні ситуації». ***(Tiffany Wang. Global Public-Private Action Disrupts Russia-Linked Sality Botnet // Information Security Media Group, Corp. (https://www.inforisktoday.com/global-public-private-action-disrupts-russia-linked-sality-botnet-a-32732). 02.09.2026).***

***

«ФБР підтвердило, що веде розслідування щодо повідомлень про те, що в «темному вебі» наразі продаються мільйони водійських посвідчень зі всіх куточків США та Канади, що, ймовірно, є одним із найбільших випадків витоку виданих урядом документів, що посвідчують особу, в історії Північної

Америки. За словами Кріса Пірсона, генерального директора компанії BlackCloak, що спеціалізується на цифровому захисті керівників, та колишнього кіберрадника Міністерства внутрішньої безпеки США, цей витік є особливо критичним, оскільки дані не є гіпотетичними, вже перебувають під контролем організованого злочинного угруповання і їх неможливо видалити з даркнету. Серед викрадених записів — зображення лицьової та зворотної сторін водійських посвідчень, дати видачі та закінчення терміну дії, а також адреси проживання, які залишаються актуальними протягом десятиліття. Пірсон зазначив, що навіть відомі особи, які приховують свою особу за допомогою юридичних фірм, товариств з обмеженою відповідальністю та фінансових радників, зазвичай мають свої справжні домашні адреси, вказані у водійських посвідченнях, виданих штатом…

Цей випадок підкреслює дедалі більшу конвергенцію кіберризиків та фізичних загроз для суддів, законодавців та керівників корпорацій — небезпеку, про яку нещодавно нагадали вбивство генерального директора UnitedHealthcare Браяна Томпсона та напади на законодавців штату Міннесота у їхніх власних будинках. Окрім фізичних загроз, Пірсон попередив, що сканування передньої та задньої сторін водійських посвідчень — разом з ультрафіолетовими та інфрачервоними знімками — надає злочинцям саме ті дані, які необхідні для обходу процедур «Знай свого клієнта» (KYC) та перевірок щодо протидії відмиванню грошей у фінансових установах. Він наголосив, що цей інцидент необхідно оцінювати в контексті попередніх випадків, таких як злом Управління кадрового менеджменту (OPM), зазначивши, що викрадені документи, що посвідчують особу, також використовуються як зброя в шахрайських операціях із застосуванням технології «діпфейк», спрямованих проти керівників та їхніх сімей». ***(Chris Riotta. Stolen Driver's Licenses Enable a Decade of Criminal Access // Information Security Media Group, Corp. (https://www.inforisktoday.com/stolen-drivers-licenses-enable-decade-criminal-access-a-32737). 07.09.2026).***

***

«Нідерландські правоохоронні органи заарештували 24-річного засудженого кіберзлочинця Пепійна ван дер Стапа, відомого під псевдонімом «Umbreon», за його ймовірну причетність до крадіжок даних та вимагань, організованих активною хакерською групою ShinyHunters, зокрема до масштабного злом телекомунікаційного провайдера Odido. У результаті різкого загострення ситуації, що сталося одразу після його затримання, решта членів «ShinyHunters» здійснили серію гучних атак у відповідь, зокрема зламали портал ФБР для подання заяв на роботу, щоб викрасти конфіденційні особисті та медичні дані тисяч посадовців, а також вимагали викуп у російського синдикату-вимагача Cl0p… Під час атаки на веб-сайт ФБР на ньому було розміщено зображення «Умбреона», що, на думку слідчих, було зроблено навмисно з метою підстави заарештованого голландця. Джерела вказують, що за цим різким поворотом у діяльності та внутрішнім саботажем стоїть підліток-хакер із Йорданії, відомий як «Рей», який нещодавно взяв під свій контроль угруповання ShinyHunters у рамках більш масштабного об’єднання кіберзлочинців і який веде тривалий конфлікт із ван дер Стапом щодо бренду угруповання та незаконних прибутків. Ці керівні

суперечки розгортаються на тлі того, що ShinyHunters наближається до отримання майже 100 мільйонів доларів від вимагань у 2026 році, після розриву партнерства з хакерською групою TeamPCP, що спеціалізується на атаках на ланцюги поставок, коли правоохоронні органи викрили їхні вкрадені облікові дані… У той час як нідерландська поліція готується до пред'явлення ван дер Стапа перед Роттердамським районним судом — на тлі нових звинувачень у тому, що він організував замахи на вбивство за кордоном — міжнародні правоохоронні органи, зокрема ФБР, активізують розшук решти членів угруповання «ShinyHunters», публічно закликаючи їх здатися, перш ніж вилучена інфраструктура та мінливі союзи викриють їхні особи». ***(Dutch Police Arrest 'Reformed' Hacker in Shiny Hunters Investigation // Krebs on Security (https://krebsonsecurity.com/2026/09/dutch-police-arrest-reformed-hacker-in-shiny-hunters-investigation/). 28.09.2026).***

***

Технічні аспекти кібербезпеки

«Файли cookie браузера — це невеликі фрагменти даних, які надсилаються веб-серверами для збереження важливих налаштувань користувача (наприклад, вмісту кошиків для покупок та сеансів входу за допомогою власних файлів cookie) або для відстеження поведінки користувачів під час перегляду різних веб-сайтів з метою показу цільової реклами за допомогою сторонніх файлів cookie. Оскільки вихід із веб-сайту не призводить до автоматичного видалення цих файлів, кіберзлочинці часто використовують файли cookie для перехоплення сеансів. Вводячи шкідливий JavaScript-код, викачуючи файли з уражених пристроїв або перехоплюючи трафік у незахищених публічних мережах Wi-Fi, зловмисники можуть викрасти дійсні файли cookie та скопіювати їх у свої системи, обманюючи такі платформи, як системи онлайн-банкінгу чи сайти криптовалют, щоб отримати повний доступ без введення облікових даних…

Щоб захиститися від крадіжки файлів cookie та перехоплення сеансів, користувачі можуть дотримуватися низки заходів безпеки та налаштувати відповідні параметри конфіденційності. Захист пристроїв шляхом уникнення невідомих публічних мереж Wi-Fi, увімкнення багатофакторної автентифікації та уникнення підозрілих посилань в електронних листах допомагає запобігти первинному доступу. Крім того, користувачі можуть зменшити ризик, вимкнувши файли cookie сторонніх розробників, використовуючи такі функції, як налаштування «Не відстежувати» у Google Chrome, регулярно вручну видаляючи постійні файли cookie та приймаючи лише необхідні власні файли cookie, що потрібні для основної роботи веб-сайту…

Незважаючи на поширені побоювання щодо безпеки, існує кілька міфів про те, як працюють файли cookie. Файли cookie не є вірусами, шпигунським програмним забезпеченням чи шкідливим кодом, хоча антивірусні програми часто позначають сторонні файли cookie для відстеження, щоб допомогти користувачам керувати конфіденційністю. Крім того, файли cookie не містять особистих контактних даних

чи імен, а також не генерують безпосередньо спам чи спливаючі рекламні оголошення. Натомість вони слугують насамперед для забезпечення безперебійного функціонування веб-сесій та надання даних відстеження для рекламних мереж, тому саме проактивне управління — а не повне уникнення — є ключем до збереження конфіденційності та безпеки в Інтернеті». ***(Gerard Griessel. How Long Do Web Cookies Last? Why Simply Logging Out Is No Longer Safe // Static Media (https://www.bgr.com/2247729/how-long-web-cookies-last-why-logging-out-no-longer-safe/). 06.09.2026).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Галузь кібербезпеки стикається з безпрецедентним сплеском критичних вразливостей у програмному забезпеченні, що значною мірою зумовлено появою інструментів виявлення на основі штучного інтелекту, таких як Project Glasswing від Anthropic. З весни 2026 року кількість повідомлень про вразливості високого та критичного рівнів серйозності від провідних технологічних компаній різко зросла, досягнувши до липня приблизно 2 500 — це значне перевищення історичних показників. Хоча досі залишається незрозумілим, чи свідчить це про реальне збільшення кількості вразливостей, які можна експлуатувати, чи просто про зміну методів їх виявлення, інструменти на основі штучного інтелекту, безперечно, прискорили темпи виявлення недоліків… Цей сплеск викриттів посилюється різким скороченням часу, необхідного зловмисникам для використання цих вразливостей у своїх цілях. Рівень експлуатації вразливостей «нульового дня» зріс майже до 87 відсотків, при цьому середній час, необхідний для їх експлуатації, скоротився до всього одного дня, а за прогнозами до наступного року він може скоротитися до однієї хвилини. Як наслідок, традиційний цикл випуску виправлень, що вимірюється тижнями, тепер є застарілим; «крива виживання експлойтів» опускається до нуля протягом 1,5 місяців після розкриття інформації, що не залишає захисникам жодного запасу часу для усунення вразливостей до того, як вони стануть об’єктом атаки… Зловмисники, що використовують програми-вимагачі, активно пристосувалися до цих умов: у 2025 році понад половина пов’язаних з ними уразливостей (CVE) була використана за допомогою експлойтів «нульового дня». Зрештою, хоча штучний інтелект обіцяє з часом покращити автоматизовані засоби захисту, наразі він прискорює розвиток наступальних можливостей такими темпами, що організації, які затримують навіть короткочасні заходи з встановлення виправлень, стають вкрай вразливими до атак». ***(Guru Baran. Critical Software Vulnerabilities Surge From Under 100 to More Than 600 a Month // Cyber Security News (https://cybersecuritynews.com/critical-software-vulnerabilities-surge/). 07.09.2026).***

***

«Зловмисники активно використовують критичну вразливість переповнення буфера на основі купи (CVE-2025-25249) у брандмауерах FortiGate для розгортання спеціально розробленого трояна віддаленого доступу (RAT) на базі Node.js під назвою PivotC2. Ця вразливість, що отримала оцінку 9,8 за шкалою CVSSv3, впливає на службу CAPWAP Control у FortiOS та FortiSwitchManager, дозволяючи неавторизованим зловмисникам виконувати довільний код за допомогою спеціально сформованих запитів. Використовуючи власний бінарний файл та JavaScript-стейджер, зловмисники розгортають PivotC2 — спеціально розроблену платформу для подальшої експлуатації, яка встановлює вихідні TLS-з'єднання для обходу обмежень вхідного брандмауера… Важливо, що PivotC2 містить специфічні для FortiGate функції, які дозволяють збирати конфігурації пристроїв та автоматично розшифровувати зашифровані поля облікових даних, розкриваючи VPN-ключі у вигляді відкритого тексту, облікові дані SSL-VPN та паролі адміністраторів. Шкідливе ПЗ також має «автоматичний режим», який забезпечує автоматичне масове проникнення без втручання користувача шляхом послідовного збору конфігурацій, розшифрування облікових даних та запуску внутрішнього сканування портів. Підрозділ SOCRadar Threat Research Unit приписує цю кампанію російськомовній кіберзлочинній групі, що діє з фінансових мотивів і, ймовірно, використовувала допомогу штучного інтелекту при розробці цього інструменту. Зловмисники просканували понад 30 000 IP-адрес і успішно заразили 178 пристроїв, причому найвищі показники зараження зафіксовано у США, Чилі, Колумбії та Великій Британії… Ці вторгнення призвели до серйозних наслідків, зокрема до латерального переміщення та витоку даних поштових скриньок Microsoft Exchange. У зв'язку з цим організаціям настійно рекомендується негайно встановити оновлення до найновіших версій Fortinet, обмежити зовнішній доступ до портів управління CAPWAP, проводити пошук підозрілих процесів Node.js та терміново змінити всі облікові дані, що зберігаються локально, у разі виявлення будь-яких ознак компрометації». ***(Guru Baran. Hackers Actively Exploiting FortiGate Firewalls to Deploy Custom Node.js Malware // Cyber Security News (https://cybersecuritynews.com/fortigate-firewalls-hacked-to-deploy-malware/). 08.09.2026).***

***

«У рамках вересневого «Вівторка оновлень» компанія Microsoft усунула рекордну кількість — 974 — вразливостей у своїх продуктах, серед яких понад 110 були класифіковані як критичні, а також дві вразливості типу «нульового дня», які вже активно експлуатувалися в мережі. Ці дві уразливості «нульового дня», відстежувані як CVE-2026-81963 у стеку Windows Update та CVE-2026-85880 у компоненті Advanced Local Procedure Call, дозволяють зловмисникам із локальним доступом підвищити свої привілеї. Експерти з кібербезпеки попереджають, що ці уразливості, пов'язані з підвищенням привілеїв, ймовірно, поєднуються з уразливими місцями, що дозволяють виконувати код, для розповсюдження шкідливого програмного забезпечення або програм-вимагачів, і закликають організації негайно усунути ці уразливості. Безпрецедентний обсяг виправлень цього місяця збільшив загальну кількість виправлень Microsoft за рік до

2 760, що більш ніж удвічі перевищує кількість уразливостей, усунених за той самий період минулого року…

Окрім активно експлуатованих уразливостей типу «нульового дня», оновлення усунуло кілька вразливостей з високим рівнем небезпеки, що можуть поширюватися як черв'яки. Серед них — уразливість Exchange Server (CVE-2026-55007), яка дозволяє виконати віддалений код без автентифікації через шкідливий вкладення електронного листа у форматі Visio, а також уразливість Outlook (CVE-2026-78509), яку можна активувати просто шляхом перегляду повідомлення у панелі попереднього перегляду. Крім того, вразливість у додатку Microsoft Authenticator для Android (CVE-2026-80097) дозволяє зловмисним додаткам викрадати токени автентифікації користувачів. Особливе занепокоєння у мережевих адміністраторів викликають 20 вразливостей, що можуть поширюватися як черв'яки, виявлених у основних службах, таких як DHCP, DNS, Netlogon, Message Queuing та SMB, а також критична вразливість Kerberos (CVE-2026-69676), яка дозволяє користувачам домену запускати код за допомогою одного спеціально сформованого запиту без необхідності введення адміністративних облікових даних…

Різке зростання кількості задокументованих вразливостей значною мірою пов'язане з поширенням інструментів для пошуку помилок, що використовують штучний інтелект, таких як автоматизовані фузери. Цю тенденцію ілюструють великі скупчення однакових вразливостей, зокрема 36 у DHCP-сервері Windows та 64 переповнення купи в біометричній службі Windows. Парадоксально, але ШІ також став джерелом нових слабких місць у безпеці, як це видно на прикладі вразливості, що впливає на SQL Copilot (CVE-2026-65669), яка дозволяє зловмисникам отримувати доступ до баз даних, використовуючи права доступу жертви. Хоча деякі критики галузі попереджають, що дослідження вразливостей за допомогою ШІ може затопити системи помилковими спрацьовуваннями та звітами низької якості, такі організації, як Mozilla, успішно використовують модель Mythos від Anthropic для виявлення сотень справжніх помилок. Незважаючи на стрімке прискорення виявлення вразливостей за допомогою ШІ, відповідного сплеску активних експлойтів поки що не спостерігається, що свідчить про перевагу в захисті, яка полягає у виявленні вразливостей до того, як зловмисники зможуть їх використати…» ***(Ana Maria. Microsoft patches a record 974 flaws, and two are already under attack // Cogneve, INC. (https://thenextweb.com/news/microsoft-september-patch-tuesday-974-flaws-two-zero-days). 10.09.2026).***

***

«Зловмисники активно використовують критичні та високоризикові вразливості в самостійно розгорнутих серверах JFrog Artifactory для обходу аутентифікації, підвищення привілеїв та розгортання шкідливих бекдорів. Згідно зі звітом компанії Wiz, що спеціалізується на хмарній безпеці, зловмисники, зафіксовані в період з серпня по вересень 2026 року, поєднують у ланцюжок уразливості CVE-2026-42018 та CVE-2026-42016, щоб спочатку отримати JSON-токен з низьким рівнем привілеїв для внутрішнього анонімного користувача, а потім, скориставшись недостатньою перевіркою токена, підвищити рівень до

токена з правами адміністратора. Крім того, третя критична уразливість, що дозволяє обійти аутентифікацію (CVE-2026-82329), використовується для безпосереднього створення токенів адміністратора. Після отримання адміністративного доступу — іноді менш ніж за п’ять хвилин — зловмисники встановлюють шкідливі плагіни Groovy для виконання довільних команд та розгортають спеціальний бекдор на базі Rust із функціями управління та контролю… Подальші дії після проникнення включають завантаження додаткових шкідливих програм у тимчасові каталоги, завантаження веб-шелів, викрадення даних конфігурації Artifactory та ключів приєднання до кластера, перелік репозиторіїв і користувачів, а також введення підроблених SSH-ключів у новостворені облікові записи. Компанія Wiz попереджає, що від 49% до 62% доступних екземплярів Artifactory залишаються вразливими принаймні до однієї з цих вразливостей. У зв’язку з цим системним адміністраторам настійно рекомендується негайно оновити Artifactory до останніх версій із виправленими вразливостями, обмежити доступ до систем лише довіреним користувачам та ретельно перевірити свої середовища на наявність ознак компрометації, таких як несподіване створення токенів, підроблені облікові записи адміністраторів та підозріла активність плагінів». ***(Bill Toulas. Artifactory flaws chained in attacks deploying backdoor malware // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/artifactory-flaws-chained-in-attacks-deploying-backdoor-malware/). 11.09.2026).***

***

«Агентство з кібербезпеки та безпеки інфраструктури (CISA) опублікувало термінове попередження щодо активного використання в реальних умовах двох критичних вразливостей типу «нульового дня» у продуктах Citrix NetScaler ADC та Gateway, що мають ідентифікатори CVE-2026-88771 та CVE-2026-88772. Ці незалежні, але надзвичайно серйозні уразливості — уразливість, що дозволяє віддалено виконати код через неналежну перевірку вхідних даних, та уразливість, пов’язана з переповненням пам’яті — спрямовані проти важливої корпоративної інфраструктури, яка використовується для автентифікації користувачів та балансування навантаження в мережі… Неминуча загроза стала приводом для попереджувальних сповіщень, у яких службам безпеки настійно рекомендувалося відключити сервери; згодом фонд Shadowserver Foundation повідомив про понад 20 000 незахищених екземплярів, які перебували під загрозою злому. У відповідь на загострення кризи CISA додала обидва CVE до свого каталогу «Відомі уразливості, що експлуатуються», а компанія Citrix опублікувала вичерпний бюлетень з безпеки, присвячений уразливостям «нульового дня» та шести додатковим вразливостям… Компанія Citrix попередила, що наслідки цих вразливостей, які можуть призвести до віддаленого виконання коду, відмови в обслуговуванні та контрабанди HTTP-запитів, залежать від конкретних конфігурацій розгортання, таких як увімкнення протоколу Datagram Transport Layer Security (DTLS) у випадку експлойта, пов’язаного з переповненням пам’яті. Відповідно, компанія закликає команди з безпеки ретельно перевіряти попередні умови розгортання перед застосуванням

оновлень та рекомендує негайно ізолювати будь-які потенційно скомпрометовані пристрої, скасувати їхні облікові дані, а у випадку віртуальних пристроїв — створити їхні знімки для збереження криміналістичних доказів». ***(David Jones. Citrix urges immediate upgrades of NetScaler amid widespread exploitation attempts // TechTarget, Inc. (https://www.cybersecuritydive.com/news/citrix-upgrades-netscaler-exploitation/831502/). 28.09.2026).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«У відповідь на ескалацію кібергонки озброєнь, що базується на штучному інтелекті, компанія CrowdStrike представила SafeMind — нову автономну систему кібербезпеки, розроблену у партнерстві з NVIDIA та CoreWeave. Система SafeMind, що працює на базі сімейства відкритих моделей NVIDIA Nemotron та хмарної платформи AI Cloud від CoreWeave для навчання та інференції, символізує стратегічний перехід від простого виявлення загроз до їх активного нейтралізування. CrowdStrike стверджує, що система значно перевершує провідні передові та відкриті моделі, забезпечуючи на 29 відсотків вищий рівень виявлення, у шість разів швидше комплексне усунення загроз та економію витрат на 99 відсотків. У відповідь на ескалацію кібергонки озброєнь, що базується на штучному інтелекті, компанія CrowdStrike представила SafeMind — нову автономну систему кібербезпеки, розроблену у партнерстві з NVIDIA та CoreWeave. Система SafeMind, що працює на базі сімейства відкритих моделей NVIDIA Nemotron та хмарної платформи AI Cloud від CoreWeave для навчання та інференції, символізує стратегічний перехід від простого виявлення загроз до їх активного нейтралізування. CrowdStrike стверджує, що система значно перевершує провідні передові та відкриті моделі, забезпечуючи на 29 відсотків вищий рівень виявлення, у шість разів швидше комплексне усунення загроз та економію витрат на 99 відсотків… Завдяки контролю над усім технологічним стеком — від датчиків до моделей — компанія CrowdStrike прагне закласти основу для наступного десятиліття безпеки на базі штучного інтелекту. Система буде доступна корпоративним клієнтам у рамках програми Project QuiltWorks, що дозволить інтегрувати її не лише з власною платформою Falcon від CrowdStrike. Зрештою, запуск SafeMind підкреслює більш широкий перехід галузі до автономних систем захисту із замкнутим циклом, здатних вживати негайних автоматизованих заходів проти кіберзагроз, а не просто позначати їх». ***(Guru Baran. CrowdStrike Launches SafeMind – First Agentic Cybersecurity Solution Built for Defenders // Cyber Security News (https://cybersecuritynews.com/crowdstrike-launches-safemind/). 06.09.2026).***

***

«Компанія ASUS випустила термінове оновлення безпеки для свого програмного забезпечення ASUS Control Center Enterprise (ACC) з метою

усунення вразливості найвищого рівня серйозності, зареєстрованої під номером CVE-2026-75754, яка має максимальний бал за шкалою CVSS 4.0 — 10,0. Ця критична вразливість дозволяє зловмисникам дистанційно отримати повний адміністративний контроль над платформою ACC та всіма керованими пристроями без необхідності введення пароля або взаємодії з користувачем. Ця вразливість є результатом ланцюжка експлойтів, що складається з трьох частин: відсутність перевірки автентифікації у критично важливій функції, вразливість типу «підробка запитів на стороні сервера» (SSRF), що розкриває ключ шифрування системи, та наявність жорстко закодованих облікових даних у самому програмному забезпеченні… Використовуючи уразливість SSRF для отримання ключа шифрування, зловмисник може змусити локальну службу відкрити прихований SSH-бекдор на TCP-порту 2222, до якого він потім отримає доступ за допомогою жорстко заданих облікових даних, щоб отримати повний root-доступ. Оскільки ACC призначена для централізованого управління парком серверів, ПК та робочих станцій, компрометація навіть одного екземпляра може надати зловмисникам можливість віддаленого контролю над усім корпоративним IT-середовищем, що дозволить їм читати, змінювати або видаляти критично важливі дані… Ця вразливість стосується всіх версій програмного забезпечення аж до версії 4.0.0.2 включно, що змусило компанію ASUS закликати організації негайно оновити програмне забезпечення до версії 3.1.0.9 або пізнішої. Для підприємств, які не мають можливості негайно встановити виправлення, тимчасовими заходами щодо мінімізації ризиків є ізоляція інтерфейсів управління ACC від публічних мереж, блокування вхідного та вихідного трафіку на порту 2222, а також перевірка хостів на наявність несанкціонованих SSH-слухачів». ***(Guru Baran. ASUS Control Center Flaw Allows Attackers to Gain Full Admin Control of the System // Cyber Security News (https://cybersecuritynews.com/asus-control-center-vulnerability/). 06.09.2026).***

***

«Компанія MaxxKonnect запустила безкоштовний веб-генератор паролів на сайті fccpassword.com, щоб допомогти радіо- та телевізійним станціям дотримуватися нових правил кібербезпеки Федеральної комісії з питань зв'язку (FCC), які набувають чинності 29 вересня. Цей інструмент працює локально в браузері користувача, генеруючи випадкові 15-символьні паролі та відфільтровуючи слова зі словника, а також поширені одно- та дволітерні слова. Хоча для доступу до генератора користувачам необхідно заповнити форму, створення облікового запису не вимагається. Майбутні вимоги FCC поширюються на обладнання Системи екстреного оповіщення, канали зв'язку між студією та передавачем, а також інші пристрої з дистанційним керуванням, які обробляють, маршрутизують або вставляють контент у програмування станції… Згідно з цими правилами, паролі, що захищають обладнання, на яке поширюються ці вимоги, повинні містити щонайменше 15 символів, не містити слів зі словника та не використовуватися повторно в інших облікових записах, додатках або на інших пристроях. Компанія MaxxKonnect наголосила, що використання паролів, які відповідають вимогам, задовольняє лише одну частину вимог FCC, оскільки станції

як і раніше зобов'язані своєчасно встановлювати оновлення прошивки та виправлення безпеки, а також ізолювати обладнання, на яке поширюються ці вимоги, за допомогою брандмауерів або аналогічних засобів захисту на основі сегментації мережі». ***(Nick Langan. MaxxKonnect Offers Free FCC Compliance Password Generator // Future Publishing Limited (https://www.radioworld.com/tech-and-gear/products/maxxkonnect-offers-free-fcc-compliance-password-generator). 11.09.2026).***

***

«Компанія Google запустила програму Fairwind — ініціативу, покликану надати клієнтам хмарних сервісів, державним установам та партнерам у сфері кібербезпеки доступ до інструментів безпеки на основі штучного інтелекту, що працюють на моделях Gemini. Програма дозволяє організаціям-учасницям самостійно виявляти та усувати вразливості систем, оптимізуючи процес усунення проблем та зменшуючи необхідність розробки власних спеціалізованих інструментів, що вимагають значних ресурсів. Для малих підприємств, яким часто доводиться шукати баланс між захистом від складних загроз та операційними й фінансовими обмеженнями, ця ініціатива пропонує доступний шлях до посилення цифрового захисту, збереження даних клієнтів та зміцнення довіри на ринку, який дедалі більше перебуває під загрозою складних кіберризиків…

Хоча програма Fairwind відкриває значні можливості для підвищення рівня безпеки та отримання конкурентної переваги, власники малих підприємств повинні ретельно оцінити практичні аспекти її впровадження. Успішна інтеграція інструментів штучного інтелекту на базі Gemini в існуючу технічну інфраструктуру може вимагати навчання персоналу, коригування робочих процесів або найму спеціалістів для управління цією технологією без перебоїв у роботі. Крім того, керівники малих підприємств повинні оцінити довгострокову окупність інвестицій, зваживши витрати та стратегічне планування, необхідні для впровадження, проти серйозних фінансових, регуляторних та репутаційних ризиків, пов'язаних із використанням застарілих засобів кіберзахисту». ***(David Wilson. Google Launches Fairwind Program to Empower Cyber Defenders with AI // Small Business Trends LLC. (https://smallbiztrends.com/google-launches-fairwind-program-to-empower-cyber-defenders-with-ai/). 13.09.2026).***

***

«SE Labs, незалежна організація з тестування кібербезпеки, оголосила про запуск PIVOT — передової програми тестування корпоративної безпеки, в якій беруть участь такі постачальники: Broadcom, CrowdStrike, Fortinet, Palo Alto Networks та Sophos. Запланована до публічного випуску на початку 2027 року, ця перша оцінка заповнює дефіцит даних технічної оцінки, що зростає внаслідок відмови провідних постачальників від участі в оцінках MITRE Engenuity ATT&CK. Замість того, щоб покладатися виключно на показники виявлення, PIVOT оцінює повні ланцюги атак, щоб визначити, наскільки далеко просунувся зловмисник, чи вдалося механізмам захисту успішно запобігти проникненню до

того, як було завдано шкоди, та чи змогли захисники зберегти контроль над ситуацією під час підвищення привілеїв або горизонтального переміщення…

Розроблений для допомоги корпоративним командам із закупівель та керівникам з інформаційної безпеки (CISO), PIVOT також оцінює зрозумілість та контекст інформації, що надається командам з оперативної безпеки під час та після інциденту... Для забезпечення більш широкого незалежного аналізу SE Labs надаватиме вихідні дані оцінки безпосередньо дослідницьким компаніям Gartner та Forrester. У першому звіті за 2027 рік будуть представлені детальні результати порівняльного аналізу сценаріїв, а також опубліковано перший публічний рейтинг PIVOT». ***(Major Cyber Security Vendors Back SE Labs' New Model for Independent Security Testing // Cision US Inc. (https://www.prnewswire.com/news-releases/major-cyber-security-vendors-back-se-labs-new-model-for-independent-security-testing-302876587.html). 15.09.2026).***

***

Питання криптографії

«Група G7 закликає уряди та організації якомога швидше впровадити квантовостійке шифрування для захисту конфіденційних даних від технологічно просунутих зловмисників. Практично всі сучасні галузі — зокрема банківська справа, оборона та телекомунікації — покладаються на традиційні стандарти шифрування, такі як AES, які на даний момент практично неможливо зламати через величезні обчислювальні ресурси, що для цього потрібні. Однак досконалі квантові комп’ютери, що застосовуються у криптографії, працюватимуть за принципово іншими принципами, які дозволять зламати сучасні стандарти шифрування. Щоб зменшити цю загрозу, G7 рекомендує організаціям спланувати та завершити перехід на постквантову криптографію (PQC) відповідно до графіків, встановлених національними органами з кібербезпеки…

Несвоєчасний перехід несе значні операційні та комерційні ризики, оскільки організації, що зволікають, можуть втратити конфіденційну інформацію, позбутися конкурентної переваги або бути виключеними з процедур державних закупівель та укладення контрактів. Для забезпечення плавного переходу G7 рекомендує організаціям провести інвентаризацію своїх криптографічних активів, проаналізувати взаємозалежності, визначити пріоритетність критично важливих систем та реалізувати поетапну стратегію, що ґрунтується на оцінці ризиків. Крім того, організації можуть зменшити загальні витрати на міграцію та запобігти небезпечним впровадженням, купуючи продукти з інтегрованою PQC та переходячи на квантово-безпечні системи під час стандартних циклів оновлення». ***(Sead Fadilpašić. G7 tells businesses to get ready for quantum cybersecurity threats // Future US, Inc. (https://www.techradar.com/pro/security/g7-tells-businesses-to-get-ready-for-quantum-cybersecurity-threats). 07.09.2026).***

***