**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

№ 11 (листопад)

Київ – 2025

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., 2025. № 11 (листопад). 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.

ЗМІСТ

Кібервійна проти України

«…Тривала війна в Україні стала критичним фронтом кібервійни, даючи важливі уроки щодо еволюції тактики Росії та важливості міжнародної співпраці в галузі кіберзахисту. З 2014 року, а особливо перед повномасштабним вторгненням 2022 року, Росія використовувала Україну як полігон для випробування складних, багатовекторних кібероперацій, що поєднують шкідливе програмне забезпечення, фішинг та дезінформацію, часто скоординовані з кінетичними військовими ударами. Оскільки ці вдосконалені кіберзброї можна легко застосувати проти інших країн, оборона України є невід'ємною частиною глобальної безпеки, що робить необхідним постійну співпрацю між Україною, США та іншими союзниками…

Незважаючи на це, інституційні заходи реагування були повільними, що було спричинено небажанням ділитися конфіденційною інформацією та складністю координації між різними юрисдикціями. Для протидії агресії Росії експерти рекомендують посилити партнерство між державним і приватним секторами, формалізувати роль цивільних «кіберволонтерів», таких як ІТ-армія України, та збільшити інвестиції в захист критичної інфраструктури. Крім того, є вагомі підстави для розширення санкцій проти російського ІТ-сектору з метою обмеження його доступу до передових технологій та інноваційних можливостей. Зрештою, конфлікт підкреслює, що, хоча технології мають вирішальне значення, люди залишаються центральним елементом кіберзахисту, що підкреслює необхідність постійного навчання та індивідуальної пильності для створення комплексної системи безпеки…» ***(Oleksandr Bakalynskyi, Maggie McDonough. Learning the lessons from Ukraine's fight against Russian cyber warfare // Atlantic Council (https://www.atlanticcouncil.org/blogs/ukrainealert/learning-the-lessons-from-ukraines-fight-against-russian-cyber-warfare/). 06.11.2025).***

***

«Проросійська хакерська група Sandworm посилила свої руйнівні кібератаки проти України, перейшовши від шпигунства до використання складних шкідливих програм для знищення даних під назвою ZEROLOT і Sting. Стратегія групи зосереджена на завданні максимальної шкоди шляхом атак на критично важливі для економіки та національної безпеки України сектори, зокрема уряд, енергетику, логістику та зернову промисловість…

Ці атаки спрямовані на те, щоб спричинити остаточну втрату даних. Шкідливе програмне забезпечення отримує доступ за допомогою спіфішингу та скомпрометованих облікових даних, а потім виконує руйнівні процедури, які перезаписують критично важливі системні файли та таблиці розділів, роблячи системи непрацездатними. ZEROLOT спеціально націлений на головні завантажувальні записи, щоб запобігти завантаженню операційних систем, а Sting використовує підвищені привілеї для широкомасштабного пошкодження. Обидва

віпери використовують антикриміналістичні техніки для видалення журналів і містять механізми синхронізації, щоб максимально поширитись по мережі до виявлення, забезпечуючи руйнівний вплив…» ***(Tushar Subhra Dutta. Sandworm Hackers Attacking Ukranian Organizations with Data Wiper Malwares // Cyber Security News (https://cybersecuritynews.com/sandworm-hackers-attacking-ukranian-organizations/). 06.11.2025).***

***

«…Останній звіт ESET про діяльність APT показує, що російські хакери, які фінансуються державою, як і раніше, атакують Україну та її союзників, але їхні методи та тактика еволюціонували:

• Sandworm (APT44/Iridium) залишається найбільш руйнівним актором, випускаючи протягом 2025 року кілька сімейств програм для знищення даних — Zerolot, Sting та інші. Серед останніх цілей — українські урядові установи, енергетичні та логістичні компанії, а також, що важливо, зерновий сектор, який є основним джерелом доходів України в умовах війни.

• Первинний доступ як і раніше отримують переважно за допомогою spear-phishing. У деяких випадках менш відома група UAC-0099 спочатку зламує мережі, а потім передає їх Sandworm для знищення.

• Gamaredon, найпродуктивніша шпигунська група, модернізувала свої програми-крадії PteroPSDoor і PteroVDoor і тепер приховує трафік за допомогою нових тунельних і безсерверних служб; також було помічено її співпрацю з Turla.

• RomCom (Storm-0978) використовував уразливість нульового дня в WinRAR для встановлення бекдорів у компаніях, що займаються обороною, фінансами, логістикою та виробництвом у Європі та Канаді.

• Окремий зловмисник під псевдонімом InedibleOchotense видавав себе за компанію ESET у фішингових атаках та повідомленнях у Signal…

ESET робить висновок, що, незважаючи на періодичні повідомлення про перехід до чистого шпигунства, атаки з видаленням даних «залишаються частим інструментом російських зловмисників в Україні». Жертви, які не є громадянами України, зазвичай пов'язані з військовими діями, що свідчить про те, що російська розвідка зосередила свої кіберресурси на конфлікті. У звіті також відстежуються паралельні кампанії китайських, іранських і північнокорейських APT, але найінтенсивніша і найруйнівніша діяльність продовжує походити з Росії…» ***(Ionut Arghire. Destructive Russian Cyberattacks on Ukraine Expand to Grain Sector // Wired Business Media Publication (https://www.securityweek.com/destructive-russian-cyberattacks-on-ukraine-expand-to-grain-sector/). 07.11.2025).***

***

Світові тенденції в галузі кібербезпеки

«У сучасному цифровому світі впровадження комплексних найкращих практик у сфері кібербезпеки є надзвичайно важливим для забезпечення безперебійної роботи бізнесу та захисту активів від нових загроз. Основні заходи

включають обов'язкове використання надійних унікальних паролів із менеджером паролів, обов'язкову багатофакторну автентифікацію (MFA) та суворе дотримання принципу мінімальних привілеїв шляхом обмеження доступу співробітників до конфіденційних даних відповідно до службової необхідності. Регулярне навчання з питань кібербезпеки має вирішальне значення, оскільки співробітники є першою лінією захисту від основних методів атак, таких як фішинг та соціальна інженерія…

Ефективний захист даних вимагає системного підходу: регулярне резервне копіювання поза межами підприємства; шифрування даних як під час зберігання, так і під час передачі; а також план швидкого реагування на інциденти, підкріплений своєчасним оновленням програмного забезпечення та систем. Безпека підприємства повинна базуватися на стійкості, ідентифікації всіх критично важливих активів та підтримці адаптивних політик із багаторівневим захистом.

Бізнес також повинен протистояти новим загрозам, посиленим технологіями. Кібератаки на основі штучного інтелекту використовують штучний інтелект для автоматичного сканування вразливостей, створення надзвичайно переконливих фішингових кампаній та генерації депфейків для соціальної інженерії. Ransomware-as-a-Service (RaaS) знизив бар'єр для входу кіберзлочинців. Крім того, розширення 5G та периферійних обчислень збільшує вразливість мереж, а внутрішні загрози посилюються в умовах віддаленої роботи. Критичні ризики також виникають через атаки на ланцюги постачання, вразливість хмарних контейнерів та конвергенцію систем IT та операційних технологій (OT)…

Сучасна безпека підприємств посилюється за допомогою спеціалізованих інструментів, таких як платформи безпеки для безперервного моніторингу, багаторівнева безпека електронної пошти та надійні функції, що пропонуються хмарними провайдерами. Надаючи пріоритет кібербезпеці в організаційній культурі, впроваджуючи ці технічні та організаційні заходи та інвестуючи в постійне зниження ризиків, підприємства можуть перетворити безпеку з питання дотримання вимог на постійну стратегічну перевагу, забезпечуючи стійкість до складних атак». ***(Renz Soliman. Top Cybersecurity Best Practices Business Leaders Must Implement Today for Ultimate Business Data Protection and Enterprise Security Basics // Tech Times LLC. (https://www.techtimes.com/articles/312482/20251104/top-cybersecurity-best-practices-business-leaders-must-implement-today-ultimate-business-data.htm). 04.11.2025).***

***

«Власники малого бізнесу стикаються з гострою проблемою кібербезпеки, оскільки мобільні пристрої стають центральним елементом їхньої діяльності. Згідно з індексом мобільної безпеки Verizon 2025 (Mobile Security Index, MSI), 85% організацій стикаються зі збільшенням кількості атак на мобільні пристрої. Ця ситуація значно погіршується через поширене використання співробітниками генеративних інструментів штучного інтелекту: хоча 93% організацій повідомляють про використання штучного інтелекту для виконання завдань, лише 17% мають конкретні засоби контролю безпеки для протидії загрозам, пов'язаним зі штучним інтелектом, і ця розбіжність робить багато підприємств вразливими…

Малі та середні підприємства (МСП) особливо вразливі: 54% вважають, що вони мають більше втратити від порушення безпеки, а 57% відчувають себе в невигідному становищі щодо ресурсів у порівнянні з більшими підприємствами. Ця вразливість підкреслюється тим фактом, що 39% співробітників МСП натиснули на шкідливі посилання під час тестів на smishing. Щоб зменшити ризики, МСП повинні терміново надати пріоритет надійному навчанню співробітників з питань мобільної безпеки (наразі це роблять лише 56%) та інвестувати в передове навчання з питань ризиків, пов'язаних зі штучним інтелектом, яке наразі пропонують лише 39% МСП.

Кріс Новак з Verizon Business підкреслює, що мобільна безпека зараз є «битвою, яка ведеться в долоні кожного співробітника», що робить проактивний, багаторівневий підхід необхідним для бізнесу. Інвестиції в інтегровані рішення з безпеки, які об'єднують захист на мобільних платформах і в мережах, мають вирішальне значення для захисту операцій, зміцнення довіри клієнтів і забезпечення безперебійної роботи бізнесу в умовах все більш складних загроз, що базуються на штучному інтелекті…» ***(David Wilson. AI-Powered Attacks Surge: Organizations Face Major Mobile Security Risks // Small Business Trends LLC. (https://smallbiztrends.com/ai-powered-attacks-surge-organizations-face-major-mobile-security-risks/). 02.11.2025).***

***

«…План реагування на інциденти кібербезпеки (IRP) забезпечує структурований, повторюваний процес, який дозволяє командам безпеки швидко та ефективно управляти кібератаками за допомогою п'яти ключових етапів: підготовка, ідентифікація, локалізація, ліквідація та відновлення, а також винесені уроки. Основою є підготовка, під час якої організації встановлюють політики, проводять оцінку ризиків та симуляції для формування «м'язової пам'яті». Наступним етапом є ідентифікація, яка передбачає використання контексту та інформації про загрози для збагачення сповіщень та визначення пріоритетності реальних загроз над помилковими спрацьовуваннями. Після підтвердження інциденту команда переходить до локалізації, ліквідації та відновлення, під час яких ізолює уражені системи, видаляє шкідливі файли та відновлює роботу з чистих резервних копій, підтримуючи при цьому чітку комунікацію та документацію…

Після інциденту фаза «вивчення уроків» має вирішальне значення для перетворення досвіду в довгострокову стійкість шляхом аналізу показників ефективності та оновлення інструкцій. Всі ці кроки об'єднує рівень координації, який автоматизує дії та інтегрує такі інструменти, як SIEM, EDR та розвідка загроз, щоб забезпечити безперебійну, скоординовану реакцію. Дотримуючись цієї структури, організації можуть перетворити потенційно хаотичну подію на контрольовану, точну операцію, мінімізуючи збитки та постійно зміцнюючи свою безпеку…» ***(Michael Lyborg. How to Create a Cybersecurity Incident Response Plan // Techstrong Group Inc. (https://securityboulevard.com/2025/11/how-to-create-a-cybersecurity-incident-response-plan-4/). 07.11.2025).***

***

«У сучасній цифровій економіці конфіденційність даних та кібербезпека стали невід'ємними складовими систем ESG (екологічних, соціальних та управлінських), виходячи далеко за межі простого дотримання законодавчих вимог. Найбільш прямим є зв'язок з «управлінням», яке вимагає надійних корпоративних структур для забезпечення законної та безпечної обробки даних, підкріпленої відповідальністю та «захистом даних за замовчуванням». Існує також чітка «соціальна» відповідальність, оскільки захист персональних даних є фундаментальним правом людини, і підприємства повинні гарантувати, що їхні інтереси не переважають право особи контролювати власну інформацію. Навіть «екологічний» аспект є актуальним: принцип мінімізації даних — збір тільки необхідної інформації — дозволяє економити ресурси, а оптимізація цифрової інфраструктури з метою підвищення енергоефективності зменшує вплив на навколишнє середовище…

Цей зв'язок є особливо важливим для фондів прямих інвестицій в Азії, де такі юрисдикції, як Китай, Гонконг і Сінгапур, мають швидко розвиваються закони про захист даних. Фонди повинні проводити ретельну перевірку конфіденційності перед інвестуванням, а потім вимагати від портфельних компаній інтегрувати конкретні політики кібербезпеки та конфіденційності даних у свої програми ESG. Універсальний підхід є неефективним; натомість необхідні індивідуальні рішення, адаптовані до конкретного регіону. Для зменшення фінансового ризику фонди також повинні забезпечити, щоб компанії з їхнього портфеля мали страхування кібервідповідальності. Зрештою, надійний захист конфіденційності даних та кібербезпека є необхідними для зменшення ризиків та побудови сталого, відповідального бізнесу…» ***(Chuan Sun and Tingting Gao. Data Privacy and Cybersecurity: Are You Prepared for the Challenges? // Morrison Foerster LLP (https://www.mofo.com/resources/insights/251106-data-privacy-cybersecurity-are-you-prepared-for-the-challenges). 06.11.2025).***

***

«…У міру того як комерційна нерухомість стає все більш інтелектуальною та технологічно досконалою, фізична безпека будівель тепер нерозривно пов'язана з кібербезпекою та конфіденційністю даних. Кібератака може паралізувати основні функції будівлі, такі як ліфти, опалення та кондиціонування, зупинивши роботу орендарів та їхніх клієнтів. Тому фахівці з нерухомості повинні проактивно інтегрувати надійні засоби захисту даних, щоб задовольнити вимоги сучасних мешканців…

Щоб зробити це ефективно, вони повинні прийняти п'ять ключових стратегій. По-перше, вони повинні знати, якими даними вони володіють, включаючи конфіденційну інформацію про орендарів та їхніх клієнтів. По-друге, вони повинні розуміти, де ці дані зберігаються і як вони захищаються, забезпечуючи їх шифрування та функціонування систем на основі принципу нульової довіри. По-третє, всі юридичні та договірні документи, такі як договори оренди, повинні чітко визначати обов'язки щодо захисту даних. По-четверте, так само як будівлі мають план дій на випадок пожежі, вони повинні мати актуальний і доступний план реагування на інциденти, пов'язані з «пожежею» даних. Нарешті, ці засоби захисту

повинні регулярно перевірятися та оцінюватися, подібно до детекторів диму, щоб переконатися, що вони працюють правильно і можуть бути вдосконалені…» ***(Erin M. Prest and Cynthia B. Keliher. Keeping the Lights On: Cybersecurity & Data Privacy Concerns in the Commercial Real Estate Industry // McCarter & English, LLP (https://www.mccarter.com/insights/keeping-the-lights-on-cybersecurity-data-privacy-concerns-in-the-commercial-real-estate-industry/). 06.11.2025).***

***

«Агентство з кібербезпеки та безпеки інфраструктури США (CISA) та Федеральне бюро розслідувань (FBI) спільно з Національним центром кібербезпеки Великобританії та іншими міжнародними партнерами опублікували нові спільні рекомендації для власників та операторів операційних технологій (OT). Ці рекомендації містять дорожню карту для забезпечення безпеки систем OT, в якій наголошується на створенні «остаточного реєстру» — постійно оновлюваного та точного переліку всіх активів OT. Такий підхід є надзвичайно важливим, оскільки системи OT все більше інтегруються з корпоративними IT-системами, хмарними серверами та сторонніми постачальниками, що робить прозорість активів необхідною для розуміння ризиків та збереження бізнес-функцій…

Ці спільні рекомендації відповідають Директиві NIS2 Європейського Союзу, що свідчить про зближення міжнародного підходу до кібербезпеки OT, який надає пріоритет прозорості активів, відповідальності третіх сторін та оперативній стійкості. У рекомендаціях викладено п'ять основних принципів створення цього остаточного реєстру:

Встановити процеси: Організації повинні визначити процеси для створення та ведення записів з використанням даних з різних джерел, перевіряючи їх на точність та впроваджуючи управління змінами для їх актуалізації.

Створити програму безпеки: Слід встановити офіційну програму управління інформаційною безпекою OT для захисту конфіденційних даних про активи в остаточних записах, використовуючи такі рамки, як ISO/IEC 27001.

Категоризація активів: Активи повинні бути ідентифіковані та категоризовані на основі їх критичності, вразливості та доступності, щоб забезпечити прийняття обґрунтованих, ризик-орієнтованих рішень щодо заходів безпеки…

Підключення до мережі: Організації повинні документувати всі підключення в своїй системі OT, включаючи посилання сторонніх організацій, щоб виявити вразливі місця та впровадити заходи безпеки, такі як сегментація мережі.

Оцінка ризиків, пов'язаних із сторонніми організаціями: Керівництво вимагає глибокого розуміння ризиків, пов'язаних із зовнішніми організаціями, включаючи їхні права доступу, договірні зобов'язання та будь-яке обладнання, яке вони впроваджують у середовище OT…

На практиці компанії повинні розвивати можливості картографування активів, впроваджувати офіційну програму безпеки OT та створювати надійну політику управління ризиками третіх сторін. Відсутність чіткого обліку може приховати вразливі місця та поставити під загрозу операційну стійкість, тоді як його створення забезпечує цілісний огляд, необхідний для ефективного управління кібербезпекою.

Цей міжнародний тиск з боку регуляторних органів дає зрозуміти, що компанії повинні знати свої активи та управляти ризиками в усьому взаємопов'язаному цифровому та фізичному середовищі». ***(William E. Ridgway, David A. Simon, Nicola Kerr-Shaw, Joshua Silverstein, Susanne Werry, Kyle G. Kysela and Josh Metzger. US and UK Issue Joint Cybersecurity Guidance for Operational Technology Systems // Skadden, Arps, Slate, Meagher & Flom LLP (https://www.skadden.com/insights/publications/2025/11/us-and-uk-issue-joint-cybersecurity-guidance). 04.11.2025).***

***

«Сьогодні організації працюють за новою парадигмою кібербезпеки, згідно з якою порушення вважаються неминучими, що кардинально змінило стратегічні пріоритети керівників підприємств. Ситуація ускладнюється розвитком штучного інтелекту, який є двосічним мечем: хоча майже половина керівників у сфері кібербезпеки побоюються, що ШІ збільшить кількість і складність атак, він одночасно став незамінним інструментом захисту. Для боротьби з цими загрозами, пов'язаними зі штучним інтелектом, переважна більшість організацій інтегрують ШІ у свої операції з безпеки, щоб автоматизувати завдання, прискорити реагування на інциденти та значно зменшити фінансовий вплив порушень. Дані показують, що широке використання ШІ може знизити витрати на порушення в середньому на 1,9 мільйона доларів…

Однак ефективність цих технологічних досягнень суттєво обмежується глобальним дефіцитом кваліфікованих кадрів, який, за оцінками, становить від 2,8 до 4,8 мільйона фахівців. Хоча ШІ забезпечує оперативну ефективність, дозволяючи аналітикам зосередитися на стратегії високого рівня, а не на повторюваних завданнях, він не може замінити необхідність людського контролю. Основною перешкодою для впровадження залишається брак персоналу з достатнім досвідом у сфері ШІ, оскільки сучасна безпека вимагає поєднання технічних знань і критичних «м'яких навичок», таких як аналітичне мислення, комунікація та гнучкість для ефективного управління ризиками…

Щоб подолати цей зростаючий розрив у кваліфікації, потрібна довгострокова, скоординована стратегія, заснована на державно-приватних партнерствах і рамках, таких як ті, що пропонуються Світовим економічним форумом. Зосередившись на трьох основних напрямках — обізнаності та освіті, цільовому навчанні та сертифікації, а також впровадженні передових технологій — організації можуть створити стійку робочу силу. Зрештою, найбільш стійкі системи безпеки будуть належати тим, хто здатний гармонізувати швидкість штучного інтелекту з нюансами людського інтелекту». ***(Melonia da Gama, Natasa Perucica. AI is revolutionizing cybersecurity. How should we train the next generation of defenders? // World Economic Forum (https://www.weforum.org/stories/2025/11/cybersecurity-ai-professionals-workers/). 20.11.2025).***

***

«У вівторок, приблизно о 11:20 за UTC, Cloudflare зазнав значного збою, що призвело до перебоїв у роботі таких великих платформ, як OpenAI, X і

Spotify. Компанія підтвердила, що проблема виникла через збій у програмному забезпеченні, відповідальному за управління трафіком, який був спричинений автоматично згенерованим файлом конфігурації для управління загрозами, розмір якого перевищив очікуваний. Cloudflare наголосила, що не було жодних доказів кібератаки або зловмисної діяльності, і пов'язала збій із внутрішньою технічною несправністю, а не з діяльністю зовнішніх суб'єктів…

Спочатку компанія відзначила сплеск «незвичайного трафіку» як потенційний фактор, який спричинив помилки при проходженні трафіку через її мережу. Однак пізніше було з'ясовано, що основною причиною був надмірно великий файл конфігурації. Проблема була повністю вирішена до 14:30 за UTC, хоча Cloudflare попередила про можливе короткочасне погіршення якості послуг у міру нормалізації рівня трафіку. Визнаючи свою важливу роль в інфраструктурі Інтернету, Cloudflare принесла вибачення за перебої в роботі та зобов'язалася опублікувати детальний аналіз на своєму блозі, щоб запобігти подібним інцидентам у майбутньому». ***(Tim Marcin. Cloudflare outage cause revealed: This is what happened // Mashable, Inc. (https://mashable.com/article/cloudflare-outage-cause-revealed-what-happened-why). 18.11.2025).***

***

«18 листопада 2025 року через збій програмного забезпечення в Cloudflare — одному з найбільших у світі постачальників послуг з доставки контенту та забезпечення безпеки — більша частина Інтернету перестала працювати. ChatGPT, X (раніше Twitter), Facebook та безліч інших сайтів стали недоступними на кілька годин, оскільки Cloudflare знаходиться між мільйонами вихідних серверів та їхніми користувачами, обробляючи DNS, оптимізуючи трафік та забезпечуючи захист від DDoS-атак. Хоча компанія відновила роботу сервісу того ж дня, вона попередила про можливі тривалі сплески помилок, проілюструвавши, скільки часу потрібно для стабілізації такої величезної розподіленої системи…

Цей випадок не був іноземною кібератакою, а одноразовою технічною несправністю, проте він все одно паралізував глобальну комунікацію, електронну комерцію та доступ до публічної інформації. Він викрив структурну слабкість: надмірна залежність від декількох посередників інфраструктури створює системний ризик, порівнянний з відключенням критичної інфраструктури…

Ключові висновки:

• Диверсифікація постачальників Підприємствам слід розподілити навантаження DNS, CDN та безпеки між декількома постачальниками, щоб у разі збою трафік міг перейти на резервний канал.

• Створіть посібники з швидкого відновлення Автоматичне перенаправлення на резервні мережі — навіть якщо продуктивність погіршується — є необхідним для безперебійної роботи.

• Проектуйте з урахуванням ізоляції несправностей Архітектура мікросервісів та гнучке планування потужностей запобігають «ефекту доміно», коли різке збільшення прямих запитів призводить до збою вихідних серверів…

Сучасна кіберзахист, отже, є ширшим поняттям, ніж просто блокування хакерів; він охоплює архітектурну стійкість до внутрішніх помилок, помилок

конфігурації та перебоїв у роботі провайдерів. Майбутній Інтернет повинен балансувати між ефективністю, надмірністю та розподілом ризиків, інакше глобальні перебої будуть ставати все частішими та матимуть все більший вплив». ***(The new global disruption and the necessity of cyber defense // Mizan News Agency (https://www.mizanonline.ir/en/news/3216/the-new-global-disruption-and-the-necessity-of-cyber-defense). 20.11.2025).***

***

«Кібербезпека в 2026 році визначається конвергенцією передових технологій і стратегічних підходів, орієнтованих на людину, що робить інновації необхідними для довіри до організації та її стійкості. Ключові тенденції змінюють ландшафт, на чолі з передовими технологіями, такими як виявлення загроз на основі штучного інтелекту для реагування в режимі реального часу та термінова розробка квантово-стійких алгоритмів для захисту від майбутніх загроз дешифрування. Однак однієї лише технології недостатньо; все більший акцент робиться на безпеці, орієнтованій на людину, підвищенні стратегічної ролі CISO та впровадженні культури безпеки в усій організації шляхом безперервної освіти та міжвідомчої співпраці…

Засоби захисту стають все більш адаптивними та інтелектуальними, виходячи за межі статичного контролю і переходячи до платформ, які навчаються на основі поведінки та об'єднують інструменти для кращої видимості. Одночасно організації посилюють свою увагу до безпеки ланцюгів постачання, впроваджуючи суворий постійний моніторинг постачальників для зменшення ризиків, пов'язаних із третіми сторонами. В основі всіх цих тенденцій лежить філософія «Trusted by Design» (Довіра завдяки дизайну), яка інтегрує безпеку на кожному етапі розробки продукту та процесу. Для середніх підприємств впровадження цих інновацій — поєднання сучасних технологій, адаптивних стратегій та сильної культури безпеки — має вирішальне значення для зменшення ризику порушень, забезпечення відповідності вимогам та підтримання безперебійної роботи в умовах дедалі більш складного середовища загроз…» ***(Alex Davis. Top Cybersecurity Innovations for 2026: Key Trends and Strategies // Sourcepass, Inc. (https://blog.sourcepass.com/sourcepass-blog/top-cybersecurity-innovations-for-2026-key-trends-and-strategies). 17.11.2025).***

***

«У четвертому кварталі, як і очікувалося, кількість кібератак різко зростає, оскільки зловмисники використовують скорочення штату, збільшення обсягів транзакцій та сезонні відволікаючі фактори, що робить необхідним проактивне посилення безпеки. Щоб зменшити ці ризики, організації повинні проводити цільові симуляції фішингу, зосереджені на сезонних темах, таких як повідомлення про доставку, проводити повторні тренінги та забезпечувати чіткі канали повідомлення про підозрілі електронні листи. Одночасно необхідно надавати пріоритет гігієні ідентичності шляхом аудиту облікових записів для виправлення відхилень MFA, видалення застарілих засобів автентифікації та скасування непотрібних адміністративних привілеїв…

Технічні засоби контролю також потребують коригування: політику умовного доступу слід переглянути, щоб врахувати особливості віддаленої роботи без шкоди для безпеки, а правила SIEM необхідно налаштувати так, щоб відрізнити законні сезонні сплески від зловмисних аномалій, таких як підвищення привілеїв або масове переміщення даних. Нарешті, стійкість до програм-вимагачів — поширеної загрози під час свят — залежить від перевірки цілісності резервних копій за допомогою тестів відновлення та забезпечення наявності незмінних копій поза межами підприємства. Систематично працюючи над цими напрямками, підприємства можуть усунути прогалини в системі безпеки та забезпечити стабільність роботи протягом періоду свят, який характеризується підвищеним ризиком…» ***(Alex Davis. Strengthening Cybersecurity Before Holiday Season Threat Spikes // (https://blog.sourcepass.com/sourcepass-blog/strengthening-cybersecurity-before-holiday-season-threat-spikes). 17.11.2025).***

***

«Опитування Bitdefender 2025 року, в якому взяли участь понад 7000 споживачів у США, Великобританії, Франції, Німеччині, Іспанії, Італії та Австралії, показує, що, хоча люди побоюються фінансових втрат, шахрайства та крадіжки особистих даних, їхня повсякденна поведінка в Інтернеті залишає їх незахищеними. 14 % респондентів (у США цей показник зростає до 17 %) визнають, що протягом останніх 12 місяців стали жертвами шахрайства, а ще 4 % не впевнені в цьому. Найпоширенішим видом шахрайства є повідомлення про доставку та відправлення (21 %), за ними йдуть спроби фішингу облікових даних, що призводять до захоплення облікових записів (19 %); далі йдуть шахрайство в сфері маркетингу, працевлаштування, криптовалютних інвестицій та романтичних стосунків. Збитки є значними: за екстрапольованими глобальними даними, злочини, пов'язані з шахрайством, зараз перевищують 1 трильйон доларів США на рік, а середній збиток на одну жертву становить 545 доларів США…

Молодші користувачі в два рази частіше стають жертвами шахрайства, ніж люди похилого віку (20 % проти 9,7 %), головним чином через те, що вони надмірно діляться інформацією в соціальних мережах, таких як TikTok, Instagram і WhatsApp, які зараз витіснили електронну пошту як улюблений канал доставки для шахраїв; тим часом старші користувачі все частіше стають жертвами шахрайства через Facebook і шахраїв, які видають себе за надійні компанії або державні органи. Чверть усіх шахрайських схем досі починається з телефонних дзвінків, під час яких використовуються зразки голосів, зібрані в Інтернеті, для створення переконливих «діпфейків» від друзів або родичів за допомогою штучного інтелекту — тактика, про яку нещодавно попередили ФБР та інші агентства.

Щоб зменшити ризик, Bitdefender радить обмежити кількість особистого аудіо- та відеоконтенту, що публікується в Інтернеті, з підозрою ставитися до небажаних дзвінків або повідомлень, що створюють відчуття терміновості, встановити сімейні «слова безпеки» для автентифікації справжніх дзвінків про допомогу, протистояти тиску страху пропустити щось важливе навколо пропозицій, що здаються занадто хорошими, щоб бути правдою, використовувати інструменти виявлення шахрайства, такі як чат-боти, що аналізують повідомлення на наявність

тривожних ознак, та бути в курсі останніх методів шахрайства в епоху, коли обман на основі штучного інтелекту розвивається швидше, ніж будь-коли». ***(Filip TRUȚĂ. 1 in 7 Consumers Got Scammed in the Past Year – Bitdefender Consumer Cybersecurity Survey 2025 // Bitdefender (https://www.bitdefender.com/en-us/blog/hotforsecurity/1-in-7-consumers-got-scammed-in-the-past-year-bitdefender-cybersecurity-survey-2025). 21.11.2025).***

***

«Австралія, Канада, Нідерланди та Нова Зеландія опублікували спільну рекомендацію, в якій закликають інтернет-провайдерів (ISP) та захисників мереж допомогти ліквідувати «куленепробивних» хостинг-провайдерів (BPH). Ці служби навмисно захищають кіберзлочинців, ігноруючи законні запити на видалення та використовуючи такі техніки, як fast flux, для маскування зловмисної діяльності, що дозволяє проводити кампанії з використанням програм-вимагачів, фішингу та шкідливого програмного забезпечення. У рекомендації надаються детальні вказівки, включаючи ретельний аналіз трафіку та встановлення стандартів відповідальності ISP, щоб погіршити роботу цієї злочинної інфраструктури та змусити зловмисників перейти на легальні платформи, які дотримуються вимог правоохоронних органів…

Одночасно з цим, Альянс з безпеки хмарних технологій (CSA) представив нову структуру, оцінку ризиків на основі можливостей (CBRA), щоб допомогти організаціям кількісно оцінити ризики автономних «агентних» систем штучного інтелекту. CBRA оцінює системи на основі критичності, автономності, прав доступу та радіусу впливу, щоб сформувати комплексну оцінку ризику, яка потім відображається на понад 240 елементах контролю в матриці контролю штучного інтелекту CSA для пропорційних заходів безпеки…

В інших новинах Центр інтернет-безпеки (CIS) опублікував низку нових та оновлених стандартів конфігурації безпеки, що охоплюють системи від Windows Server 2025 та різних дистрибутивів Linux до продуктів від Google, IBM та Oracle. Тим часом CISA попередила, що системи виявлення дронів самі по собі становлять ризик для кібербезпеки, закликаючи власників критичної інфраструктури ретельно перевіряти постачальників на предмет безпеки даних, оновлювати політики та специфікації програмного забезпечення. Нарешті, у звіті CIS MS-ISAC за III квартал 2025 року зазначається, що кількість інфікувань шкідливим програмним забезпеченням зросла на 38% за квартал, причому найпоширенішим варіантом залишається фальшиве програмне забезпечення для оновлення програмного забезпечення SocGholish, за яким слідують CoinMiner і Agent Tesla, а також з'явилися нові інфокрадії, такі як Jinupd». ***(Juan Perez. Cybersecurity Snapshot: Global Agencies Target Criminal "Bulletproof" Hosts, as CSA Unveils Agentic AI Risk Framework // Techstrong Group Inc. (https://securityboulevard.com/2025/11/cybersecurity-snapshot-global-agencies-target-criminal-bulletproof-hosts-as-csa-unveils-agentic-ai-risk-framework/). 21.11.2025).***

***

«Кібератаки зараз вражають усі верстви суспільства — від окремих осіб, які стають жертвами фішингових атак, до корпорацій, які паралізуються через програми-вимагачі, і, що найнебезпечніше, критичну інфраструктуру, таку як телекомунікаційні, транспортні та енергетичні мережі, вихід з ладу яких спричинить економічний і фізичний хаос. Оскільки зловмисники постійно вигадують нові тактики, кібербезпека є не лише технічною проблемою, а й питанням суспільної довіри, національної стабільності та міжнародної безпеки. Жодна країна не може ізолювати себе у взаємопов'язаному світі, де такі загрози, як експлойти на основі штучного інтелекту та транскордонні програми-вимагачі, поширюються швидше, ніж традиційні засоби захисту…

Тому ефективний захист вимагає широкого розуміння кіберстійкості: надійних технологій, пильних громадян і, перш за все, скоординованих партнерських відносин між урядами, промисловістю, науковими колами та союзними країнами. Багатосторонні ініціативи, такі як зобов'язання QUAD 2024, взяте на себе Сполученими Штатами, Японією, Індією та Австралією з метою захисту критичної інфраструктури та узгодження стандартів кібербезпеки, а також новий японський закон про посилення кібернетичних можливостей реагування, ілюструють, як спільні норми та спільне нарощування потенціалу можуть підвищити регіональний базовий рівень…

Для Філіппін та інших держав Індо-Тихоокеанського регіону використання цих альянсів забезпечує доступ до інформації про загрози, швидке реагування на інциденти та спільні правила відповідальної поведінки в Інтернеті. Конференція Stratbase Institute «2025 Pilipinas» сприятиме реалізації цієї програми, зібравши політиків, дипломатів, бізнес-лідерів та експертів для розробки практичних заходів: поглиблення кіберініціатив для забезпечення безпеки Індо-Тихоокеанського регіону, визначення стратегічної ролі кібербезпеки в умовах транскордонних загроз та вдосконалення правових, політичних і технічних рамок, що лежать в основі національної та регіональної стійкості. Коротко кажучи, обіцянки цифрової ери можуть бути реалізовані лише в тому випадку, якщо країни колективно зміцнять свою оборону, обмінюються знаннями та впровадять кібергігієну в усі верстви суспільства…» ***(Victor Andres C. Manhit. Cybersecurity as the defining challenge of our time: Security at home, cooperation outside // BusinessWorld Publishing (https://www.bworldonline.com/opinion/2025/11/19/713069/cybersecurity-as-the-defining-challenge-of-our-time-security-at-home-cooperation-outside/). 19.11.2025).***

***

«Згідно з доповіддю Immersive «2025 Cyber Workforce Benchmark Report», існує тривожна розбіжність між впевненістю та реальністю в питаннях кібербезпеки. Хоча 91% керівників вважають, що їхня організація здатна впоратися з серйозним інцидентом, загальні показники стійкості не покращилися з 2023 року, а час реагування на критичні ситуації залишається незмінним. Наприклад, у модельованому кризовому сценарії учасники в середньому продемонстрували низьку точність прийняття рішень (22%) і витратили 29 годин на локалізацію інциденту…

Ця стагнація пояснюється недосконалими методами навчання. Згідно з доповіддю, 60% навчання зосереджено на вразливостях, які існують вже понад два роки, через що команди не готові до сучасних загроз. Крім того, лише 41% організацій включають у свої симуляції нетехнічні ролі, такі як юридичні та комунікаційні, що означає, що важливі бізнес-рішення залишаються неперевіреними доти, доки не настане реальна криза.

Для поліпшення ситуації Immersive рекомендує організувати регулярні, комплексні тренінги з ротаційними сценаріями, безпосередньо залучаючи вище керівництво, а також розширити вправи, включивши в них функції, не пов'язані з IT. Компанія також наголошує на необхідності зосередитися на поточних загрозах і трирівневому підході «довести, поліпшити, повідомити». Як зазначив засновник, справжня стійкість вимагає впевненості, підкріпленої доказами, а не лише припущеннями, яку можна здобути, практикуючи правильні дії в умовах тиску…» ***(Phil Muncaster. Cyber Readiness Stalls Despite Confidence in Incident Response // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news/cyber-readiness-stalls-incident/). 17.11.2025).***

***

«…Швидке та добре структуроване повідомлення про порушення є основою сучасного реагування на інциденти. Після виявлення вторгнення кожна втрачена хвилина збільшує втрату даних, перебої в роботі бізнесу та юридичні ризики; швидке повідомлення запускає процес локалізації, зберігає криміналістичні докази та забезпечує дотримання нормативних термінів. Однак загрози — програми-вимагачі, APT, атаки на основі штучного інтелекту — стають дедалі більш витонченими, тому організації повинні поєднувати надійний захист периметра з досконалим, відпрацьованим протоколом повідомлення та реагування…

Комплексний звіт про порушення повинен містити хронологію виявлення, обсяг, точні часові мітки, вжиті заходи, індикатори компрометації та всі внутрішні та зовнішні комунікації. Ефективне реагування складається з шести дисциплінованих етапів: негайна ізоляція та оцінка; миттєве сповіщення міжфункціональної команди реагування на інциденти; ретельне документування; зовнішні повідомлення, що відповідають законодавству; криміналістичне розслідування; та постмортальний аналіз, що посилює контроль…

Добре підготовлені команди реагування на інциденти, підкріплені чіткими шляхами ескалації, регулярними навчальними вправами та культурою повідомлення про порушення без покарань, перетворюють хаотичні порушення на події, з яких можна винести уроки. Серед переваг — скорочення часу простою, збереження репутації, дотримання нормативних вимог, посилення захисту та розумніше розподілення ресурсів. Такі виклики, як складні гібридні IT-системи, вагання людей та закони різних юрисдикцій, можна пом'якшити за допомогою постійного навчання, актуальних інструкцій, уніфікованого ведення журналів та міцних зв'язків з юридичними та судовими експертами.

У майбутньому штучний інтелект, машинне навчання і навіть блокчейн покращать виявлення та цілісність доказів, але людський контроль залишається необхідним. Організації, які впроваджують обізнаність з питань безпеки,

відпрацьовують чіткі протоколи та повторюють їх після кожного інциденту, не тільки швидше локалізують майбутні порушення, але й формують стійку стійкість та довіру зацікавлених сторін…» ***(Shweta Dhole. Master how to report a breach for fast and effective cyber incident response // Techstrong Group Inc. (https://securityboulevard.com/2025/11/master-how-to-report-a-breach-for-fast-and-effective-cyber-incident-response/). 18.11.2025).***

***

«У сучасному світі, де кібератаки є неминучими, просто захищатися від них недостатньо. Організації повинні розвивати кіберстійкість — здатність готуватися до атак, протистояти їм, відновлюватися після них і адаптуватися до них, підтримуючи безперервність бізнес-процесів. На відміну від кібербезпеки, яка зосереджена переважно на запобіганні та захисті, кіберстійкість спрямована на вирішення більш широкого завдання — забезпечення безперервності роботи під час тривалих багатовекторних атак…

Практична основа для формування стійкості починається з аналізу впливу на бізнес (BIA) та оцінки ризиків для виявлення критично важливих послуг та взаємозалежностей. Далі проводиться аналітичне моделювання ймовірних векторів атак, що дозволяє організаціям вибірково посилювати механізми безпеки та розробляти цільові плани реагування та відновлення. На останньому етапі ці плани перевіряються за допомогою настільних вправ та кіберсимуляцій, в яких бере участь уся команда…

Щоб бути ефективною, кіберстійкість повинна бути інтегрована в існуючі IT- та безпекові процеси:

Управління ризиками починається з динамічної інвентаризації активів для визначення пріоритетності захисту критично важливих систем.

Тестування на проникнення та вправи «червоної команди» імітують атаки для перевірки функціональності системи після порушення.

Управління вразливостями визначає пріоритетність усунення вразливостей на основі бізнес-ризиків та впроваджує багаторівневі заходи захисту, такі як сегментація мережі та безпечне резервне копіювання.

Постійний моніторинг та реагування на інциденти узгоджуються з планами безперервності бізнесу, автоматизуючи дії, де це можливо, та проводячи аналіз після інциденту для вдосконалення.

Тестування та відновлення передбачають регулярні навчання для оцінки відмовостійкості та можливостей відновлення…

Платформи управління, ризиків та відповідності (GRC) є необхідними для централізації контролю ризиків, автоматизації управління інцидентами та забезпечення дотримання нормативних вимог. Зрештою, кіберстійкість є спільною відповідальністю бізнесу, що вимагає активної участі всіх підрозділів для визначення вимог до відновлення, розподілу ресурсів та участі в тестуванні безперебійності роботи. Поєднуючи захисні заходи кібербезпеки з цілісним підходом до стійкості — інтегруючи людей, процеси та технології — організації можуть не тільки зменшити ймовірність атак, але й мінімізувати їхній вплив, забезпечуючи стабільну роботу в умовах мінливого середовища загроз…» ***(Alex***

Vakulov. Building and Implementing Cyber Resilience Strategies // Communications of the ACM (https://cacm.acm.org/blogcacm/building-and-implementing-cyber-resilience-strategies/). 21.11.2025).

***

«Стрімкий розвиток додатків, хмарних сховищ, підключених пристроїв та віддаленої роботи випередив традиційні, ізольовані інструменти кібербезпеки. Зараз зловмисники автоматизують багаторівневі атаки, які використовують слабкі паролі, неправильні налаштування та застарілі системи швидше, ніж можуть зреагувати людські команди… Щоб відновити контроль, організації об'єднуються навколо нової моделі кіберстійкості, побудованої на семи тенденціях:

Уніфіковані платформи безпеки, наприклад, розширене виявлення та реагування (XDR), об'єднують кінцеві точки, мережу, ідентифікацію та хмарну телеметрію в одну консоль, зменшуючи кількість помилкових сповіщень та виявляючи шляхи атак від початку до кінця.

Автоматизація на основі штучного інтелекту сканує величезні масиви даних у режимі реального часу, позначає аномалії та може ізолювати пристрої або блокувати трафік за лічені секунди, даючи аналітикам час на розслідування.

Аналітика поведінки вивчає звичайні моделі поведінки користувачів і пристроїв, щоб виявляти раніше небачені загрози, такі як передача даних опівночі з облікового запису, який зазвичай працює з 9 до 17…

Архітектура Zero-Trust не передбачає жодної неявної довіри; кожен користувач, пристрій і робоче навантаження повинні постійно пройти аутентифікацію та бути мікросегментованими, що обмежує бічне переміщення у разі викрадення облікових даних.

Хмарна безпека супроводжує дані всюди, застосовуючи послідовні засоби контролю в SaaS, IaaS та віддалених кінцевих точках у безмежному робочому середовищі…

Інформація про загрози в режимі реального часу перетворює глобальні дані про шкідливе програмне забезпечення та зловмисників на автоматизовані списки блокування та пріоритети виправлень, допомагаючи організаціям запобігати атакам, а не просто реагувати на них.

Людський досвід залишається незамінним для прийняття рішень, розробки стратегій та творчого вирішення проблем; машини прискорюють виявлення та локалізацію загроз, але люди пов'язують технічні підказки з реальними ризиками…

Разом ці елементи формують сучасну, інтегровану систему захисту, здатну охоплювати всю цифрову інфраструктуру, виявляти сигнали раннього попередження та реагувати з машиною швидкістю, одночасно керуючи довгостроковим управлінням ризиками. Мета більше не полягає лише в блокуванні вторгнень, а в тому, щоб передбачати їх, протистояти їм і швидко відновлюватися після них, підтримуючи безперервність бізнесу та довіру в епоху все більш інтелектуальних загроз…» ***(The Future of Cyber Defense: Smarter Tools for a Smarter***

Threat Landscape // Talk Android (https://www.talkandroid.com/518366-the-future-of-cyber-defense-smarter-tools-for-a-smarter-threat-landscape/). 17.11.2025).

***

«Нове дослідження Microsoft «Кібербезпека 2025: виклики та стратегії в епоху штучного інтелекту для підприємств Пуерто-Рико» показує, що цифрові загрози зростають швидше, ніж захисні заходи більшості організацій. Серед 100 місцевих фахівців з безпеки та IT 74% стверджують, що за останні два-три роки кількість атак зросла, а 77% очікують, що кібербезпека залишиться головним пріоритетом. Проте лише 28% відчувають себе «дуже добре підготовленими», а участь керівництва обмежується трохи більше ніж половиною організацій, причому лише 34% описують поточні інвестиції як більш ніж помірні…

Традиційні загрози, такі як шкідливе програмне забезпечення та фішинг, як і раніше домінують, але увага все більше переходить на слабкі місця хмарних технологій (25%), несанкціоноване використання штучного інтелекту (23%) та дипфейки (14%). 62% компаній мають офіційну стратегію безпеки, а 90% стверджують, що безпека принаймні частково інтегрована в бізнес-планування, але підготовка зосереджена головним чином на контролі конфіденційності та реагуванні на інциденти.

Штучний інтелект швидко стає основою оборони: 60% компаній вже мають політику безпеки на основі ШІ, а 56% фахівців вважають, що ШІ суттєво змінить практику в найближчі кілька років. Microsoft виділяє «агентів» ШІ, які автоматизують розслідування загроз, координують реагування та забезпечують дотримання політик щодо ідентифікації та даних, особливо в поєднанні з системами Zero-Trust та широкою телеметрією…

Однак впровадження відбувається нерівномірно. Найбільший прогрес спостерігається у фінансовій сфері (44% на проміжному етапі впровадження ШІ), тоді як у сфері управління персоналом цей показник становить лише 35%, що свідчить про те, що розрізнене впровадження послаблює потенційні вигоди. Microsoft закликає компанії зробити кібербезпеку пріоритетним питанням для вищого керівництва, посилити цифрову гігієну, обмінюватися інформацією про загрози та навчати персонал, одночасно впроваджуючи інструменти ШІ в масштабах підприємства, щоб протистояти новим ризикам і підтримувати безперебійність бізнесу в умовах стрімкого розвитку кіберпростору Пуерто-Рико». ***(Survey shows cybersecurity rising as top priority in Puerto Rico // News is my Business (https://newsismybusiness.com/survey-shows-cybersecurity-rising-as-top-priority-in-puerto-rico/). 21.11.2025).***

***

«Кібербезпека та сталий розвиток більше не можуть розглядатися як окремі пріоритети, особливо для сектору відновлюваної енергетики, який не тільки забезпечує реалізацію амбіційних планів Великобританії щодо чистої енергії до 2030 року, але й становить високоцінну критичну національну інфраструктуру. Надійні цифрові засоби захисту є необхідними для захисту вітрових електростанцій, сонячних батарей, систем управління розумними

мережами та населення, проте традиційні заходи безпеки — постійне копіювання даних, безперервний моніторинг, розгалужені резервні сховища — споживають велику кількість енергії і можуть становити до 17 % вуглецевого сліду ІТ-інфраструктури. І навпаки, ігнорування кіберстійкості може спричинити екологічні катастрофи, як показали хакерська атака на каналізаційну систему Маручі в Австралії та майже вибух на нафтохімічному заводі в Саудівській Аравії…

Щоб примирити «двосічний меч», компанії повинні зробити безпеку «сталою за задумом» шляхом проведення ризик-орієнтованого аналізу своєї ІТ-інфраструктури:

• Визначте пріоритетність та дедуплікацію критичних даних; використовуйте диференціальні резервні копії та коротші періоди зберігання.

• Планувати резервне копіювання в години найменшого навантаження, коли електромережа працює в більш екологічному режимі.

• Застосовувати дисциплінована політику життєвого циклу даних, яка передбачає архівування або видалення невикористаної інформації.

• Впроваджувати екологічні ІТ-звички — вимикати пристрої, видаляти непотрібні файли та встановлювати оновлення програмного забезпечення, щоб продовжити термін експлуатації обладнання та зменшити площу атаки…

Ключове значення мають освіта, міжвідомча співпраця та показники вуглецевого сліду для кіберконтролю. Інтегруючи сталі практики в планування стійкості, компанії, що працюють у сфері відновлюваної енергетики, можуть скоротити викиди, зменшити витрати і при цьому відповідати підвищеним вимогам щодо загроз, опублікованим Національним центром кібербезпеки Великої Британії.

Коротко кажучи, екологічна відповідальність та кіберстійкість взаємодоповнюють одна одну: розумні заходи безпеки з меншим впливом на навколишнє середовище захищають планету та енергопостачання, забезпечуючи підприємствам, що працюють у сфері чистої енергії, конкурентну перевагу та довіру інвесторів у майбутньому, яке буде вимогливим з точки зору цифрових технологій та екології…» ***(Matthew Bancroft. Cyber security and the environment: can we make cyber security green? // Capgemini (https://www.capgemini.com/gb-en/insights/expert-perspectives/green-cybersecurity-sustainability/). 25.11.2025).***

***

«Кібербезпека залишається головним питанням у звіті Softcat «Business Tech Report 2024»: 47 % з 4000 опитаних клієнтів назвали безпеку даних своїм головним пріоритетом на наступний рік. На другому місці — впровадження штучного інтелекту (46 %), при цьому організації визнають необхідність стандартизованого, безпечного та економічно виправданого підходу, оскільки «агентний» штучний інтелект починає змінювати робочі процеси. Незважаючи на ажіотаж, компанії все ще вважають людей своїм найбільшим активом і хочуть надати співробітникам можливість творчо та стратегічно використовувати штучний інтелект…

Кінцеві пристрої та програмне забезпечення зберігають сильну привабливість (37 %), і більше половини тих, хто зосереджений на цифровому робочому просторі, заявляють, що їх першочерговою метою є отримання більшої вигоди від

інструментів, якими вони вже володіють. Управління, ризики та відповідність вимогам займають високе місце (36 %), оскільки компанії продовжують розвивати гібридні робочі середовища.

Що стосується інфраструктури, керівники модернізують мережі за допомогою моніторингу на основі штучного інтелекту, більш екологічних конструкцій та більшої «спостережності», прагнучи виявляти несправності до їхнього погіршення та скорочувати викиди відповідно до цілей сталого розвитку. Сталий розвиток, фактично, пронизує стратегію: 80 % вибрали б варіанти викупу або обміну старих технологій, а 75 % вже мають або створюють офіційні плани сталого розвитку…

Придбавши технології, клієнти найбільше цінують конкурентні ціни (83 %), високу якість обслуговування (77 %) та глибоку експертизу (68 %), але зараз відділи закупівель також враховують соціальні та екологічні фактори. Популярність керованих послуг зростає, особливо серед малих і середніх підприємств, причому помітне зростання спостерігається в галузі інструментів кібербезпеки, штучного інтелекту та управління пристроями.

Керівники державного сектору поділяють багато з цих побоювань: 65 % вважають пріоритетом технології для стимулювання інновацій, а 59 % називають головним джерелом занепокоєння контроль витрат…» ***(Alex Wright. Cybersecurity top priority for businesses, finds study // Mark Allen Group (https://www.commsbusiness.co.uk/content/news/cybersecurity-top-priority-for-businesses-finds-study). 24.11.2025).***

***

«У сучасній цифровій економіці сильна присутність в Інтернеті є необхідною для підприємств будь-якого розміру, але вона також наражає їх на широкий спектр загроз кібербезпеки. Ризики є подвійними і походять як з внутрішніх, так і з зовнішніх джерел. Внутрішньо, людські помилки, недостатнє навчання та недбалі практики, такі як неправильне поводження з даними або неправильна конфігурація хмарного сховища, є основними причинами порушень. Зовні підприємства стикаються зі складними загрозами, включаючи просунуті схеми фішингу, крадіжку паролів, експлойти «нульового дня» та атаки, такі як SQL-ін'єкції, перехоплення «людина посередині» та DDoS-перевантаження…

До цих існуючих небезпек додаються нові технології, які використовують кіберзлочинці. Штучний інтелект використовується для створення більш ефективних і адаптивних атак, а майбутнє поява квантових обчислень загрожує порушити існуючі стандарти шифрування. Крім того, поширення фейкових відео та пристроїв Інтернету речей розширює площу атаки, що робить підроблені особисті дані та вразливість підключених пристроїв серйозною проблемою.

З огляду на те, що фінансовий збиток і шкода репутації від порушення безпеки часто набагато перевищують витрати на запобігання, підприємства не можуть дозволити собі пасивний підхід. Необхідна проактивна і комплексна стратегія, що включає надійні заходи безпеки, постійне навчання співробітників і стратегічні інвестиції в засоби захисту для захисту як корпоративних даних, так і даних клієнтів в умовах постійно мінливого середовища загроз…» ***(Nathan Spears. The cybersecurity threats business owners need to include in their 2026 forecasts // Canary***

Media Ltd (https://www.thecanary.co/discovery/tech/2025/11/24/the-cybersecurity-threats-business-owners-need-to-include-in-their-2026-forecasts/). 24.11.2025).

***

«Фахівці з кібербезпеки ведуть війну на два фронти: один проти невпинних зловмисників, а інший проти культури робочого середовища, яка прославляє цілодобову пильність, нестачу персоналу та мовчання про стрес. Дослідження показують зростання «кібервтоми»: постійні сповіщення, етичний тиск, нестача ресурсів та швидкі зміни в законодавстві призводять до хронічної тривоги, безсоння, депресії та навіть посттравматичного стресового розладу у аналітиків та керівників служб інформаційної безпеки. Вигорання підриває процес прийняття рішень, сприяє плинності кадрів і, зрештою, послаблює безпеку організації…

Основні фактори стресу

• Постійна пильність: пейджери для повідомлення про інциденти та дзвінки о 2 годині ночі тримають нервову систему в напрузі.

• Моральна та оперативна відповідальність: одна пропущена латка може коштувати мільйони та репутацію.

• Ізоляція та недооцінка: команди з безпеки або невидимі, або звинувачуються після порушень.

• Перевантаження функціями: скорочення бюджету змушує одну людину поєднувати моніторинг SOC, звітування перед правлінням, IAM та дотримання вимог.

• Культура досконалості: міфи про «нульові порушення» заважають говорити про перевантаження…

Наслідки

• Погіршення психічного здоров'я — панічні атаки, депресія, синдром самозванця.

• Висока плинність кадрів — втрата знань і слабкі захисні механізми.

• Стратегічний ризик — втомлені команди не помічають загроз, надмірно ускладнюють контроль, породжують тіньові IT-системи…

Виправлення повинні здійснюватися на трьох рівнях.

Індивідуальний

• Встановіть чіткі межі між робочим та неробочим часом.

• Зверніться за допомогою до терапевта, коуча, груп підтримки на ранній стадії.

• Слідкуйте за своїм календарем; не все є терміновим.

Організаційний

• Створіть психологічну безпеку, щоб співробітники могли без страху повідомляти про перевантаження.

• Визначте ролі та забезпечте їх ресурсами; відокремте стратегію від щоденного гасіння пожеж.

• Відстежуйте показники вигорання разом із ключовими показниками ефективності безпеки.

Промисловість

• Покласти край міфу про «героїв», який виправдовує виснаження.

• Включити вимоги щодо психічного здоров'я в такі стандарти, як ISO та NIST.

• Фінансувати дослідження та інструментарій для навчання лідерів та підвищення стійкості команд…

Вигорання є порушенням людських систем; обидва явища сигналізують про те, що щось не працює. Щоб забезпечити безпеку цифрових фортець, підприємства повинні насамперед захищати людей, які працюють за екранами». ***(Maman Ibrahim. Invisible battles: How cybersecurity work erodes mental health in silence and what we can do about it // FoundryCo, Inc. (https://www.csoonline.com/article/4094657/invisible-battles-how-cybersecurity-work-erodes-mental-health-in-silence-and-what-we-can-do-about-it.html). 24.11.2025).***

***

«Кібер-вигорання зростає, оскільки недоукомплектовані команди з безпеки стикаються з безперервними загрозами, що мають велике значення. Аналітики працюють довгими, нерегулярними годинами, переглядають тисячі сповіщень і знають, що одна помилка може коштувати мільйони і зруйнувати довіру. Світова нестача талантів залишає мільйони вакансій у сфері кібербезпеки незаповненими, що призводить до хронічної виснаженості, тривоги та зниження продуктивності праці решти персоналу…

Виснажені захисники повільніше виявляють інциденти, роблять більше помилок і частіше звільняються, що послаблює всю організацію та збільшує ризик порушення безпеки і витрати на плинність кадрів…

Керівництво повинно вжити таких заходів:

• Наймати та підвищувати кваліфікацію персоналу для полегшення робочого навантаження; впроваджувати штучний інтелект/автоматизацію для зменшення кількості помилкових тривог.

• Ввести обмеження на чергування, обов'язкову ротацію та реальний відпочинок.

• Забезпечити підтримку психічного здоров'я та відкриті канали комунікації.

• Підтримувати чіткі інструкції щодо реагування на інциденти та проводити постійне навчання.

• Створити культуру, в якій кожен відділ несе спільну відповідальність за безпеку…

Захист людей, які працюють за екранами, зараз є настільки ж важливим, як і будь-який технічний контроль; це необхідно для підтримки стійкості організації в епоху безперервних кібератак». ***(Naveen Goud. What Is a Cyber Burnout Crisis? Understanding the Growing Threat to Cybersecurity Teams // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/what-is-a-cyber-burnout-crisis-understanding-the-growing-threat-to-cybersecurity-teams/). 11.2025).***

***

«До 2026 року більшість організацій працюватимуть на основі робочих процесів, що підтримуються штучним інтелектом, архітектур, орієнтованих на

хмарні технології, та широко розподілених команд, проте вирішальним фактором як у випадках інцидентів кібербезпеки, так і в проектах цифрової трансформації залишається поведінка людей. Коли відбувається порушення, першою причиною невдачі рідко є технічні проблеми, а емоційна плутанина. Клієнтам і колегам потрібна проста мова, чіткість наступних кроків і видиме лідерство, перш ніж їм знадобиться захоплення пакетів. Команди, які відпрацювали комунікаційні вправи та розподіл ролей, реагують із стійкістю, яку не може забезпечити сама технологія…

Та сама людська динаміка керує цифровою трансформацією. Впровадження штучного інтелекту та автоматизації є успішним лише тоді, коли зміни впроваджуються поступово, тестуються та супроводжуються зворотним зв'язком, що враховує можливості персоналу та реалії робочого процесу. Поспішне впровадження інструменту без підготовки персоналу просто переносить неефективність на нижчі рівні…

Отже, інциденти та трансформація мають спільну основу: чітка, чесна комунікація, поетапне планування та усвідомлення того, що не кожне впровадження — або заходи з обмеження поширення — будуть бездоганними. Технології повинні прискорювати прийняття рішень людьми, а не замінювати їх; штучний інтелект може сортувати сповіщення або автоматизувати завдання, але він не може проявити емпатію або відновити довіру.

Лідери, які поєднують технічну компетентність з емоційним інтелектом — спокійні, прозорі, орієнтовані на вирішення проблем — визначатимуть стійкість у 2026 році. Вони усвідомлюватимуть, що навіть попри зростання потужності інструментарію, сила організації все ще базується на комунікації, чіткості ролей та здатності утримувати людей у стабільному стані, коли ставки найвищі…» ***(IT's human side of cyber incidents and digital transformation // TechDay (https://itbrief.co.uk/story/it-s-human-side-of-cyber-incidents-and-digital-transformation). 22.11.2025).***

***

«Два нещодавні випадки порушення безпеки в компаніях M&S (збитки у розмірі 300 млн фунтів стерлінгів) та Co-op (206 млн фунтів стерлінгів) показують, що кіберризик залежить не тільки від технологій, а й від поведінки співробітників. Традиційні курси з підвищення обізнаності, що базуються на «відмітках у списку», не дають результату, оскільки спираються на факти та статистику, що змушує співробітників перебувати в режимі «аналізу та мислення». Справжні зміни відбуваються завдяки моделі Коттера «бачити-відчувати-змінюватися»: занурюйте людей у реалістичні сценарії з високим тиском, які викликають емоційну реакцію та формують інстинктивні звички…

Ключові кроки для керівників служб безпеки та команд з навчання та розвитку:

• Замініть презентації на практичні вправи, що імітують складні атаки соціального інжинірингу — авторитет, терміновість, точне брендування, розлючені дзвінки, реалістичні рахунки-фактури.

• Адаптуйте вправи до кожної ролі (наприклад, співробітники служби підтримки повинні перевіряти особу дзвонячого). Оцінюйте успішність за поведінкою: зупинка, перевірка, ескалація — а також швидкість і якість звітів…

• Створіть відчуття терміновості, запросивши керівників компаній, що зазнали зломів, описати емоційний вплив; відвідування об'єктів допоможе співробітникам «побачити» і «відчути» наслідки.

• Впроваджуйте культуру, що ставить безпеку на перше місце, з самого початку роботи; визнавайте та винагороджуйте правильні реакції як короткострокові перемоги.

• Подолайте ізольованість: співпрацюйте з ІТ-відділом для технічного контролю, з керівниками бізнесу для забезпечення відповідності конкретним ролям, а також залучайте «чемпіонів безпеки» для навчання колег та підтримки зворотного зв'язку…

Кіберстійкість — це програма постійних змін. У міру розвитку загроз навчання має постійно адаптуватися, щоб співробітники діяли інстинктивно та спільно для захисту активів організації». ***(Nick Petschek. Why your compliance training won't stop the next cyber-attack // HR Zone Ltd (https://trainingzone.co.uk/why-your-compliance-training-wont-stop-the-next-cyber-attack/). 19.11.2025).***

***

«Звіт SANS Institute про кібербезпеку ICS/OT за 2025 рік показує, що промислові системи швидше виявляють і локалізують кіберінциденти — майже половина з них протягом 24 годин і 60% протягом 48 годин — але усунення наслідків все ще затягується: 22% атак вимагають від двох до семи днів для відновлення, 19% — більше місяця, а 3% — більше року. Минулого року кожна п'ята організація зазнала кіберінциденту; 40% з них призвели до порушення роботи. Половина з них була спричинена несанкціонованим віддаленим доступом, проте лише 13% об'єктів повністю впровадили сучасні засоби контролю (запис сеансів, доступ з урахуванням ICS)…

Розриви в рівні готовності є значними: лише 14% респондентів відчувають себе готовими до нових загроз, але рівень готовності зростає в 1,7 раза, коли технічні фахівці, що працюють на передовій, беруть участь у навчаннях. Пріоритетами інвестицій на 2026–2027 роки є видимість активів, виявлення загроз, безпечний віддалений доступ та сегментація. Організації, що мають центри оперативного реагування (SOC) або підлягають регуляторному нагляду, демонструють вищий рівень зрілості та витрачають більше коштів на ці заходи контролю…

Плани реагування на інциденти існують у 57% компаній (70% у регульованих галузях), а щоквартальне тестування планів стає все більш поширеним. Використання інформації про загрози становить 67%, переважно це дані від постачальників та ISAC. Регулювання посилюється: 58% компаній мають об'єкти, що підпадають під обов'язкові кіберправила, а 26% з них стикалися з можливими порушеннями під час аудиту.

Незважаючи на покращення виявлення, передові практики — пошук загроз, об'єднання червоної/фіолетової команд, тести на проникнення з урахуванням безпеки — залишаються обмеженими. Лише 31 % підтримують централізований

інвентар точок віддаленого доступу ОТ; брак ресурсів та обмеження застарілих систем перешкоджають впровадженню безпечного доступу…

Ключові рекомендації: розширити охоплення та сегментацію, що стосуються операційних технологій, перенести акцент з виявлення на стійке відновлення (надійні резервні копії, відмовостійкість), залучити інженерів та керівників до навчань, розглядати відповідність вимогам як мінімальний рівень та надавати пріоритет інвестиціям у безпеку віддаленого доступу, видимість активів та інтеграцію інформації про загрози, щоб усунути прогалини моделі Пердью, перш ніж ними скористаються зловмисники». ***(Anna Ribeiro. SANS Institute 2025 survey finds OT cybersecurity incidents rising as ransomware and remote access risks grow // Industrial Cyber (https://industrialcyber.co/news/sans-institute-2025-survey-finds-ot-cybersecurity-incidents-rising-as-ransomware-and-remote-access-risks-grow/). 20.11.2025).***

***

«…Оскільки штучний інтелект продовжує розвиватися експоненціальними темпами, організаціям доводиться адаптуватися до нових способів роботи – і захищатися від дедалі складніших кібератак.

Згідно з щорічним дослідженням Beazley Risk & Resilience, в якому взяли участь 3500 світових бізнес-лідерів, стурбованість щодо кіберризиків зросла – 29% респондентів опитування назвали цей ризик своєю найбільшою загрозою, порівняно з 26% у 2024 році. Однак, хоча обізнаність про кіберризики зростає, як не парадоксально, керівники почувалися більш підготовленими до розвитку кіберзагроз, а сприйняття стійкості зросло з 75% у 2024 році до 83% цього року.

Ця суперечність недооцінює сучасний ландшафт кібер- та технологічних загроз, який стає дедалі динамічнішим та непередбачуванішим, що тривожно чітко продемонстрували нещодавні гучні атаки програм-вимагачів на великих роздрібних торговців та інші підприємства. Невизнання цієї реальності робить бізнеси беззахисними, непідготовленими та дедалі більш вразливими до сучасних швидкозмінних цифрових загроз…» ***(Emily Douglas. The hidden cost of a hack: Unpacking the ripple effect of cybercrime // KM Business Information US, Inc (https://www.insurancebusinessmag.com/us/news/cyber/the-hidden-cost-of-a-hack-unpacking-the-ripple-effect-of-cybercrime-557023.aspx). 18.11.2025).***

***

«Опитування BlueVoyant «Стан захисту ланцюгів поставок» за 2025 рік показує, що програми управління ризиками третіх сторін (TPRM) досягли зрілості на папері, але все ще не здатні знизити реальні ризики. Основні висновки, отримані від понад 300 глобальних компаній:

• Епідемія порушень – 97 % зазнали принаймні одного кіберінциденту, пов'язаного з постачальниками, протягом останнього року (у порівнянні з 81 % у 2024 році), хоча 46 % описують свої програми TPRM як «впроваджені та оптимізовані».

• Зрілість без сили – лише 24 % щомісяця інформують керівництво, а 60 % називають внутрішній опір, ізольованість команд та слабку підтримку з боку

керівництва головними перешкодами; майже половина програм не входить до сфери відповідальності служби безпеки…

• Дотримання вимог безпеки – Лише 16 % використовують TPRM переважно для зменшення ризиків; більшість робить це для виконання вимог кіберстрахування, контрактів або правління. Як наслідок, 96 % планують додати постачальників, а половина вважає до 50 % постачальників «критичними», що розмиває фокус.

• Інвестиції без інтеграції – бюджети зростають (95 % очікують зростання), але відсутність інтеграції з інструментами GRC/підприємницького ризику є головним викликом, що призводить до фрагментованої видимості та повільної реакції на інциденти…

Позитивні моменти: 45 % зараз працюють безпосередньо з постачальниками над виправленням ситуації; 36 % перенесли відповідальність за TPRM на кібер/IT-команди; сектори оборони, енергетики та комунальних послуг демонструють кращу узгодженість та нижчі показники порушень. Постійний моніторинг на основі штучного інтелекту вважається необхідним, але сама по собі технологія не вирішить проблему неузгодженості в організації…

Рекомендації: забезпечити підтримку керівництва шляхом регулярного звітування; інтегрувати дані TPRM у платформи управління ризиками підприємства; запровадити класифікацію за рівнем ризику (на основі доступу до даних та впливу на операційні технології, а не вартості контракту); розглядати управління постачальниками як спільну стійкість, а не як перевірку відповідності вимогам. ***(Anna Ribeiro. BlueVoyant's supply chain defense report finds TPRM programs growing, despite rising breaches // Industrial Cyber (https://industrialcyber.co/supply-chain-security/bluevoyants-supply-chain-defense-report-finds-tprm-programs-growing-despite-rising-breaches/). 24.11.2025).***

***

Сполучені Штати Америки та Канада

«…Аудит, проведений Офісом генерального інспектора Федеральної резервної системи (OIG), виявив, що триваюче скорочення штату Бюро захисту прав споживачів у фінансовій сфері (CFPB) за адміністрації Трампа призвело до неефективності загальної програми інформаційної безпеки агентства. Рівень зрілості програми безпеки CFPB значно знизився з «керованого та вимірюваного» (рівень 4) до рівня 2 у 2025 фінансовому році, головним чином через масовий відтік персоналу та втрату підтримки підрядників для постійного моніторингу. OIG виявило, що агентство не встигає оновлювати авторизації для багатьох систем і використовує «меморандуми про прийняття ризиків без задокументованого аналізу ризиків кібербезпеки»…

Незважаючи на ці серйозні обмеження, співробітники CFPB, що залишилися, отримали високу оцінку за вжиття позитивних заходів, зокрема за формалізацію протоколів реагування на інциденти з програмним забезпеченням-вимагачем та проведення щотижневих нарад з управління ризиками. Однак агентство продовжує боротися зі старими IT-системами, що працюють на застарілому програмному

забезпеченні, яке більше не отримує оновлень безпеки, що є основною причиною погіршення ситуації. OIG утрималося від винесення нової рекомендації з цього питання, запропонувавши керівництву надати пріоритет заходам щодо зменшення ризиків, пов'язаних із застарілим програмним забезпеченням. Аудит з'явився через кілька тижнів після того, як Рассел Воут, виконуючий обов'язки директора CFPB та директора Управління з питань управління та бюджету, публічно оголосив про плани закрити агентство протягом декількох місяців після періоду, що характеризувався масовими скороченнями персоналу та припиненням роботи з захисту прав споживачів…» ***(Matt Bracken. CFPB's cybersecurity program 'not effective' after staff cuts, watchdog says // Scoop News Group (https://fedscoop.com/cfpb-cybersecurity-struggles-watchdog-audit/). 04.11.2025).***

***

«Американські законодавці, сенатор Рон Вайден і представник Раджа Крішнамурті, закликали Федеральну торгову комісію (FTC) провести розслідування щодо компанії Flock Safety, яка управляє однією з найбільших мереж камер для сканування номерних знаків у США, за нібито невиконання вимог щодо забезпечення необхідних заходів кібербезпеки. Законодавці конкретно посилаються на те, що Flock не вимагає багатофакторної автентифікації (MFA) для своїх клієнтів з правоохоронних органів, що є вразливістю, яка наражає її величезну базу даних з мільярдами фотографій номерних знаків американців на хакерів та іноземних шпигунів, які отримують доступ до паролів користувачів…

Законодавці надали докази від компанії з кібербезпеки Hudson Rock та незалежного дослідника Бенна Джордана, які свідчать про те, що деякі облікові дані правоохоронних органів для веб-сайту Flock вже були викрадені та поширені або продані на російських форумах кіберзлочинців. Компанія Flock, яка обслуговує понад 5000 поліцейських відділків, відповіла на запит, заявивши, що з листопада 2024 року вона зробила MFA стандартною функцією для всіх нових клієнтів, і що 97% існуючих клієнтів з правоохоронних органів увімкнули цю функцію. Однак це залишає значний відсоток клієнтів — потенційно десятки агентств — які відмовилися від MFA з «власних причин», що, на думку законодавців, є прогалиною в безпеці, яку FTC повинна усунути для захисту національної безпеки та публічних даних…» ***(Zack Whittaker. Lawmakers say stolen police logins are exposing Flock surveillance cameras to hackers // TechCrunch Media LLC (https://techcrunch.com/2025/11/03/lawmakers-say-stolen-police-logins-are-exposing-flock-surveillance-cameras-to-hackers/). 03.11.2025).***

***

«Уряд США намагається стримати наслідки серйозного порушення безпеки постачальника програмного забезпечення F5, яке, як широко вважається, було ініційоване Китаєм, оскільки відпустки та нестача персоналу серйозно перешкоджають зусиллям федеральних органів влади. Порушення, підтверджене Агентством з кібербезпеки та безпеки інфраструктури (CISA) в екстреній директиві, призвело до того, що державний суб'єкт викрав конфіденційні

файли, включаючи вихідний код BIG-IP та деталі нерозкритих вразливостей, які можуть бути використані для створення спеціальних експлойтів…

Федеральні агентства намагаються знайти та виправити вразливі системи, але нинішні та колишні чиновники повідомляють, що закриття уряду сповільнило роботи з усунення недоліків на кілька днів, що перевищує стандартні терміни реагування на інциденти. Мережеві інженери, які перебувають у відпустці, за законом не можуть виконувати аварійні роботи, що залишає CISA, яка працює з сильно скороченим штатом і не має затвердженого Сенатом директора, нездатною надати рівень підтримки, який очікується під час серйозного кіберінциденту…

Вразливості F5, виявлені Unit 42, підвищують ризик підвищення привілеїв та несанкціонованого доступу до пристроїв F5, які широко використовуються у федеральних мережах та мережах критичної інфраструктури. Незважаючи на те, що виконавчий заступник директора CISA Нік Андерсен заявляє, що агентство залишається «повністю відданим своїй справі», а його співробітники працюють без оплати, агентство серйозно постраждало від постійного політичного тиску та скорочення штату, що змусило багатьох співробітників шукати роботу в приватному секторі. Зрештою, відсутність повної оперативної спроможності через закриття ускладнює реагування на те, що описується як серйозна кіберподія, залишаючи федеральні мережі вразливими до потенційного повного компрометації». ***(Chris Riotta. 'It's Been a Mess': Shutdown Slows Federal F5 Hack Response // Information Security Media Group, Corp. (https://www.databreachtoday.com/its-been-mess-shutdown-slows-federal-f5-hack-response-a-29930). 04.11.2025).***

***

«Опитування NordVPN, в якому взяли участь 1000 дорослих американців (віком 18–74 роки), виявило поширену плутанину щодо того, що роблять засоби кібербезпеки, зокрема антивіруси, незважаючи на те, що 52% опитаних використовують антивіруси щодня. Понад чверть опитаних помилково вважають, що антивірус «повністю» захищає їх в Інтернеті, а багато хто плутає антивірус із захистом від крадіжки особистих даних, блокуванням реклами/трекерів, менеджерами паролів, брандмауерами та VPN. Технічний директор NordVPN попередив, що переоцінка можливостей одного інструменту підвищує ризик крадіжки особистих даних та інших загроз, що свідчить про загальний брак знань у сфері кібербезпеки… Проблему ускладнює те, що більше третини респондентів взагалі не використовують програмне забезпечення для забезпечення безпеки, хоча приблизно половина з них повідомили, що їхні особисті дані були викрадені в результаті зломів. Хоча багато хто покладається на «найкращі практики» (уникання підозрілих посилань, використання надійних паролів), сучасні загрози, такі як безклікове шкідливе програмне забезпечення та складні фішинг/смішинг-кампанії, означають, що одних лише гігієнічних заходів недостатньо. Більшість витоків даних стосується електронних листів, телефонних номерів та фізичних адрес, які часто вважаються низькоризиковими, але вони є основним джерелом для цілеспрямованих шахрайств, що можуть призвести до компрометації надзвичайно конфіденційних ідентифікаторів та фінансових рахунків…

Експерти рекомендують багаторівневий підхід: поєднати надійний антивірус із безпечною VPN для шифрування трафіку та маскування IP-адрес (особливо в публічних мережах Wi-Fi), увімкнути багатофакторну автентифікацію для запобігання захопленню облікових записів та використовувати надійні унікальні паролі для кожного облікового запису. Не менш важливою є постійна пильність — обмеження інформації, яку ви ділитеся в Інтернеті, та скептичне ставлення до небажаних електронних листів, текстових повідомлень і дзвінків. Основне повідомлення: антивірус — це хороший початок, але не панацея. Ефективний захист вимагає поєднання декількох інструментів, дотримання надійних цифрових звичок та підвищення обізнаності користувачів про те, що може, а що не може зробити кожна технологія». ***(Kristin Hassel. 70% of Americans think antivirus will protect their online privacy – here's the real truth // Future US, Inc. (https://www.tomsguide.com/computing/online-security/70-percent-of-americans-think-antivirus-will-protect-their-online-privacy-heres-the-real-truth). 03.11.2025).***

***

«Університет Пенсильванії, який потрапив у поле зору Вашингтона через свої зв'язки з відомими випускниками Ілоном Маском і Дональдом Трампом, тепер зазнав політично забарвленої кібератаки. Після того, як федеральний уряд скоротив гранти на дослідження, погрожував розслідуваннями та намагався (без успіху) зобов'язати Пенсильванію дотримуватися незвичайної угоди, що обмежує свободу слова, 31 жовтня невідомий хакер скористався соціальною інженерією, щоб зламати кілька систем Пенсильванії, включаючи Salesforce, SharePoint, Box та кілька маркетингових додатків. Зловмисник викрав надзвичайно конфіденційну базу даних донорів університету, що містила банківські квитанції, особисті ідентифікатори та внутрішні меморандуми, і почав викласти її частину на LeakForums…

В електронному листі під назвою «Нас зламали (необхідні дії)» зловмисник звинуватив Пенсильванський університет у «елітарності» та «політичній коректності», які сприяють наданню переваги спадкоємцям, донорам та особам, прийнятим за програмою позитивної дискримінації. Пізніше в інтерв'ю BleepingComputer хакер заявив, що справжньою мотивацією було просто пограбування «величезного, надзвичайно багатого» списку донорів Пенсильванського університету, хоча його риторика повторювала скарги, які часто висловлювали Трамп і Маск. Цей випадок є продовженням аналогічного політично зарядженого порушення в Колумбійському університеті на початку цього року, що підкреслює, як хактивізм і можливе втручання національних держав збігаються на кампусах США.

Пенн залучив до розслідування ФБР та компанію з кібербезпеки CrowdStrike, а також стикається з принаймні одним позовом про недбалість від випускника. Викладачам та співробітникам було повідомлено, що вони повинні пройти обов'язкове навчання з питань безпеки, щоб запобігти майбутнім атакам соціального інжинірингу…» ***(Nate Anderson. Musk and Trump both went to Penn—now hacked by someone sympathetic to their cause // Condé Nast***

(https://arstechnica.com/security/2025/11/musk-and-trump-both-went-to-penn-now-hacked-by-someone-sympathetic-to-their-cause/). 06.11.2025).

***

«…Світ кіберзлочинності 2025 року зазнав кардинальних змін під впливом штучного інтелекту: на зрілому підпільному ринку тепер пропонуються потужні шкідливі інструменти ШІ, які знизили бар'єр для входу злочинців. За даними Threat Intelligence Group від Google, ця екосистема зазнала вибухового зростання, а такі платформи, як WormGPT, FraudGPT та більш просунуті Xanthorox і NYTHEON AI, продаються як послуги за передплатою. Ці інструменти призначені для автоматизації таких завдань, як створення надзвичайно переконливих фішингових електронних листів, написання шкідливого коду, виявлення вразливостей і навіть створення дипфейків…

Основним застосуванням цих інструментів є фішинг, який, за документальними даними, зріс на 1265% завдяки контенту, створеному штучним інтелектом, який є настільки ж ефективним, як і створені людьми приманки. Окрім фішингу, ці платформи дозволяють створювати поліморфне шкідливе програмне забезпечення, яке постійно змінюється, щоб уникнути виявлення антивірусом. Цей стрибок підживлюється бізнес-моделлю, яка віддзеркалює легальне програмне забезпечення як послугу, з багаторівневими підписками та низькими вхідними витратами, що демократизує складні кіберзлочини для менш кваліфікованих учасників. Оскільки фішинг, що підтримується штучним інтелектом, вже становить понад 80% спостережуваної соціальної інженерії, агентства з безпеки попереджають, що швидкість, масштаб і складність цих атак будуть продовжувати зростати, що кардинально змінить виклики кібербезпеки в найближчому майбутньому…» ***(Guru Baran. List of AI Tools Promoted by Threat Actors in Underground Forums and Their Capabilities // Cyber Security News (https://cybersecuritynews.com/ai-tools-promoted-by-threat-actors/). 06.11.2025).***

***

«…Нова сертифікація моделі зрілості кібербезпеки 2.0 (CMMC) Пентагону починає діяти з 10 листопада і зрештою змусить понад 300 000 американських підрядників у сфері оборони довести, що вони відповідають багаторівневим стандартам безпеки, а не просто самостійно підтверджувати це. Однак опитування в галузі показують, що понад половина ланцюга поставок все ще не готова. Протягом багатьох років підрядники могли самостійно оцінювати свою відповідність вимогам NIST 800-171, вперше введеним у 2016 році; CMMC, представлена у 2021 році, додає аудити з боку третіх сторін або уряду, які залежать від ступеня конфіденційності даних, з якими працює компанія…

Ця загроза ретельного контролю викликала хвилю активності інформаторів. Співробітники служб кібербезпеки, які виявляють прогалини, відмовляються підписувати оптимістичні оцінки або просять виділити бюджет, необхідний для усунення слабких місць, все частіше повідомляють про репресії — маргіналізацію, пониження в посаді, навіть звільнення. Недавні угоди з компаніями Raytheon та Aerojet Rocketdyne, укладені на підставі Закону про неправдиві заяви, показують, що

Міністерство юстиції готове вживати заходів у таких випадках, а Закон про захист інформаторів-підрядників у сфері оборони, Закон про неправдиві заяви, Закон Сарбейнса-Окслі та кілька жорстких законів штатів захищають співробітників, які викривають порушення…

Компанії можуть розглядати витрати на CMMC — нові інструменти, навчання та архітектуру — як удар по маржі, але покарання внутрішніх критиків створює юридичні ризики і, що ще важливіше, робить дані національної безпеки вразливими. Тому успішна реалізація CMMC 2.0 залежить не тільки від технічних засобів контролю, але й від формування культури, в якій фахівці з кібербезпеки можуть висловлюватися без побоювання репресій». ***(Matthew LaGarde. Defense Contractors Are Silencing Their Cybersecurity Watchdogs // Bloomberg Industry Group, Inc. (https://news.bloomberglaw.com/privacy-and-data-security/defense-contractors-are-silencing-their-cybersecurity-watchdogs). 07.11.2025).***

***

«…8 серпня 2025 року було представлено двопартійний законопроект Палати представників — Закон про готовність та стійкість до квантового шифрування — з метою посилення кіберзахисту США до того, як квантові комп'ютери зможуть зламати сучасне шифрування… На основі Закону про готовність до кібербезпеки квантових обчислень 2022 року, цей захід покладає на Підкомітет з економічних та безпекових наслідків квантової інформатики три завдання: (1) розробити критерії для виявлення «криптографічно релевантного» квантового комп'ютера (такого, що здатний зламати алгоритми, які не під силу класичним машинам); (2) протягом року, а потім щорічно протягом чотирьох років, подавати звіт, в якому порівнюються досягнення США з досягненнями країн-конкурентів як у розробці квантових комп'ютерів, так і у впровадженні постквантової криптографії, з одночасним виділенням економічних секторів, які піддаються найбільшому ризику; та (3) розробити національний план заходів щодо зменшення ризиків, який сприятиме обміну інформацією між державним і приватним секторами та визначатиме конкретні кроки, які уряд і промисловість повинні вжити для впровадження постквантових заходів безпеки… Законодавці посилаються на попередження GAO та NIST про те, що такі машини для розшифрування кодів можуть з'явитися протягом 10–20 років, тому для захисту конфіденційних даних та національної безпеки необхідно завчасно підготуватися». ***(Courtney Otto. House Bill Introduced to Shield the U.S. From Cybersecurity Risks Posed by Quantum Computing // Perkins Coie LLP (https://perkinscoie.com/insights/blog/house-bill-introduced-shield-us-cybersecurity-risks-posed-quantum-computing). 07.11.2025).***

***

«Федеральна комісія з питань зв'язку (FCC) на чолі з головою Бренданом Карром проголосувала за скасування правил кібербезпеки епохи Байдена, які були встановлені у відповідь на вторгнення китайських хакерів у мережу «Salt Typhoon». Скасовані правила, які ґрунтувалися на повноваженнях Закону про допомогу в комунікаціях для правоохоронних органів (CALEA) 1994 року, раніше

вимагали від великих телекомунікаційних операторів, таких як AT&T і Verizon, забезпечити безпеку своїх мереж і щорічно подавати сертифікати своїх планів з кібербезпеки…

Карр стверджував, що початкові заходи були поспішним і неефективним застосуванням CALEA, яка спочатку була розроблена для прослуховування телефонних розмов, а не для кіберзахисту, і виступав за спільний підхід з приватним сектором, а не за вертикальні розпорядження. Однак цей крок зазнав різкої критики з боку демократів, зокрема сенаторки Марії Кантвелл і комісарки Анни Гомес, які попередили, що скасування цих заходів захисту без надання негайної заміни залишає критичну інфраструктуру країни в небезпеці перед майбутнім шпигунством і саботажем…» ***(Kelcee Griffis. FCC Rescinds Biden-Era Cyber Rule Meant to Address Salt Typhoon // Bloomberg L.P. (https://www.bloomberg.com/news/articles/2025-11-20/fcc-rescinds-biden-era-cyber-rule-meant-to-address-salt-typhoon). 20.11.2025).***

***

«На кіберсаміті в Аспені національний кібердиректор Шон Кернкросс окреслив майбутню стратегію адміністрації Трампа в галузі кібербезпеки, наголосивши на єдиному підході, спрямованому на протидію іноземним супротивникам та зменшення регуляторного навантаження. Кернкросс заявив, що нова стратегія включатиме план дій із шести основних напрямків, у якому особлива увага приділятиметься заходам щодо накладення реальних витрат на таких суб'єктів, як Росія, Китай та угруповання, що займаються викраденням даних з метою вимагання викупу, з метою стримування ескалації агресії — це перехід від простої реакції на атаки до усунення першопричин зловмисної поведінки…

Крім того, адміністрація прагне тісно співпрацювати з приватним сектором з метою виявлення та усунення непотрібних нормативних вимог, тим самим звільняючи ресурси для захисту критично важливих активів. Іншим ключовим напрямком є розширення кадрового потенціалу в сфері кібербезпеки за допомогою нової ініціативи, яка об'єднує підприємства, навчальні заклади та інвесторів, включаючи створення «академії» кібербезпеки для сприяння навчанню та розвитку культури. Хоча ці пріоритети — стримування, співпраця з приватним сектором та розвиток кадрового потенціалу — перегукуються з темами адміністрації Байдена, конкретні заходи плану Трампа ще не були детально опрацьовані…» ***(Eric Geller. Trump's cyber strategy will emphasize adversary deterrence, industry partnerships // TechTarget, Inc. (https://www.cybersecuritydive.com/news/trump-administration-national-cyber-strategy-preview-sean-cairncross-aspen/805782/). 18.11.2025).***

***

«На тлі ескалації геополітичної напруженості та складних кіберзагроз Канада прийняла Закон про захист критичних кіберсистем Канади (CCSPA) як ключовий компонент законопроекту C-26, спрямованого на зміцнення критичної інфраструктури країни. Цей закон, спрямований на такі важливі сектори, як телекомунікації, фінанси, енергетика, транспорт та державні системи, перетворює кібербезпеку з добровільної практики на обов'язкову нормативну базу. Закон спрямований на захист національних служб від збій у роботі, спричинених

програмним забезпеченням-вимагачем, порушеннями ланцюга поставок та атаками, що фінансуються державою, шляхом впровадження надійних, стандартизованих заходів безпеки та підвищення відповідальності на рівні виконавчої влади та правління…

Відповідно до CCSPA, призначені оператори мають суворі зобов'язання щодо дотримання вимог, включаючи розробку комплексних програм кібербезпеки, що охоплюють як IT, так і операційні технології, а також суворе управління ризиками ланцюга поставок. Основним принципом законодавства є вимога щодо оперативного повідомлення про інциденти до Управління безпеки комунікацій (CSE), що забезпечує повідомлення про значні порушення у строго встановлені терміни. Для забезпечення дотримання цих стандартів уряд встановив режим обов'язкових аудитів та потенційних штрафів, які можуть сягати мільйонів доларів, змушуючи організації надавати пріоритет прозорості та управлінню над відносинами з постачальниками та внутрішнім контролем…

Хоча закон буде впроваджуватися поетапно — від призначення та опублікування нормативних актів до остаточного періоду виконання — організації стикаються з негайними перешкодами, включаючи тягар модернізації застарілих систем, усунення дефіциту талантів та управління збільшеними витратами на дотримання вимог. Отже, керівникам IT-відділів настійно рекомендується проактивно проводити оцінку готовності, складати карту критичних системних залежностей та модернізувати робочі процеси реагування на інциденти, а не чекати на повне введення закону в дію. Зрештою, CCSPA є стратегічним поворотним моментом для Канади, перетворюючи кіберстійкість на фундаментальне оперативне завдання, необхідне для забезпечення цифрового майбутнього країни…» ***(Canadian Critical Cyber Systems Protection Act: Key Requirements, Timelines, and Risks // Demand Media BPM (https://ittech-pulse.com/our-tech-insights/canadian-critical-cyber-systems-protection-act-key-requirements-timelines-and-risks/). 19.11.2025).***

***

«**Державні та місцеві органи влади, які вже є головними цілями для програм-вимагачів, вторгнень у шкільні системи та підозрюваних китайських вторгнень у мережі питного водопостачання, з 2021 року покладаються на федеральну програму грантів з кібербезпеки для штатів та місцевих органів влади (SLCGP), яка протягом чотирьох років виділяє 1 мільярд доларів (80% з яких проходить через штати) для допомоги юрисдикціям, що відчувають брак коштів, у зміцненні захисту та розробці спільних планів реагування на кіберзагрози.** Програма має закінчитися 30 січня 2026 року, але Палата представників одностайно схвалила двопартійний закон про захист інформації місцевими лідерами для забезпечення стійкості агентств (PILLAR), щоб продовжити та оновлювати її ще на сім років…

PILLAR розширить допустимі види використання, включивши захист операційних технологій та систем штучного інтелекту, зобов'яже здійснювати закупівлі з урахуванням принципу «безпека за замовчуванням» та винагороджуватиме швидке впровадження багатофакторної автентифікації та інструментів управління ідентифікацією та доступом. У той час як частка

федеральних витрат SLCGP знизилася з 90 відсотків у 2022 фінансовому році до 60 відсотків у 2025 фінансовому році, PILLAR встановить стабільну федеральну частку, обмежену 60 відсотками (65 відсотків для юрисдикцій, які достроково досягли цілей MFA та IAM). Він не вказує конкретну суму фінансування, залишаючи майбутні асигнування на розсуд Конгресу…

Прихильники стверджують, що SLCGP вже допомогла виявити атаки — Юта зупинила одну з них на місцевому аеропорту, Луїсвілл створив платформу для обміну інформацією про загрози в режимі реального часу — але наголошують, що постійне, передбачуване фінансування є надзвичайно важливим, оскільки невеликі юрисдикції не мають достатньої кількості персоналу або бюджетів, щоб самостійно захищатися від хакерів з національних та транснаціональних злочинних угруповань. Зараз законопроект очікує на розгляд у Сенаті; якщо його не ухвалять, програма грантів втратить чинність». ***(Jule Pattison-Gordon. States and Localities May Get More Federal Cybersecurity Money // e.Republic LLC (https://www.governing.com/policy/states-and-localities-may-get-more-federal-cybersecurity-money). 19.11.2025).***

***

«Комісія з цінних паперів і бірж США завершила судову тяганину з компанією SolarWinds і її головним спеціалістом з інформаційної безпеки Тімоті Г. Брауном, спільно подавши 20 листопада 2025 року клопотання до суду про відхилення позову, в якому стверджувалося, що компанія ввела інвесторів в оману щодо заходів безпеки, вжитих до хакерської атаки на ланцюжок поставок у 2020 році. Позов, поданий у жовтні 2023 року, містив звинувачення у шахрайстві, порушеннях внутрішнього контролю та навмисному применшенні відомих кіберризиків, а також звинувачення Брауна в ігноруванні неодноразових «червоних прапорців»… Багато з цих звинувачень вже були відхилені федеральним суддею Нью-Йорка в липні 2024 року як такі, що ґрунтуються на ретроспективному аналізі та спекуляціях. Хоча в добровільному відмові SEC зазначається, що це «не обов'язково відображає» її позицію в інших питаннях — насправді, з того часу агентство висунуло звинувачення проти кількох інших постачальників у зв'язку з відповідними розкриттями інформації — це поклало край гучній справі SolarWinds…» ***(Ravie Lakshmanan. SEC Drops SolarWinds Case After Years of High-Stakes Cybersecurity Scrutiny // The Hacker News (https://thehackernews.com/2025/11/sec-drops-solarwinds-case-after-years.html). 21.11.2025).***

***

«Агентство з кібербезпеки та безпеки інфраструктури США (CISA) бореться з тим, що виконуючий обов'язки директора Мадху Готтумуккала називає «серйозною кадровою кризою» після втрати майже третини своїх співробітників під час тривалого закриття уряду цього року та подальшого скорочення штату. У меморандумі від 5 листопада Готтумуккала попередив, що приблизно 40 відсотків ключових посад залишаються вакантними, що обмежує здатність CISA виконувати завдання національної безпеки, і закликав до активного

найму персоналу — з використанням системи управління кіберталантами DHS — щоб до кінця 2026 фінансового року залучити «висококваліфікованих фахівців»…

Ця апеляція суперечить зусиллям адміністрації Трампа, яка постійно скорочувала штат агентства, закривала офіси та скоротила відділ взаємодії із зацікавленими сторонами приблизно на 35 %. Нинішні та колишні чиновники заявляють, що вакансії уповільнили реагування на інциденти, оцінку ризиків, технічні консультації та координацію з партнерами на рівні штатів, місцевих органів влади та критичної інфраструктури. Відділ зв'язків з громадськістю CISA відмовився обговорювати чисельність персоналу, тоді як законодавці вимагають оновлених даних про штат, щоб оцінити повний вплив скорочень». ***(Chris Riotta. US Cyber Defense Agency Admits to Major Staffing Crisis // Information Security Media Group, Corp. (https://www.govinfosecurity.com/us-cyber-defense-agency-admits-to-major-staffing-crisis-a-30062). 18.11.2025).***

***

«Опитування Binalyze, проведене серед 200 керівників служб інформаційної безпеки (CISO) у США, показує, що неефективні методи реагування на інциденти обходяться підприємствам дуже дорого: за останні п'ять років нечіткі розслідування обійшлися кожній компанії в середньому в 1,1 мільйона доларів — близько 48 мільярдів доларів по всій країні — і кожна додаткова година до вжиття заходів додає приблизно 114 000 доларів…

Хоча 84% керівників служб безпеки зараз визнають, що успішне порушення безпеки є неминучим, 79% бюджетів все ще розподіляються у співвідношенні 2:1 на користь профілактики, а не реагування. На практиці лише половина керівників служб інформаційної безпеки можуть швидко відповісти на основні питання після порушення безпеки, наприклад, чи мають зловмисники доступ до даних і які саме дані були викрадені. 75% вважають, що подібна атака може повторитися, а 65% визнають, що їхні компанії не винесли належних уроків…

За останній рік 70% компаній мали труднощі з усуненням інцидентів, 61% отримали штрафи від регуляторних органів, а 56% отримали відмову у виплаті страхового відшкодування за кіберстрахуванням через відсутність доказів щодо необхідних заходів контролю. В середньому залучення команд з розслідування інцидентів займає 8,6 годин, що призводить до додаткових збитків у розмірі майже 1 мільйона доларів, частково через те, що організації бачать лише 57% своїх IT-ресурсів. Binalyze стверджує, що швидке «розслідування кіберінцидентів», краща видимість та негайний аналіз є життєво важливими для скорочення витрат, задоволення вимог регуляторних органів та страхових компаній, а також запобігання повторним вторгненням». ***(Binalyze Report Highlights High Cost of Slow Cyber Incident Response // SecurityInfoWatch (https://www.securityinfowatch.com/cybersecurity/press-release/55331753/binalyze-report-highlights-high-cost-of-slow-cyber-incident-response). 20.11.2025).***

***

«Адміністрація Трампа переорієнтувала політику США в галузі кібербезпеки на стратегічні технології — штучний інтелект, постквантову

криптографію, безпеку ланцюгів постачання програмного забезпечення та загрози, що фінансуються державою — шляхом ухвалення в червні 2025 року виконавчого наказу, який зберігає чинну федеральну структуру, але перерозподіляє пріоритети щодо ресурсів. Водночас запропоновані скорочення бюджету на 2026 рік призведуть до зменшення фінансування Агентства з кібербезпеки та безпеки інфраструктури (CISA) на 17 відсотків, ліквідації 1000 посад та скорочення вдвічі штату Управління директора національної розвідки. Ці скорочення, а також ліквідація підрозділів, що стежать за Росією, можуть послабити зв'язки з промисловістю та союзниками, зменшити підтримку з боку штатів та місцевих органів влади і залишити критичну інфраструктуру більш вразливою до атак програм-вимагачів та атак з боку інших держав…

Недавні інциденти підкреслюють важливість цього питання: «Salt Typhoon», пов'язаний з Китаєм, зламав телекомунікаційні та урядові мережі США; російські, іранські та північнокорейські оператори посилюють саботаж і шпигунство; кількість атак з використанням програм-вимагачів за п'ять років зросла в п'ять разів, що коштувало державним установам США до 9,5 мільйонів доларів за кожен інцидент. Штучний інтелект прискорює як напад, так і захист, що викликає дискусії про створення спеціальних військових кібервійськ…

Виникають три сценарії:

Цільова реформа: зосередившись на штучному інтелекті, постквантових технологіях та державних APT, можна оптимізувати захист і прискорити впровадження безпечних за своєю конструкцією рішень, але це залишить прогалини в захисті від повсякденних програм-вимагачів, які атакують школи та комунальні підприємства.

Скорочення та політизація: значне скорочення CISA та розвідки в поєднанні з партійною ротацією підривають обмін інформацією, готовність на державному та місцевому рівнях та фахівців-талантів, що відображає провали російської розвідки до 2022 року.

Напруження в альянсі: транзакційна позиція США щодо європейського регулювання технологій та скорочення обміну розвідданими (наприклад, конфлікт між країнами «П'яти очей») послаблює колективну кіберстійкість у міру зростання атак на інфраструктуру НАТО…

Більш чітка спрямованість виконавчого розпорядження може покращити високоефективні засоби стримування, проте без стабільного фінансування, професійного персоналу та тісної координації з союзниками, загальна система безпеки Заходу залишатиметься вразливою в епоху швидкої еволюції загроз, що зумовлена розвитком штучного інтелекту». ***(Frank Umbach. U.S. cybersecurity policy under Trump // Geopolitical Intelligence Services AG (https://www.gisreportsonline.com/r/trump-cyber/). 26.11.2025).***

***

«Країни-кандидати в ЄС поспішають дотримуватися цифрових стандартів: перед вступом до ЄС країни-кандидати повинні відповідати технологічним стандартам блоку, включаючи цифрові гаманці до 2026 року, надійну кібербезпеку відповідно до NIS2 та правила AI Act. Цифрові гаманці швидко розвиваються: молдовський додаток EVO (за підтримки ЄС) цього року запускає пілотну версію підписів; Північна Македонія до грудня запускає «супердодаток» m.Uslugi з функціями зберігання документів та нагадувань; албанська компанія Identitek пропонує багатофункціональні ідентифікатори на основі телефону; Україна, Сербія та Албанія встигли до терміну, а Боснія, Північна Македонія та Молдова вже випробували пілотні версії…

У сфері кібербезпеки спостерігається значний прогрес: Україна лідирує завдяки угодам з ENISA, спеціалізованій кіберлабораторії та підтримці Талліннського механізму; Албанія, Чорногорія, Грузія, Молдова та Північна Македонія можуть похвалитися національними стратегіями, узгодженими з ЄС (Молдова приєднується до кризового резерву ENISA; Чорногорія приймає центр потенціалу Західних Балкан). План Туреччини викликає критику за те, що він дозволяє масове стеження, тоді як Сербія розробляє стратегію боротьби з кіберзлочинністю за допомогою ЄС…

Готовність до впровадження ШІ дещо відстає: Албанія, Молдова, Сербія та Україна мають стратегії, але ще не мають законів. Албанія унікальним чином призначила першого в світі міністра з питань ШІ, «Діелу», для нагляду за проведенням публічних тендерів без корупції (незважаючи на занепокоєння щодо упередженості), а також 83 політичних помічників з питань ШІ; Сербія встановила етичні рекомендації та законодавчу раду…» ***(Anna Desmarais. Here are the digital changes EU candidate countries are making to align with the bloc // Euronews (https://www.euronews.com/next/2025/11/04/here-are-the-digital-changes-eu-candidate-countries-are-making-to-align-with-the-bloc). 04.11.2025).***

***

«…Незважаючи на те, що Європейський Союз має одні з найсуворіших у світі законів про захист даних, включаючи GDPR, журналісти в Європі продемонстрували, що «легко» шпигувати за високопосадовцями ЄС, використовуючи комерційно отримані історії місцезнаходження, які продають брокери даних. Коаліція репортерів отримала безкоштовний зразок набору даних, що містить 278 мільйонів точок даних про місцезнаходження з мільйонів телефонів у Бельгії, який розкриває детальну історію місцезнаходження високопосадовців Європейської комісії та пристроїв у Європейському парламенті… Ця конфіденційна інформація, яка зазвичай завантажується звичайними мобільними додатками, а потім продається брокерами даних, часто купується урядами та військовими. З того часу чиновники ЄС висловили занепокоєння та видали нові вказівки для персоналу щодо протидії відстеженню, оскільки брокерська діяльність з даними перетворилася на мільярдну індустрію. Легкість, з якою було здійснено це спостереження, підкреслює повільність заходів, що вживаються наглядовими органами проти

посередників у торгівлі даними, навіть попри те, що ризики для безпеки, такі як витік даних Gravy Analytics у 2024 році, який розкрив дані про місцезнаходження десятків мільйонів людей, продовжують зростати…». ***(Zack Whittaker. Phone location data of top EU officials for sale, report finds // TechCrunch Media LLC (https://techcrunch.com/2025/11/04/phone-location-data-of-top-eu-officials-for-sale-report-finds/). 04.11.2025).***

***

«…Європа переживає різке зростання загроз кібербезпеці, що посилюється її близькістю до конфлікту в Україні та Південно-Західній Азії, що робить її другою за популярністю ціллю в світі після Північної Америки (22% спеціалізованих сайтів з витоками інформації). Багатство регіону та його статус привабливої цілі приваблюють потужні синдикати кіберзлочинців, відомі як «мисливці на велику дичину», які легко переносять свої операції з північноамериканських цілей на багаті країни, такі як Велика Британія, Німеччина та Франція, використовуючи «здорову екосистему для придбання доступу до скомпрометованих організацій»…

Загрози мають як фінансове, так і політичне підґрунтя. Національні держави, зокрема Росія, Китай, Північна Корея та Іран, активно займаються кібершпигунством та деструктивними атаками, спрямованими на збір розвідданих, поширення дезінформації та залякування дисидентів, часто з подвійною метою: створення хаосу та фінансування таємних операцій. Російські атаки залишаються зосередженими на Центрально-Західній та Східній Європі через війну в Україні, тоді як Китай і Північна Корея націлені на великі західноєвропейські держави, включаючи Велику Британію, Іспанію та Італію. Захист від цього складного ландшафту загроз, за даними CrowdStrike, вимагає знання супротивника та зосередження тактичної оборони на забезпеченні ідентичності, контролі доступу до хмари, усуненні прогалин у міждоменній видимості та пріоритетності виправлень, спрямованих на супротивника, щоб швидко нейтралізувати найбільші ризики…» ***(Eoin Higgins. Europe faces down threat actors // Morning brew Inc. (https://www.itbrew.com/stories/2025/10/30/europe-faces-down-threat-actors). 03.11.2025).***

***

«Звіт CrowdStrike про загрози в Європі у 2025 році малює сувору картину регіону, який зазнає все більш витончених кіберзагроз. Майже 22 % усіх глобальних випадків використання програм-вимагачів та вимагання грошей зараз стосуються європейських організацій, що підсилюється процвітанням тіньової економіки, де пропозиції «зловмисного програмного забезпечення як послуги» та ринки облікових даних роблять атаки дешевими та масштабованими… Шпигунство з боку національних держав також набирає обертів: суб'єкти, пов'язані з Китаєм, розширили свою діяльність на 150 %, зосередившись на фінансах, ЗМІ та виробництві, тоді як іранські групи експериментують з генеративним штучним інтелектом, щоб виявити нові вразливості та створити вдосконалені експлойти. Водночас кампанії з соціальної інженерії досягають нових рівнів реалістичності;

лише інциденти з вішингом зросли на 442 % за шість місяців, а такі групи, як CURLY SPIDER, CHATTY SPIDER та PLUMP SPIDER, використовують штучний інтелект для створення переконливих фішингових та підроблених приманок… Традиційне шкідливе програмне забезпечення більше не є домінуючою точкою входу — 79 % початкових вторгнень зараз базуються на викрадених облікових даних, що відображається у 50 %-му зростанні реклами посередників доступу. Північнокорейська група FAMOUS CHOLLIMA є прикладом цієї зміни, використовуючи інсайдерські персони у 40 % своїх 304 зареєстрованих операцій. Тим часом середній час прориву електронної злочинності скоротився до всього 48 хвилин, а найшвидше вторгнення було здійснено всього за 51 секунду. Хмарні середовища також піддаються ризику: кількість вторгнень у хмарні середовища зросла на 26 % у порівнянні з минулим роком, а зловживання дійсними обліковими записами спричинило 35 % початкових спроб доступу. Більше половини всіх експлуатованих вразливостей пов'язані з цими початковими точками входу. Щоб протистояти цьому «переповненому і складному полю бою», CrowdStrike закликає організації застосовувати захист на основі розвідки, посилювати контроль ідентичності та доступу, покращувати видимість хмари, прискорювати виправлення та управління вразливостями, контролювати ланцюжок постачання кіберзлочинності та консолідувати захист на масштабованих, уніфікованих платформах безпеки, які можуть виявляти, вистежувати та реагувати зі швидкістю машини…» ***(Rabia Noureen. Ransomware Surge and AI-Driven Threats Reshape Europe's Cybersecurity Landscape // Petri Media LLC (https://petri.com/ransomware-surge-ai-threats-europe-cybersecurity/). 04.11.2025).***

***

«За даними аналізу урядових даних про порушення, проведеного money.co.uk, кібератаки зараз коштують малим і мікропідприємствам Великобританії приблизно 921,2 млн фунтів стерлінгів на рік, причому адміністративні та нерухомі компанії втрачають понад 125,9 млн фунтів стерлінгів, що робить їх другим сектором, який найбільше постраждав у фінансовому плані. Професійні, наукові та технічні послуги очолюють список із 152,3 млн фунтів стерлінгів, за ними йдуть будівництво (115,7 млн фунтів стерлінгів), роздрібна/оптова торгівля (115,1 млн фунтів стерлінгів) та інформація/комунікації (76,4 млн фунтів стерлінгів). Майже половина (48%) нерухомісних компаній повідомили про порушення за останні 12 місяців, що робить цей сектор одним з найбільш уразливих, головним чином через значну залежність від цифрових платформ для виставлення рахунків та управління проектами, які створюють слабкі місця для шахрайства з рахунками, фішингу та програм-вимагачів. Оскільки фішинг фігурує у 85% повідомлених порушень, компанії, які мають справу з декількома зацікавленими сторонами та гібридними операціями, є особливо вразливими…

Джо Фелан з Money.co.uk попереджає, що середні витрати малих підприємств на усунення інцидентів зросли на понад 90% у порівнянні з минулим роком, і закликає підприємства будь-якого розміру інтегрувати кібербезпеку в повсякденну діяльність: надавати пріоритет навчанню персоналу, регулярному оновленню

програмного забезпечення та системам раннього виявлення, а також планувати фінансові наслідки збою в роботі. Створення грошового резерву на бізнес-рахунку з високими відсотками та миттєвим доступом може допомогти покрити несподівані витрати та фінансувати постійні поліпшення безпеки. Використання спеціального бізнес-рахунку з вбудованими засобами контролю шахрайства (наприклад, Positive Pay) додає профілактичний захист, позначаючи підозрілі перекази та зменшуючи ризик захоплення рахунку. Проактивне технічне та фінансове планування дає найкращий шанс швидко відновитися та мінімізувати довгостроковий вплив кіберзлочинів…» ***(Marc da Silva. Cyberattacks cost small real estate firms £125m each year, says report // Property Industry Eye (https://propertyindustryeye.com/cyberattacks-cost-small-real-estate-firms-125m-each-year-says-report/). 03.11.2025).***

***

«Критична інфраструктура Ірландії є «надзвичайно вразливою» до кібератак, за словами Девіда Сільке, керуючого директора європейської штаб-квартири Centripetal, який попереджає, що цифрова атака може паралізувати цю країну, яка сильно залежить від цифрових технологій. Аналіз Centripetal, представлений на нещодавній конференції Cyber Ireland, виявив «значні прогалини в кібербезпеці» по всій країні, підкресливши, що 40% (98) з приблизно 200 критично важливих національних інфраструктурних організацій Ірландії, що охоплюють уряд, охорону здоров'я та вищу освіту, мають ідентифіковані вразливості в своїх мережах. Загалом 349 000 ірландських мереж вразливі до викриття та захоплення, часто через автоматизовані атаки, спрямовані на незахищені або застарілі системи автоматизації…

Сільке підкреслив, що кібербезпека повинна стати вищим національним пріоритетом, попередивши, що вразливість Ірландії робить її привабливою відправною точкою для комерційних і підтримуваних державою хакерів, які прагнуть поширювати атаки за межі країни. Результатом цього може стати значна шкода репутації, особливо з огляду на залежність Ірландії від прямих іноземних інвестицій (ПІІ). Сільке високо оцінив Національний центр кібербезпеки, але наголосив на необхідності проактивного підходу, стверджуючи, що в 98% випадків інформація про загрозу стає доступною до того, як відбувається атака. Він закликає організації використовувати цю інформацію та займати проактивну позицію, особливо щодо нових загроз, таких як зловживання штучним інтелектом, щоб створити стійкі системи безпеки, необхідні для захисту даних та активів…» ***(James Cox. Ireland's critical infrastructure 'extremely vulnerable' to cyberattacks, expert warns // BreakingNews.ie (https://www.breakingnews.ie/ireland/irelands-critical-infrastructure-extremely-vulnerable-to-cyberattacks-expert-warns-1825700.html). 03.11.2025).***

***

«…Як одна з найбільш цифрових економік Європи, Данія стикається з розширенням і критичним зростанням площі атаки, оскільки 92% організацій покладаються на хмарну інфраструктуру, а серйозні загрози впливають на її ключові сектори. Тільки в 2024 році кількість кіберінцидентів зросла на 47% у

порівнянні з попереднім роком, кількість випадків використання програм-вимагачів зросла на 52%, а середня вартість порушення безпеки досягла 26,4 млн датських крон. Загрози характеризуються програмним забезпеченням для вимагання викупу 2.0, націленим на системи ОТ, фішингом, що генерується штучним інтелектом, який з'являється в 31% інцидентів, та зондуванням з боку державних суб'єктів, таких як Sandworm і Volt Typhoon, що призводить до збільшення середнього часу відновлення до 28 днів…

Це зростання ризику збігається з введенням в дію Директиви ЄС NIS2 (жовтень 2025 р.), яка вимагає цілодобового звітування та підзвітності на рівні правління, а також з критичною нестачею понад 7000 вакансій у сфері кібербезпеки в Данії. Для подолання операційної втоми, спричиненої управлінням численними інструментами безпеки та великим обсягом тривожних повідомлень, необхідні автоматизація та штучний інтелект… Такі платформи, як Open Threat Management (OTM) від Seceon на базі штучного інтелекту, об'єднують SIEM, SOAR, XDR та OT/IoT, зменшуючи складність SOC на 80% і скорочуючи час виявлення з місяців до хвилин, що дозволяє невеликій команді аналітиків досягти результату, який зазвичай досягають 20 і більше фахівців. Цей уніфікований підхід також допомагає данським підприємствам автоматизувати дотримання критично важливих вимог, включаючи NIS2, GDPR, DORA та Національну кіберстратегію, перетворюючи кіберзахист з набору розрізнених інструментів на прогнозовану, автоматизовану національну стратегію стійкості…» ***(Kamna Srivastava. Denmark's Digital Defense 2025: AI Security Cutting Cyber Losses by Billions // Techstrong Group Inc. (https://securityboulevard.com/2025/11/denmarks-digital-defense-2025-ai-security-cutting-cyber-losses-by-billions/). 04.11.2025).***

***

«Банк Англії прямо пов'язав нижчий, ніж очікувалося, ріст ВВП Великобританії з кібератакою на Jaguar Land Rover (JLR) у вересні, зазначивши, що цей інцидент, поряд із падінням експорту до США, призвів до скорочення виробництва у третьому кварталі приблизно на 0,2%. Ця атака, класифікована Кібермоніторинговим центром як системна подія категорії 3, змусила уряд вжити фінансових заходів, закрила заводи JLR на кілька тижнів і відбилася на всьому ланцюжку поставок. Економісти оцінюють збитки JLR у понад 2 млрд фунтів стерлінгів, а збитки економіки в цілому — у 2,1 млрд фунтів стерлінгів. Це перший випадок, коли кібератака була визнана такою, що завдала істотної макроекономічної шкоди Великобританії…

Зупинка роботи JLR стала завершенням літа, яке ознаменувалося серйозними порушеннями безпеки у Великобританії. Атаки, які, ймовірно, пов'язані з бандою Scattered Spider, торкнулися роздрібних мереж M&S, Co-op і Harrods, що змусило M&S зарезервувати 136 мільйонів фунтів стерлінгів на витрати з усунення наслідків і попередити, що витрати, пов'язані з кібербезпекою, можуть досягти 300 мільйонів фунтів стерлінгів до кінця року, незважаючи на страховий ліміт у 100 мільйонів фунтів стерлінгів. Національний центр кібербезпеки повідомляє, що кількість інцидентів національного значення зріс до 204 за рік до вересня, порівняно з 89, а кількість особливо значущих випадків зросла на 50 відсотків. Керівник

Національного центру кібербезпеки (NCSC) Річард Хорн закликав бізнес-лідерів «діяти негайно», аргументуючи це тим, що кібербезпека більше не є опцією, а є життєво важливою як для виживання корпорацій, так і для національної стійкості…» ***(Connor Jones. Bank of England says JLR's cyberattack contributed to UK's unexpectedly slower GDP growth // The Register (https://www.theregister.com/2025/11/07/bank_of_england_says_jlrs/). 07.11.2025).***

***

«Закон ЄС про кіберстійкість (CRA) або Регламент (ЄС) 2024/2847 встановлює обов'язкові вимоги до кібербезпеки для всіх продуктів з цифровими елементами — як апаратного, так і програмного забезпечення — що розміщуються на ринку ЄС. Його основною метою є створення більш безпечної та прозорої екосистеми цифрових продуктів шляхом встановлення чіткого «ланцюжка відповідальності». У рамках цієї структури виробники несуть основні зобов'язання, а імпортери та дистриб'ютори мають вторинні обов'язки щодо перевірки відповідності та повідомлення про невідповідності…

CRA застосовується до широкого кола економічних операторів, включаючи виробників, імпортерів та дистриб'юторів, а також постачальників рішень для віддаленої обробки даних, таких як SaaS та хмарні сервіси. Його правила застосовуються екстериторіально, що означає, що будь-який продукт, розміщений на ринку ЄС, повинен відповідати вимогам, незалежно від місця знаходження виробника. Однак Закон не поширюється на сектори, що мають власні специфічні закони про кібербезпеку, такі як медичні пристрої, авіація, автомобілебудування та морське обладнання, а також не застосовується до запасних частин, військового обладнання або некомерційного програмного забезпечення з відкритим кодом…

Для виробників зобов'язання є широкими і починаються ще на етапі проектування. Вони повинні забезпечити «безпеку за замовчуванням і за дизайном», що означає, що продукти повинні розроблятися без відомих вразливостей, які можна використати, і мати безпечні конфігурації. Це вимагає проведення комплексних оцінок ризиків, складання детальної технічної документації та проходження процедури оцінки відповідності, що відповідає класу ризику продукту — від самодекларації для стандартних продуктів до залучення «нотифікованого органу» для товарів з підвищеним ризиком. Для спрощення цього процесу дотримання гармонізованих стандартів забезпечує «презумпцію відповідності».

Крім того, виробники зобов'язані надавати безкоштовні оновлення безпеки протягом щонайменше п'яти років (або протягом очікуваного терміну експлуатації продукту, якщо він коротший), чітко повідомляти користувачам про термін підтримки та наносити маркування CE, що свідчить про відповідність вимогам. Вони також повинні встановити надійні процеси управління вразливостями та повідомлення про інциденти, зберігати записи протягом десяти років і вживати негайних коригувальних заходів, таких як відкликання, якщо продукт визнано таким, що не відповідає вимогам. Імпортери та дистриб'ютори повинні перевіряти відповідність продуктів вимогам і повідомляти про будь-які проблеми владі…

Критичний термін наближається набагато раніше, ніж основна дата дотримання вимог. Хоча більшість положень CRA набувають повної чинності 11

грудня 2027 року, зобов'язання щодо повідомлення про вразливість та інциденти відповідно до статті 14 набувають чинності 11 вересня 2026 року. Це вимагає від виробників заздалегідь підготувати триетапний процес повідомлення з чіткими термінами для інформування органів влади та користувачів про активно експлуатовані вразливості або серйозні інциденти (24 години), а потім надати детальні звіти (72 години) та остаточний аналіз першопричин (від 14 днів до 1 місяця).

Недотримання вимог CRA тягне за собою суворі санкції у вигляді штрафів у розмірі до 15 мільйонів євро або 2,5% від глобального річного обороту компанії. Для підготовки компанії повинні негайно розпочати оцінку своїх продуктових портфелів, класифікацію продуктів за рівнем ризику, підготовку технічної документації, створення систем управління вразливістю та перегляд контрактів з постачальниками та дистриб'юторами з метою забезпечення відповідності новим нормативним вимогам…» ***(Pierre-Emmanuel Froge. The Cyber Resilience Act is Rewriting the Rules of Digital Products Safety // Bryan Cave Leighton Paisner LLP (https://www.bclplaw.com/en-US/events-insights-news/the-cyber-resilience-act-is-rewriting-the-rules-of-digital-products-safety.html). 07.11.2025).***

***

«Директива ЄС NIS 2 (Directive (EU) 2022/2555), впроваджена в Італії законодавчим декретом № 138/2024, фундаментально підносить кібербезпеку з технічної проблеми ІТ до основної відповідальності керівництва. Ця нова система робить керівників компаній безпосередньо і особисто відповідальними за нагляд за стратегіями кібербезпеки, політикою управління ризиками та планами реагування на інциденти. Дія директиви є широкою і охоплює велику кількість «основних» та «важливих» суб'єктів у багатьох секторах, що виходять за межі традиційної критичної інфраструктури…

Ця зміна означає перехід від формального дотримання вимог до суттєвого, задокументованого управління ризиками, що вимагає від правлінь продемонструвати, що кіберстійкість є невід'ємною частиною ДНК компанії. Недотримання вимог має серйозні наслідки, включаючи адміністративні штрафи для членів правління в розмірі до 10 мільйонів євро, а в тяжких випадках — тимчасове позбавлення права обіймати керівні посади…

NIS 2 ставить перед міжнародними компаніями кілька складних завдань, серед яких: екстериторіальна сфера застосування, що вимагає від компаній, які не є членами ЄС, призначити представника в ЄС; ризик фрагментації регулювання в різних державах-членах; нова відповідальність за ланцюжок поставок, що вимагає переоформлення контрактів з постачальниками; а також складність управління зобов'язаннями, що дублюються з іншими нормативно-правовими актами, такими як GDPR і DORA.

Для правлінь найближчими пріоритетами є визначення класифікації їхніх компаній відповідно до NIS 2, посилення процедур нагляду правління, зміцнення кібербезпеки ланцюгів постачання та інтеграція різних режимів звітності. В Італії суб'єкти, що підпадають під дію закону, мають чіткий графік: вони повинні бути готові до повідомлення про інциденти до січня 2026 року та повністю відповідати

всім обов'язкам з управління та управління ризиками до жовтня 2026 року. Зрештою, NIS 2 — це не просто виконання вимог, а фундаментальний обов'язок управління, який має вирішальне значення для захисту бізнесу, його репутації та довіри зацікавлених сторін…» ***(Alessandro Seganfreddo, Giulia Mariuz, Maria Lucia Passador and Cecilia Canova. NIS2: Cyber governance as a boardroom matter // Hogan Lovells (https://www.hoganlovells.com/en/publications/nis2-cyber-governance-as-a-boardroom-matter). 12.11.2025).***

***

«…Португалія зробила вирішальний крок у напрямку транспонування Директиви ЄС NIS2, опублікувавши 22 жовтня 2025 року Закон № 59/2025. Цей закон не є остаточним транспонуванням, а скоріше дозволом, який встановлює керівні принципи для уряду щодо створення комплексного законодавчого пакету протягом 180 днів, встановлюючи остаточний термін для імплементаційних актів 21 квітня 2026 року…

Проект остаточного імплементаційного акту, декрету-закону, вже доступний і, як очікується, не зазнає істотних змін. Він тісно слідує Директиві NIS2, приймаючи її точну сферу застосування та визначення «основних» та «важливих» суб'єктів у таких секторах, як енергетика, транспорт, банківська справа та охорона здоров'я. Основні зобов'язання для цих суб'єктів включають впровадження надійних заходів кібербезпеки та безпеки ланцюгів постачання, призначення відповідального за кібербезпеку та контактної особи, а також реєстрацію на електронній платформі, яка буде створена найближчим часом…

Очікується, що новий режим набуде чинності через 120 днів після опублікування Декрету-закону, ймовірно, наприкінці літа 2026 року. Однак після цього буде встановлено значний перехідний період тривалістю 24 місяці для повного виконання основних зобов'язань, таких як прийняття конкретних заходів з кібербезпеки та застосування режиму санкцій. Це надає зацікавленим суб'єктам важливий час для підготовки. Компаніям настійно рекомендується використати цей час для визначення своєї класифікації відповідно до нового закону та розпочати адаптацію своїх внутрішніх процедур і залучення вищого керівництва для забезпечення своєчасного дотримання вимог». ***(Ana Mira Cordeiro. NIS2 Directive transposition in Portugal: Status and brief overview // Bird & Bird (https://www.twobirds.com/en/insights/2025/nis2-directive-transposition-in-portugal-status-and-brief-overview). 12.11.2025).***

***

«…Німеччина значно посилила свої закони про ІТ-безпеку, прийнявши Закон про впровадження NIS2, який переносить Директиву ЄС NIS2 у національне законодавство. Це законодавство значно розширює сферу регулювання організацій, виходячи далеко за межі традиційного сектора «KRITIS» (критична інфраструктура), і тепер охоплює широке коло великих і середніх компаній у таких секторах, як енергетика, транспорт, охорона здоров'я та цифрова інфраструктура, як правило, на основі таких критеріїв, як наявність 50 і більше співробітників…

Основні зобов'язання для цих «особливо важливих» та «важливих» суб'єктів є всеосяжними. Вони повинні впровадити надійні заходи з управління ризиками, включаючи суворий контроль доступу, реагування на інциденти та плани забезпечення безперервності бізнесу. Обов'язковим є багаторівнева система повідомлення про значні інциденти, яка вимагає попередження протягом 24 годин. Крім того, компанії тепер несуть відповідальність за забезпечення безпеки ланцюга поставок, що означає, що вони повинні вимагати від своїх постачальників та постачальників послуг дотримання вимог на договірній основі…

Важливо, що закон набирає чинності негайно після його опублікування, без перехідного періоду. Тому компанії повинні негайно переглянути свою класифікацію, провести аналіз розбіжностей з новими вимогами та створити ефективну організацію інформаційної безпеки. Керівництво несе пряму відповідальність, а за невиконання вимог передбачені суворі штрафи, які можуть досягати 10 мільйонів євро або 2% від глобального річного обороту для найбільш критичних суб'єктів господарювання. Отже, для зменшення юридичних, фінансових та репутаційних ризиків зараз необхідний структурований підхід до досягнення відповідності вимогам». ***(Michael Kuska and Manuel Poncza. Bundestag approves NIS2 implementation law - What companies need to know and do now // HEUKING (https://www.heuking.de/en/news-events/newsletter-articles/detail/bundestag-approves-nis2-implementation-law-what-companies-need-to-know-and-do-now.html). 14.11.2025).***

***

«Законопроект про кібербезпеку та стійкість (мережеві та інформаційні системи), поданий до парламенту Великої Британії 12 листопада 2025 року, є найзначнішим переглядом британської системи кібербезпеки за останнє десятиліття. Законопроект, розроблений з метою модернізації Регламенту NIS 2018 року та приведення його у відповідність до Директиви NIS2 ЄС, є прямою реакцією на різке зростання кількості кібератак — на 50 % згідно з щорічним оглядом NCSC за 2025 рік — та щорічних економічних збитків у розмірі 14,7 млрд фунтів стерлінгів, які вони завдають…

Законодавство значно розширює сферу прямого регулювання. Окрім існуючих операторів основних послуг (охорона здоров'я, енергетика, водопостачання, транспорт, цифрова інфраструктура) та відповідних постачальників цифрових послуг (онлайн-ринки, пошукові системи, хмарні послуги), тепер до нього додаються:

середні та великі постачальники керованих послуг (регулюються Комісією з інформації),

центри обробки даних потужністю 1 МВт або більше (10 МВт для внутрішніх центрів підприємств),

та організації, що контролюють 300 МВт або більше електричного навантаження для дистанційного управління приладами (регулюються спільно Департаментом енергетичної безпеки та Net Zero і Ofgem)…

Регулюючі органи також отримають нові повноваження для визначення «критично важливих постачальників», порушення роботи яких може серйозно

порушити функціонування основних служб або економіки в цілому, усунувши тим самим значну вразливість ланцюга поставок, яка неодноразово використовувалася в останніх атаках…

Повідомлення про інциденти стає набагато суворішим і швидшим: організації повинні подати попереднє повідомлення протягом 24 годин і повний звіт протягом 72 годин після значного інциденту, одночасно надіславши копії до NCSC. Визначення інциденту, про який необхідно повідомляти, розширено і тепер включає програми-вимагачі, крадіжку даних та попередньо підготовлені атаки, навіть якщо вони не спричиняють негайних порушень. Постраждалі клієнти постачальників цифрових послуг, постачальників керованих послуг та центрів обробки даних також повинні бути повідомлені…

Повноваження з питань правозастосування значно посилені. Штрафи будуть розраховуватися як відсоток від глобального річного обороту: до 4% (мінімум 17 мільйонів фунтів стерлінгів) за найсерйозніші порушення і 2% (мінімум 10 мільйонів фунтів стерлінгів) за менш серйозні, з щоденними штрафами до 100 000 фунтів стерлінгів за тривалі порушення. Регулюючі органи будуть відшкодовувати свої витрати на нагляд у повному обсязі за рахунок періодичних зборів.

Державний секретар матиме право видавати заяву про стратегічні пріоритети, яких повинні дотримуватися всі 13 регуляторних органів, керувати конкретними діями під час серйозних інцидентів (включаючи тимчасову ізоляцію мережі) та швидко включати додаткові сектори до сфери дії або оновлювати вимоги безпеки за допомогою вторинного законодавства…

Для підприємств цей законопроект є стратегічним поворотом, а не простою вимогою дотримання норм. Організаціям настійно рекомендується негайно провести аудит ланцюгів постачання, включити нові кіберзобов'язання в контракти, переглянути плани реагування на інциденти з урахуванням 24-годинного терміну повідомлення, розробити протоколи щодо програм-вимагачів, вдосконалити можливості виявлення та SOC, а також інтенсифікувати навчання персоналу. Оскільки закон має набути чинності в 2026 році, а потім будуть прийняті детальні вторинні законодавчі акти та кодекси практики, зараз необхідно завчасно та ретельно підготуватися, щоб відповідати більш жорстким і проактивним вимогам Великобританії щодо кіберстійкості». ***(Patrick Arben, Loretta Pugh, Jocelyn Paulley, Amber Strickland and Louise Macdonald. The UK Cyber Security and Resilience Bill and what it means for your business // Gowling WLG (https://gowlingwlg.com/fr/insights-resources/articles/2025/the-uk-cyber-security-and-resilience-bill-and-what-it-means-for-your-business). 13.11.2025).***

***

«Великобританія готується запровадити нові суворі закони про кібербезпеку, які змусять тисячі середніх і великих постачальників керованих послуг — компаній, що надають послуги з управління IT, технічної підтримки, кібербезпеки та інші критично важливі послуги як державному, так і приватному сектору — дотримуватися суворих стандартів безпеки та підкорятися прямому державному регулюванню…

Цей крок був зроблений після низки гучних атак у 2024 та 2025 роках, серед яких злом системи нарахування заробітної плати Міністерства оборони, інцидент, що призвів до скасування понад 11 000 прийомів та процедур у Національній службі охорони здоров'я, а також атаки програм-вимагачів, що паралізували роботу компаній Marks & Spencer, Co-op та Jaguar Land Rover.

За пропонованим режимом, ці «критично важливі сторонні постачальники» будуть зобов'язані без затримки повідомляти уряд та своїх клієнтів про значні кіберінциденти, впроваджувати надійні плани реагування на інциденти та підкорятися нагляду з боку регуляторних органів, які отримають нові повноваження призначати важливих постачальників та накладати більш суворі штрафи за серйозні порушення…

Паралельно уряд законодавчо заборонить усім органам державного сектору та операторам критичної національної інфраструктури, включаючи Національну службу охорони здоров'я, місцеві ради та школи, виплачувати викуп кіберзлочинцям, усунувши лазівку, яка спонукала зловмисників атакувати британські установи». ***(UK plans tougher laws to protect public services from cyberattacks // Reuters (https://www.reuters.com/world/uk/uk-plans-tougher-laws-protect-public-services-cyberattacks-2025-11-12/). 13.11.2025).***

***

«19 листопада 2025 року Європейська комісія оприлюднила комплексний законодавчий пакет «Digital Omnibus», спрямований на спрощення цифрового управління та стимулювання інновацій шляхом зменшення регуляторної складності для підприємств ЄС. Центральною пропозицією є створення єдиної точки входу для повідомлення про інциденти в сфері кібербезпеки, уніфікованого порталу, який дозволить компаніям виконувати всі зобов'язання щодо повідомлення відповідно до таких нормативних актів, як NIS2, GDPR та DORA, одночасно, а не через окремі, дублюючі звіти…

Пакет також передбачає цільові поправки до Закону про штучний інтелект (AI Act) з метою забезпечення балансу між інноваціями та безпекою. Основні зміни включають прив'язку термінів впровадження правил щодо штучного інтелекту високого ризику до наявності інструментів підтримки, поширення спрощень у сфері дотримання вимог на малі та середні компанії, а також дозвіл на обробку даних особливої категорії для виявлення упередженості. Пакет також централізує нагляд за моделями штучного інтелекту загального призначення під егідою Управління з питань штучного інтелекту та розширює можливості для регуляторних пісочниць.

Крім того, Digital Omnibus прагне покращити доступ до даних шляхом консолідації правил ЄС щодо даних за допомогою Закону про дані, надання пільг для малих і середніх підприємств та запровадження типових договірних умов для стимулювання інновацій у сфері штучного інтелекту. Інші важливі пропозиції включають цільові поправки до GDPR, такі як продовження терміну повідомлення про порушення безпеки даних з 72 до 96 годин та уточнення правил використання персональних даних у навчанні штучного інтелекту. Він також модернізує правила згоди на використання файлів cookie, щоб зменшити частоту банерів та дозволити управління одним кліком через налаштування браузера. Пакет, доповнений

Стратегією Союзу даних та пропозицією щодо Європейського бізнес-гаманця, тепер буде розглянуто Європейським парламентом та Радою для прийняття…» ***(EU Digital Omnibus Introduces a Single Reporting Point for Cybersecurity Incidents // National Law Forum, LLC (https://natlawreview.com/article/eu-digital-omnibus-introduces-single-reporting-point-cybersecurity-incidents). 20.11.2025).***

***

«Університет Борнмута отримав грант від Управління у справах студентів у розмірі 2,3 млн фунтів стерлінгів на створення Центру кіберкомпетентності, метою якого є усунення регіональних і національних прогалин у кібернавичках. Проект передбачає модернізацію існуючих приміщень і до березня 2026 року запуск «Центру безпеки майбутнього» на базі штучного інтелекту, де студенти разом з партнерами з галузі, такими як Battle Lab, ESET і JPMorgan, будуть практикувати виявлення та реагування на реалістичні кібератаки. Центр також буде надавати підтримку у сфері психічного здоров'я для боротьби з вигоранням серед кіберфахівців…

Окрім навчальних програм, співробітники університету та студенти будуть пропонувати місцевим підприємствам та громадськості навчальні табори, тренінги під керівництвом роботодавців та короткі курси через Dorset Digital Skills Partnership, зміцнюючи кіберстійкість у графстві, де майже всі підприємства є малими та середніми. Керівництво університету заявляє, що центр сприятиме зміцненню кадрового потенціалу у сфері кібербезпеки у Великій Британії, підтримуючи економічне зростання та відповідаючи національним цілям промислової стратегії…

Центр планується відкрити в березні 2026 року». ***(Bournemouth University receives £2.3 million to boost regional and national cyber security // Bournemouth University (https://www.bournemouth.ac.uk/news/2025-11-19/bournemouth-university-receives-23-million-boost-regional-national-cyber-security). 19.11.2025).***

***

«…Економічна та національна безпека Великої Британії все більше загрожується кібератаками, проте фундаментальні ринкові збої залишаються, заявляє Комітет з питань бізнесу та торгівлі парламенту Великої Британії. У новому звіті депутати ставлять кіберризики вище за кліматичні зміни та наводять приклади нещодавніх інцидентів, що завдали збитків на мільйони фунтів, таких як злом Jaguar Land Rover на суму 2 млрд євро, щоб продемонструвати масштаби потенційних збитків. Вони закликають уряд вжити заходів у трьох напрямках:

1. Ввести відповідальність постачальників програмного забезпечення.

• Сьогодні незахищений код перекладає приховані витрати на користувачів; змусивши розробників взяти на себе ці витрати, можна буде інтерналізувати «негативні зовнішні ефекти» та стимулювати практику забезпечення безпеки на етапі проектування.

• Комітет хоче, щоб добровільні рекомендації Національного центру кібербезпеки щодо безпечного кодування стали обов'язковими та підлягали примусовому виконанню з накладенням штрафів.

• Цей крок протидіє лобіюванню з боку галузі (наприклад, Microsoft, AWS), яке попереджає, що відповідальність може гальмувати інновації…

2. Стимулювання інвестицій у кіберстійкість.

• Оскільки оновлення тепер здійснюються через підписку на SaaS, вони не підпадають під податкові пільги на капітальні витрати. Члени парламенту рекомендують внести зміни до режиму, щоб поточні витрати на безпеку, такі як функції багатофакторної автентифікації, також підпадали під пільги.

3. Ввести обов'язкове повідомлення про інциденти.

• Великі британські компанії не зобов'язані повідомляти про кібератаки, що не дозволяє уряду та галузі отримати реальне уявлення про загрози. Комітет закликає до обов'язкового повідомлення про всі зловмисні інциденти, а не тільки про випадки використання програм-вимагачів, щоб скласти точну картину ситуації в країні…

У звіті також підкреслюється «кіберрозрив»: малі та середні підприємства мають слабший контроль і нижчий рівень страхового покриття, ніж великі підприємства, що робить їх слабкими ланками ланцюга поставок. Члени парламенту відзначають кроки ЄС і США (Закон ЄС про кіберстійкість, дебати в США щодо відповідальності) і попереджають, що Великобританія повинна йти в ногу з ними, інакше ризикує стати системно вразливою». ***(Alexander Martin. Software companies must be held liable for British economic security, say MPs // Recorded Future News (https://therecord.media/software-companies-liable-britain-security). 24.11.2025).***

***

«Новий звіт Комітету з питань бізнесу та торгівлі Палати громад Великої Британії «На шляху до нової доктрини економічної безпеки» попереджає, що відкрита економіка середнього розміру Великої Британії стає все більш вразливою до «економічної війни», а кібератаки очолюють список загроз. Голова комітету Ліам Бірн заявив, що залежність від іноземного капіталу, технологій та власності в поєднанні з низьковитратною кібератакою на основі штучного інтелекту робить нинішні засоби захисту «непридатними для майбутнього»…

У звіті перераховано 10 основних ризиків для економічної безпеки та понад 100 разів згадуються кіберзагрози. У ньому зазначається, що нещодавні атаки на критичну національну інфраструктуру та компанії (такі як інцидент з Jaguar Land Rover на суму 1,9 млрд фунтів стерлінгів) показують, як одне порушення може паралізувати діяльність компаній, споживачів та ланцюгів постачання. Члени парламенту стверджують, що «економічна безпека не може бути досягнута без кібербезпеки», і закликають до значного посилення оборони Великобританії…

Основні рекомендації включають:

• Перетворити добровільний Кодекс практики безпеки програмного забезпечення уряду на закон і надати регуляторним органам повноваження для забезпечення його дотримання.

• Розширити податкові пільги на витрати на ІТ, що підвищують оперативну стійкість, включаючи програмне забезпечення для кібербезпеки, оновлення застарілих систем та інструменти захисту даних.

• Провести консультації щодо обов'язкової системи повідомлення про кіберінциденти, яка замінить нинішню систему, що є переважно добровільною…»

(Phil Muncaster. Mounting Cyber-Threats Prompt Calls For Economic Security Bill // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news/mounting-cyber-threats-economic/). 25.11.2025).

***

«…Глобальні оцінки за 2025 рік показують, що лише кілька країн встановлюють стандарти кіберстійкості на національному рівні. Глобальний індекс кібербезпеки Міжнародного союзу електрозв'язку та Національний індекс кібербезпеки враховують шість факторів — правові рамки, технічні засоби контролю, централізовану координацію, потенціал робочої сили, а також внутрішнє та міжнародне співробітництво — для оцінки готовності…

• Чехія очолює рейтинг NCSI (98,3/100), що відображає два десятиліття інтегрованої політики, стійкої інфраструктури та сильної міжгалузевої координації.

• Фінляндія, яка вже давно є лідером GCI, поєднує суворі закони зі зрілою національною структурою CERT та навчаннями, які забезпечують безперебійну роботу служб навіть під час атак, пов'язаних з державою.

• Національний центр кібербезпеки Великої Британії, широке регулювання та зростаючий бюджет дозволяють їй залишатися в світовій еліті.

• Німеччина різко збільшила фінансування та посилила свою правову та технічну базу, визнаючи свою економічну вагу та вразливість критичної інфраструктури.

• Багато країн Північної Європи та Західної Європи також займають високі позиції завдяки стабільним інвестиціям, державно-приватній співпраці та обов'язковим режимам повідомлення про інциденти…

Загальні фактори успіху: цілісні, довгострокові стратегії, а не ситуативні рішення; стабільне фінансування; сучасні, ефективні закони про кібербезпеку; офіційні мережі обміну інформацією; постійна адаптація до загроз, пов'язаних із штучним інтелектом, програм-вимагачів та атак на ланцюги постачання…

Навіть найкраще підготовлені країни стикаються з нестачею кваліфікованого персоналу, швидко розвиваються методи атак і зберігаються вразливі місця в енергетичних, водопостачальних і телекомунікаційних мережах. Пріоритети на період після 2026 року включають поглиблення співпраці між державним і приватним секторами, виявлення на основі розвідданих, планування відновлення та забезпечення стійкості, а також більш широкий обмін даними між країнами. Для країн, що відстають, урок очевидний: послідовні інвестиції та скоординована національна стратегія можуть значно знизити кіберризики». ***(Naveen Goud. Which Countries Stood Out for Strong Cyber-Defenses in 2025 // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/which-countries-stood-out-for-strong-cyber-defenses-in-2025/). 11.2025).***

***

«Національний центр кібербезпеки Великобританії (NCSC) повідомляє, що кількість інцидентів, у вирішенні яких він брав участь з вересня 2024 року по серпень 2025 року, практично не змінилася (429), але їх вплив різко зріс: 204 інциденти були класифіковані як «важливі на національному рівні» (категорія

2 або 3) проти 89 у попередньому році, а кількість «надзвичайно значущих» випадків зросла на 50 % до 18. У відповідь на це NCSC змінив свою стратегію з чистої профілактики на «інженерію стійкості»…

Ключові елементи цього підходу:

• Розробка систем для миттєвого відновлення за допомогою Infrastructure-as-Code та незмінних офлайн-резервних копій.

• Стримування зловмисників за допомогою сегментації, доступу за принципом «нульової довіри», захищених робочих станцій адміністраторів та суворих заходів контролю з мінімальними привілеями.

• Проведення навчань з хаос-інженерії та повномасштабних тестів відновлення; моніторинг та реєстрація всіх подій.

• Запуск критично важливих служб у дубльованих, незалежних середовищах, щоб можна було миттєво перейти на резервне джерело…

Мета полягає не тільки в тому, щоб вижити в умовах кризи, але й стати «антикрихким», зміцнюючи захист після кожного інциденту.

Заходи підтримки включають:

• Активна кіберзахист (ACD): автоматичне, масштабне блокування загроз для зареєстрованих організацій.

• Навчання з кіберуправління, щоб допомогти радам директорів застосовувати новий Кодекс практики кіберуправління.

• Просування програми Cyber Essentials для зміцнення партнерів у ланцюжку поставок…

NCSC закликає ради директорів та керівників IT-відділів визнати, що порушення безпеки є неминучими, і впровадити інженерію стійкості поряд із традиційним управлінням ризиками, щоб критично важливі служби Великобританії могли продовжувати працювати та швидко відновлюватися навіть у разі прориву початкових захисних систем під час серйозних кібератак». ***(Josh Breaker-Rolfe. What Did We Learn from the NCSC's 2025 Annual Review? // Fortra, LLC (https://www.tripwire.com/state-of-security/what-learn-ncsc-2025-annual-review). 21.11.2025).***

***

«Зіткнувшись із різким зростанням кількості ворожих хакерських атак та дезінформаційних кампаній, Швеція доручила своєму національному агентству з кібербезпеки розробити більш надійні засоби захисту до загальних виборів, запланованих на 13 вересня 2026 року. Міністр цивільної оборони Карл-Оскар Болін заявив, що країна переживає «серйозну ситуацію з безпекою» і що загрози в кіберпросторі «зростають, і Швеція далеко не в безпеці». Агентство має оцінити поточні ризики, запропонувати нові контрзаходи та провести кібернавчання, а до березня 2026 року подати попередній звіт до міністерства оборони…

Європейські вибори неодноразово зазнавали зривів через деструктивні кібероперації, часто пов'язані з Росією: Румунія скасувала результати президентських виборів у грудні минулого року після втручання Росії, а Молдова нещодавно звернулася за допомогою до ЄС після кібератак на свою виборчу інфраструктуру, які, як вважається, були здійснені Москвою. Швеція сподівається,

що завчасна підготовка запобіжить подібним зривам під час майбутніх виборів…» ***(Sam Clark. Sweden braces for election hacks ahead of 2026 vote // Politico (https://www.politico.eu/article/sweden-braces-for-election-hacks-ahead-of-2026-vote/). 21.11.2025).***

***

Австралія та Нова Зеландія

«Новий план кібервідповіді Австралії, опублікований у червні 2025 року, посилює національне кризове управління шляхом додавання четвертого рівня — «Координація дій у разі катастрофічних інцидентів національного масштабу» — для реагування на надзвичайно складні кіберінциденти, що мають екстремальні міжюрисдикційні наслідки для критичної інфраструктури, державних активів та даних. Хоча це є позитивним кроком, це лише початок; пріоритетом має бути проактивна стійкість, щоб план не довелося активувати. Для цього необхідна оцінка загрози національних катастрофічних кіберінцидентів з метою кількісної оцінки ризиків і ймовірностей, узагальнення розвідувальної інформації та оперативних даних від уряду та промисловості (громадська безпека, охорона кордонів, критична інфраструктура, економічна безпека) та інформування державного і приватного секторів про найнагальніші загрози…

Озброївшись надійною оцінкою, Австралія може ідентифікувати та пріоритезувати ризики; визначати та формувати необхідні можливості; розробляти, координувати та підтримувати плани готовності; а також перевіряти їх шляхом регулярних навчань та моделювань, з постійним переглядом та оновленням. Ілюстративні сценарії планування повинні моделювати ймовірні кіберкатастрофи, такі як складний напад на енергетичну мережу, порушення роботи якої може спричинити ланцюгову реакцію у сферах водопостачання, охорони здоров'я, фінансів, виробництва, роздрібної торгівлі та транспорту, що потенційно може паралізувати економіку на рік або більше і навіть підірвати зусилля з реагування. Планування готовності також повинно відображати взаємозалежності мереж, щоб запобігти або пом'якшити шкідливі ланцюгові ефекти…

Національна система готовності повинна дотримуватися дисциплінованого циклу: виявлення та оцінка ризиків; оцінка потреб у можливостях; створення та підтримка можливостей (з пріоритетом найвищих ризиків); планування та координація реалізації серед усіх зацікавлених сторін; перевірка за допомогою навчань; та регулярний перегляд і оновлення. Кінцевою метою є кіберстійкість — здатність запобігати, де це можливо, але, що більш важливо, адаптуватися, відновлюватися та підтримувати діяльність у непередбачених або швидко мінливих умовах. Регулярні кібернавчання дозволяють перевірити плани та сформувати адаптивні можливості, що визначають справжню стійкість. Структура рівня 4 свідчить про прогрес; тепер Австралія повинна завершити цю роботу, запровадивши комплексну Національну систему планування кіберготовності, засновану на ретельній оцінці загроз та постійному розвитку можливостей». ***(Gary Waters. Preparing for cyberattacks is good; preventing them is better // The Australian Strategic***

Policy Institute (https://www.aspistrategist.org.au/preparing-for-cyberattacks-is-good-preventing-them-is-better/). 03.11.2025).

***

«Австралійські підприємства працюють із серйозною «сліпою плямою в кібербезпеці», попереджає місцева консалтингова компанія OutsourcedCISO. Загальнонаціональний дефіцит кваліфікованих керівників з інформаційної безпеки, поєднаний з обмеженими бюджетами на найм персоналу та низьким рівнем кіберграмотності на рівні керівництва та ради директорів, означає, що багато організацій не мають стратегічних рекомендацій з безпеки, поки серйозне порушення не змушує їх витратити кошти. Засновник компанії Максим Куссо каже, що зазвичай компанії виділяють кошти лише після втрати довіри клієнтів і різкого зростання витрат на відновлення — набагато більше, ніж вимагали б проактивні інвестиції…

Ця прогалина стає все більш небезпечною, оскільки Канберра посилює правила щодо конфіденційності та повідомлення про порушення відповідно до Закону про конфіденційність Співдружності, а зловмисники активізують атаки на основі штучного інтелекту. У щорічній оцінці загроз ASIO за 2025 рік зазначається, що протягом останнього року австралійська інфраструктура неодноразово ставала об'єктом атак. Без чітких вказівок від CISO швидкозростаючі компанії намагаються розробити стратегії безпеки, визначити пріоритети усунення недоліків, задовольнити стандарти відповідності та оцінити рентабельність інвестицій у наявні засоби захисту, що призводить до фрагментованих, реактивних рішень та підвищеного регуляторного ризику.

OutsourcedCISO позиціонує свою модель «часткового CISO» як засіб вирішення проблеми, пропонуючи стратегію, управління та підтримку у сфері дотримання нормативних вимог на рівні підприємства — відповідно до таких стандартів, як ISO 27001 та SOC 2 — за частку вартості та часу, необхідних для найму постійного керівника. Куссо стверджує, що доступне, досвідчене керівництво є зараз необхідним, якщо австралійські організації хочуть побудувати стійкість, виконати нові юридичні зобов'язання та зберегти довіру клієнтів до того, як відбудеться наступне порушення…» ***(Gordon Peters. Australian organisations face a 'concerning cybersecurity leadership gap'// iTWire (https://itwire.com/business-it-news/security/australian-organisations-face-a-%E2%80%98concerning-cybersecurity-leadership-gap%E2%80%99.html). 19.11.2025).***

***

«Хвиля вторгнень у ланцюги постачання викрила серйозні вразливості в оборонних програмах Австралії…

• Група хакерів Cyber Toufan, що спеціалізується на викраденні та оприлюдненні конфіденційної інформації, стверджує, що протягом 18 місяців працювала всередині ізраїльської субпідрядної компанії MAYA Technologies, викравши «десятки терабайтів» інформації з 17 оборонних компаній, включаючи постачальника башт Elbit. В середині листопада група опублікувала 3D-візуалізації

та інші технічні деталі програми австралійської армії з розробки бойової машини піхоти Redback вартістю 7 мільярдів доларів…

• Окремо, група хакерів-вимагачів «J Group» заявляє, що протягом п'яти місяців перебувала в мережі компанії IKAD Engineering, розташованої в Перті, яка постачає компоненти для фрегатів класу «Хантер» і підводних човнів класу «Коллінз», після того як зламала стару VPN. Група хвалиться, що викрала 800 ГБ тендерних документів, файлів відділу кадрів та електронних листів і «могла б створити музей корпоративних таємниць». Генеральний директор IKAD підтверджує факт порушення, але наполягає, що були викрадені лише «неконфіденційні» дані та записи про персонал і що компанія не має прямого зв'язку з мережами ADF…

Аналітики з питань безпеки попереджають, що навіть на перший погляд нешкідливі технічні дані — імена файлів, відносини з постачальниками, технічні креслення — мають стратегічне значення, оскільки допомагають супротивникам створювати більш переконливі кампанії з фішингу та складати карту військової екосистеми Австралії. Етичний хакер Джеймісон О'Рейлі називає цей інцидент «прикладом впливу на ланцюжок поставок: зловмисники атакують найслабшу ланку, а не головного підрядника».

Австралійський центр кібербезпеки, Федеральна поліція та Програма безпеки оборонної промисловості проводять розслідування. Генеральний директор ASIO Майк Берджес неодноразово попереджав, що кілька іноземних держав, зокрема Китай та Іран, посилюють шпигунство проти критичної інфраструктури та ланцюга поставок оборонної промисловості Австралії. Аналітик CyberCX Кетрін Манстед зазначає, що тактика Cyber Toufan нагадує «хактивізм», пов'язаний з іранською державою, тоді як J Group, здається, керується фінансовими мотивами…

Відставний генерал-майор Маркус Томпсон, колишній керівник відділу інформаційної війни Міністерства оборони, заявляє, що Міністерство оборони повинно «тримати підрядників у тонусі», оскільки «сильна ланка визначається найслабшою ланкою». Він та інші експерти закликають до запровадження більш суворих стандартів безпеки, постійного моніторингу та кращого обміну інформацією про загрози в усій оборонно-промисловій базі, щоб запобігти порушенням у майбутньому». ***(Annika Burgess. Australia's weapons programs exposed in defence industry cyber attacks // ABC (https://www.abc.net.au/news/2025-11-19/defence-cyber-attacks-adf-military-projects-redback-hackers/105999222). 18.11.2025).***

***

«Дані про свободу інформації показують, що з 2018 року гірничодобувні та виробничі компанії Австралії зареєстрували щонайменше 187 повідомлень про порушення, в результаті яких було розкрито особисту інформацію про 3,6 мільйона осіб, проте багатьом компаніям знадобилося кілька місяців, а іноді й більше року, щоб виявити вторгнення, і ще місяць або більше, щоб повідомити про це регуляторні органи. Один оператор виявив порушення через 520 днів після його початку і чекав ще 84 дні, перш ніж повідомити про це Управління австралійського комісара з питань інформації (OAIC); в середньому жертви

затримували повідомлення на 39 днів після виявлення. Сім інцидентів перевищили повний рік від моменту порушення до повідомлення OAIC…

Оскільки формулювання «як тільки це буде можливо» в Законі про конфіденційність не встановлює фіксованого терміну, компанії можуть вільно тлумачити зобов'язання щодо звітності, зазначає директор Центру кібербезпеки Університету Маккуорі Далі Каафар, який закликає встановити чіткі терміни та більш чіткі пороги. Затримки розширюють можливості зловмисників для збору облікових даних, викрадення даних або розгортання програм-вимагачів, що збільшує витрати на відновлення та шкоду для суспільства.

Хоча гірники та виробники рідко мають справу безпосередньо зі споживачами, вони зберігають великі масиви даних про співробітників та підрядників: 53% випадків порушення безпеки стосувалися фінансових даних, 40% — податкових номерів та 88% — контактної інформації. Більше 90% випадків були зловмисними, а найбільшою причиною було використання програм-вимагачів; виявлення порушень, пов'язаних із шкідливим програмним забезпеченням, займало в середньому 146 днів…

Архітектор безпеки Secolve Ріана Кук попереджає, що ці цифри є «досить тривожними», зазначаючи, що супротивники — від геополітичних акторів до опортуністичних банд — вважають майнінг прибутковим і націлилися на австралійські компанії, оскільки санкції проти Росії збільшили попит на австралійські ресурси. Вона додає, що атаки на операційні технології (OT) — вантажівки, роботи, дамби — часто не повідомляються, якщо вони не стосуються особистих даних, незважаючи на потенційно «страшні» наслідки.

Експерти закликають до введення більш суворих і прозорих правил: фіксованих термінів повідомлення, обов'язкового повідомлення про інциденти в позаробочий час, обміну інформацією про загрози в режимі реального часу між різними галузями та скорочення обсягу непотрібного зберігання даних. Федеральний уряд переглядає закони про повідомлення про порушення в рамках своєї Стратегії кібербезпеки на 2023-2030 роки, а OAIC запустив публічну інформаційну панель для основних секторів, хоча гірничодобувна та виробнича галузі до неї ще не включені…» ***(FOI data shows Australian mining and manufacturing sectors take months to detect cyber breaches // ABC (https://www.abc.net.au/news/2025-11-20/delays-detecting-data-breaches-australian-mining-manufacturing/105978234). 19.11.2025).***

***

«У Новій Зеландії переважна більшість кібератак ніколи не стає надбанням громадськості, тому керівники підприємств і страхові компанії приймають рішення щодо безпеки, маючи в своєму розпорядженні, можливо, лише десяту частину реальних даних. Керівник служби інформаційної безпеки NSP Джорді Стюарт (Geordie Stewart) вважає, що на кожний інцидент, про який повідомляють або висвітлюють ЗМІ, припадає щонайменше десять інших, які вирішуються тихо — внутрішньо, за допомогою приватних компаній, що реагують на інциденти, або шляхом таємних виплат викупу. Організації обирають мовчання, щоб уникнути значних фінансових втрат і шкоди репутації, які зараз спричиняють

публічні порушення: Звіт Aon про кіберризики на 2025 рік показує, що після серйозних інцидентів акціонерна вартість в середньому падає на 27 %, а останнє опитування Beazley показує, що кібербезпека є головним питанням для 29 % керівників…

Зокрема, програми-вимагачі маскуються під шести- та семизначними виплатами, які здійснюються під тиском з метою відновлення критично важливих для бізнесу систем; три чверті опитаних австралійських та новозеландських компаній визнають, що здійснювали такі виплати, зазвичай через професійних перемовників. Оскільки про ці транзакції та багато інших порушень не повідомляється CERT NZ, загальна картина загроз у країні є сильно спотвореною, а також панує «хибне відчуття безпеки»…

Недостатнє інформування найсильніше вражає малі та середні підприємства. Більше половини малих та середніх підприємств Нової Зеландії стикалися з кіберзагрозами протягом останніх шести місяців, що на 36% більше, ніж у попередньому періоді, проте їм бракує інформації від колег, яка б допомогла їм організувати захист. Реальні аналізи порушень показують, що більшість інцидентів спричинені невеликим набором типових вразливостей; без належної видимості малі та середні підприємства не можуть ефективно розставити пріоритети у виправленні недоліків.

Приховані порушення спотворюють ціни на страхування, перешкоджають інвестиціям у стійкість та роблять економіку більш вразливою, ніж це випливає з офіційних даних». ***(Roxanne Libatique. Most cyberattacks on NZ businesses stay hidden from public view // KM Business Information NZ (https://www.insurancebusinessmag.com/nz/news/cyber/most-cyberattacks-on-nz-businesses-stay-hidden-from-public-view-557636.aspx). 25.11.2025).***

***

Китай, Індія та країни Індо-тихоокеанського регіону

«28 жовтня 2025 року Китай прийняв перші поправки до Закону про кібербезпеку (CSL) 2016 року, що свідчить про посилення контролю та розширення нагляду за штучним інтелектом, які набудуть чинності з 1 січня 2026 року. Зміни передбачають різке збільшення штрафів: за загальні зобов'язання з кібербезпеки (наприклад, технічний контроль, реагування на інциденти) максимальні штрафи зростають до 10 млн юанів для операторів критичної інформаційної інфраструктури (з 1 млн юанів) і до 2 млн юанів для non-CIIO (critical information infrastructure operators, “CIIO“ (з 100 000 юанів), причому тепер відповідальність несуть навіть ті, хто порушив закон вперше. Штрафи за порушення контролю за контентом (наприклад, за невиконання вимог щодо припинення передачі, видалення незаконного контенту, збереження записів або повідомлення) зростають до 10 млн юанів (з 500 000 юанів)… Штрафи за незаконні послуги з кібербезпеки, такі як несанкціонована сертифікація, тестування, оцінка ризиків або розкриття інформації про помилки/атаки, також зростають з 100 000 до 1 мільйона юанів. Нові санкції спрямовані на постачальників критичного мережевого

обладнання та спеціалізованих продуктів кібербезпеки, які не відповідають обов'язковим стандартам або сертифікації, включаючи штрафи до 100 000 юанів або 1–5-кратного розміру незаконного прибутку, залежно від того, яка сума більша, а також нефінансові заходи (призупинення діяльності, анулювання дозволу/ліцензії). Користувачі також повинні стежити за відповідністю ланцюга поставок: невідповідні продукти або послуги можуть бути вилучені з обігу, що призведе до порушення роботи, а СІІО можуть бути оштрафовані на суму до 10-кратного розміру вартості придбання певних невідповідних товарів. Екстериторіальна сфера застосування закону розширюється від закордонної діяльності, що завдає шкоди критичній інформаційній інфраструктурі Китаю, до будь-якої закордонної діяльності, що завдає шкоди кібербезпеці Китаю. Водночас поправки кодифікують пом'якшувальні та звільняючі від відповідальності фактори відповідно до Закону про адміністративні покарання та дискреційних критеріїв САС, наприклад, необхідне пом'якшення за добровільне виправлення, примус/спонукання, саморозкриття або співпрацю; а також потенційні звільнення від відповідальності за перші, незначні, оперативно виправлені порушення. Нова загальна стаття про штучний інтелект зобов'язує державу посилити етичні норми, моніторинг та оцінку ризиків, а також нагляд за безпекою, прокладаючи шлях для подальшого регулювання штучного інтелекту. Разом із нещодавно скороченими строками повідомлення про інциденти, ці зміни свідчать про посилення контролю: організації в Китаї — та закордонні суб'єкти, що здійснюють діяльність, пов'язану з Китаєм, — повинні посилити програми та заходи контролю, щоб відповідати більш суворим вимогам щодо дотримання нормативних вимог…» ***(Carolyn Bigg, Qiuyang Zhao, Amanda Ge. CHINA: Amendments to Cybersecurity Law Effective 1 January 2026 // DLA Piper (https://privacymatters.dlapiper.com/2025/11/china-amendments-to-cybersecurity-law-effective-1-january-2026/). 03.11.2025).***

***

«…Сінгапур посилив свою систему національної безпеки, внісши поправки до Закону про кібербезпеку 2018 року, які набудуть чинності 31 жовтня 2025 року. Хоча первинний закон був зосереджений на захисті «критичної інформаційної інфраструктури» (CII), такої як енергетика, транспорт і системи охорони здоров'я, поправка до закону 2024 року розширює як визначення CII, так і повноваження комісара з кібербезпеки…

По-перше, комісар тепер може призначити CII будь-яку сторонню або віртуальну комп'ютерну систему, розташовану в Сінгапурі або за кордоном, якщо вона має важливе значення для надання необхідних послуг. Власники CII повинні надати детальну інформацію про конструкцію та використання системи на запит; відмова може спричинити штраф у розмірі до 100 000 сінгапурських доларів, два роки позбавлення волі та щоденні штрафи, а комісар може наказати відключити систему.

По-друге, закордонні системи можуть бути позначені як «CII, що належать провайдеру», якщо їх втрата може порушити роботу критично важливої послуги в Сінгапурі, що підпадає під повний режим дотримання вимог Закону…

По-третє, правила повідомлення про інциденти стали більш суворими. Оператори CII повинні протягом двох годин повідомляти Агентство з кібербезпеки (CSA) про будь-яку підозру на діяльність, пов'язану з просунутими постійними загрозами, або про будь-який інцидент, що порушує роботу важливих служб, навіть якщо він стався в непідключеній системі, яку вони контролюють…

По-четверте, нова категорія — «Система тимчасової кібербезпеки» (STCC) — охоплює державні або приватні системи, які стикаються з короткостроковими ризиками з високими ставками (виборчі платформи, мережі розподілу вакцин тощо). Після призначення власники STCC повинні вжити певних заходів безпеки, пройти затверджені аудити та повідомляти про інциденти, інакше їм загрожують такі самі штрафи в розмірі 100 000 SGD за два роки.

Основні додаткові реформи, що стосуються «організацій, які мають особливе значення для кібербезпеки», та постачальників «основної цифрової інфраструктури», будуть впроваджені пізніше, але дата початку 2025 року вже сигналізує про значний перехід від статичного захисту, заснованого на активах, до динамічного нагляду, заснованого на місії. Організації, системи яких можуть підпадати під ці нові позначення, повинні вже зараз оновити свої політики безпеки, плани реагування на інциденти та процедури звітності, щоб залишатися у відповідності до вимог…» ***(Charmian Aw and Ciara O'Leary. Provisions in Singapore's Cybersecurity (Amendment) Act came into force on 31 October 2025 // Hogan Lovells (https://www.hoganlovells.com/en/publications/provisions-in-singapores-cybersecurity-amendment-act-came-into-force-on-31-october-2025). 04.11.2025).***

***

«На конференції National Cybersecurity Connect 2025 в Індонезії глава Національного агентства з кібербезпеки (BSSN) Нугрохо Сулістіо Буді заявив, що сильна кіберстійкість є основою бурхливого розвитку цифрової економіки країни, обсяг якої, за прогнозами, досягне 120 мільярдів доларів. Хоча таке зростання позиціонує Індонезію як нову економічну потугу, Буді попередив, що воно також збільшує вразливість до кіберзагроз, зазначивши, що багато галузей промисловості ставлять ефективність вище за безпеку…

Буді підкреслив, що 90% кібератак в Індонезії пов'язані з шкідливим програмним забезпеченням, а фішинг та соціальна інженерія на основі штучного інтелекту стають все більш витонченими. Він наголосив, що формування культури обізнаності про кібербезпеку є настільки ж важливим, як і впровадження технологій, та окреслив три основні аспекти стійкості: конфіденційність, цілісність та доступність. Для зміцнення своєї безпеки Буді закликав Індонезію прагнути технологічної незалежності та не покладатися на іноземні ліцензії чи обладнання, які можуть заважати її цифровому суверенітету.

Підтримуючи цю думку, міністр креативної економіки Теуку Ріфкі Харсія закликав Індонезію стати виробником, а не лише споживачем технологій цифрової безпеки. Він висловив впевненість у місцевих талантах і підкреслив роль міністерства у підтримці таких стартапів, як Peris.AI, для розробки власних рішень, здатних конкурувати на світовому рівні…» ***(Ghita Permatasari. Cyber resilience the***

foundation for Indonesia's thriving digital economy // Clarion Events Pte Ltd (https://govinsider.asia/intl-en/article/cyber-resilience-the-foundation-for-indonesias-thriving-digital-economy). 06.11.2025).

***

«В'єтнам робить автономність кібербезпеки головним національним пріоритетом, оскільки його урядові, фінансові, енергетичні, транспортні, медичні та телекомунікаційні системи стають все більш цифровими і все більше піддаються масштабним кібератакам, включаючи кампанії з використанням програм-вимагачів, масове шифрування даних та вторгнення, які в деяких випадках мають ознаки державної підтримки. Лідери країни розуміють, що значна залежність від іноземних інструментів кібербезпеки, вихідний код, алгоритми та потенційні приховані механізми збору даних яких вони не контролюють, робить країну реактивною та вразливою в кризових ситуаціях і створює ризик витоку конфіденційної національної інформації. У відповідь на це Закон про кібербезпеку 2025 року зобов'язує державні органи та підприємства надавати пріоритет продуктам безпеки «Make in Vietnam» та розглядати інвестиції в кібербезпеку як важливу інфраструктуру, нарівні з електроенергією чи водопостачанням, створюючи внутрішній ринок для в'єтнамських брандмауерів, систем виявлення вторгнень, моніторингу поведінки та аналітичних рішень, адаптованих до місцевих потреб…

Стратегія В'єтнаму щодо самозабезпечення в галузі кібербезпеки базується на трьох основах: локалізована розробка продуктів, кваліфіковані кадри та вибіркове, але суверенне міжнародне співробітництво. Керівники кібербезпеки, відповідальні за основні інформаційні системи, тепер повинні мати офіційні сертифікати, що свідчить про очікування, що самі керівники розуміють загрози, а не делегують їх повністю ІТ-персоналу, в той час як країна працює над створенням багаторівневого персоналу з кібербезпеки, здатного запобігати складним атакам і реагувати на них…

Водночас В'єтнам прагне інтегруватися в глобальні мережі збору інформації про загрози, проводити спільні розслідування кіберзлочинів та обмінюватися передовим досвідом, але в рамках правових механізмів, розроблених для збереження національного контролю. Визнаючи, що багато порушень починаються з помилок користувачів, уряд також розширює освіту з питань кібербезпеки в школах, проводить кампанії з підвищення обізнаності громадськості та навчання на робочому місці, щоб громадяни та працівники стали першою лінією захисту від фішингу, слабких паролів та шахрайства. Зрештою, оволодіння власним «цифровим щитом» — від технологій і талантів до інформування громадськості — розглядається не тільки як технічна мета, але й як політична та економічна необхідність для захисту суверенітету даних, прав громадян і критично важливих послуг, а також для того, щоб В'єтнам міг безпечно конкурувати та брати участь у глобальних цифрових ланцюгах створення вартості». ***(Vietnam pushes for cybersecurity autonomy to safeguard its digital sovereignty // VietNamNet Global (https://vietnamnet.vn/en/vietnam-pushes-for-cybersecurity-autonomy-to-safeguard-its-digital-sovereignty-2464376.html). 21.11.2025).***

***

«Фахівці з кібербезпеки є останньою і найважливішою лінією оборони В'єтнаму, проте, за даними Національної асоціації кібербезпеки (NCA) та представників Міністерства громадської безпеки, країна стикається з серйозною нестачею висококваліфікованих експертів, здатних протистояти все більш складним і частим атакам. На конкурсі «Студент кібербезпеки» 2025 року підполковник Тріу Ман Тунг попередив, що ця прогалина загрожує не тільки національній інформаційній інфраструктурі, але й ключовим бізнес-системам. Опитування NCA, проведене в 2024 році, показало, що майже 21% організацій не мають спеціалізованого персоналу з кібербезпеки, а 35,5% мають п'ять або менше таких співробітників, що, за оцінками, призводить до дефіциту близько 700 000 фахівців по всій країні…

Ву Нгок Сон з NCA підкреслив, що технології та процедури самі по собі недостатні без кваліфікованих фахівців — «останнього захисного щита» — і що три основи кібербезпеки — це технології, процеси та людські ресурси. Хоча хакери все частіше використовують штучний інтелект для аналізу викрадених даних і розробки індивідуальних атак, Сон застеріг, що штучний інтелект не може замінити експертів, які знають, як проектувати безпечні архітектури, вибирати безпечні рішення для зберігання даних і підтримувати цілодобовий моніторинг. Він пояснив, що цифра 700 000 відображає необхідність цілодобового покриття, а не абсолютну чисельність персоналу, і запропонував використовувати спільні служби безпеки та інструменти штучного інтелекту для оптимізації людських ресурсів, особливо для невеликих організацій…

Відповідно до національних цілей цифрової трансформації, Міністерство освіти і навчання просуває модель співпраці «три сторони», що об'єднує уряд, університети та промисловість для підготовки фахівців у галузі кібербезпеки, а NCA закликає до розробки стандартизованих сертифікатів та систем оцінки для професіоналізації галузі, встановлення стандартів якості та зміцнення загального потенціалу кіберзахисту В'єтнаму». ***(Vietnam needs 700,000 cybersecurity professionals to meet rising threats // VietNamNet Global (https://vietnamnet.vn/en/vietnam-needs-700-000-cybersecurity-professionals-to-meet-rising-threats-2462077.html). 13.11.2025).***

***

«Експерти у В'єтнамі стверджують, що об'єднання Закону про кібербезпеку 2018 року та Закону про безпеку мережевої інформації 2015 року є необхідним для створення єдиної, узгодженої правової бази, яка зменшить дублювання, поліпшить правозастосування та дозволить йти в ногу з швидкозмінними цифровими загрозами. З моменту підключення до Інтернету 28 років тому В'єтнам реалізує амбітні програми в галузі ІТ та цифрової трансформації, кульмінацією яких стала Резолюція 57-NQ/TW Політбюро від 2024 року про прориви в науці, технологіях, інноваціях та цифровій трансформації…

Однак у міру поглиблення цифровізації у фінансах, енергетиці, телекомунікаціях, уряді та інших критично важливих секторах країна стикається з

дедалі складнішими кібератаками, шпигунством, програмним забезпеченням-вимагачем, витоками даних і поширеним зловживанням персональними даними, а також ворожою пропагандою та кіберзлочинністю, що процвітають у соціальних мережах і на підпільних ринках. Хоча два існуючі закони сприяли зміцненню національної оборони, інституційні реформи відповідно до Резолюції 18-NQ/TW та Декрету 02/2025/ND-CP перенесли відповідальність за інформаційну безпеку мережі з Міністерства інформації та комунікацій до Міністерства громадської безпеки, а саме до його Департаменту кібербезпеки та запобігання високотехнологічним злочинам, який тепер контролює ліцензування, регулювання даних та безпеку мережі. Ця реструктуризація зробила юридичну консолідацію нагальною. Переглянутий проект закону Національної асамблеї, розроблений на основі публічних консультацій та міжвідомчого огляду в рамках прискореної, але повноцінної процедури, об'єднує обидва закони в єдиний закон про кібербезпеку, який поважає існуючі функції відомств, не вводить нових загальних політик і залишає детальне впровадження на розсуд урядових постанов…

Хоча кібербезпека (захист систем та критичної інфраструктури від атак) та інформаційна безпека мережі (забезпечення цілісності та конфіденційності даних під час передачі та обробки) концептуально відрізняються, на практиці вони тісно пов'язані між собою, і об'єднання їх регулювання, як очікується, дозволить усунути конфлікти, оптимізувати операції та створити більш чітке середовище для цифрової економіки. З міжнародної точки зору, консолідований закон також повинен допомогти В'єтнаму більш ефективно співпрацювати в розслідуванні транскордонних кіберзлочинів та обміні інформацією про загрози, одночасно посилюючи захист персональних даних та юридичну ясність для підприємств і громадян. Закон про кібербезпеку 2025 року запроваджує єдину систему визначення та призначає єдиний керівний орган, зосереджується лише на питаннях, що належать до компетенції Національної асамблеї, щоб уникнути процедурної надмірності, та додає кілька важливих положень: обов’язкова ідентифікація IP-адрес інтернет-провайдерами для органів кібербезпеки; спеціальні бюджетні статті для завдань кібербезпеки в державних органах та державних підприємствах; пріоритетність вітчизняних продуктів кібербезпеки для забезпечення технологічної самодостатності; обов'язкова сертифікація кібербезпеки для осіб, які керують критичними національними інформаційними системами; посилення міжнародного співробітництва, включаючи структуровані механізми обміну даними про загрози та координації спільних оборонних дій…» ***(Vietnam seeks unified cybersecurity law to enhance digital protection // VietNamNet Global (https://vietnamnet.vn/en/vietnam-seeks-unified-cybersecurity-law-to-enhance-digital-protection-2464381.html). 20.11.2025).***

***

«Департамент інформаційних і комунікаційних технологій (DICT) Філіппін вважає кібербезпеку пріоритетним напрямком діяльності, оскільки вона є основою для пожвавлення стагнаційної цифрової економіки країни та формування довіри, необхідної для залучення іноземних інвестицій. Виступаючи на конференції Pilipinas Conference 2025, міністр ІКТ Генрі Роел Агуда наголосив,

що цифровізація повинна базуватися на довірі та стійкості, попередивши, що країна перебуває в «стані цифрового занепаду» і повинна терміново модернізувати свою інфраструктуру, щоб наздогнати сусідів з ASEAN. Щоб змінити цю тенденцію, DICT реалізує національну стратегію, що базується на трьох основних напрямках: швидке розгортання інфраструктури, сприяння впровадженню цифрових технологій у різних секторах та інституціоналізація управління та кібербезпеки. Ці зусилля підкріплюються ключовими міжнародними партнерствами, зокрема поновленою угодою з Програмою розвитку Організації Об'єднаних Націй про спільну розробку та масштабування програм цифрового управління в рамках ініціативи «Digital Bayanihan». Крім того, нова угода про співпрацю з Європейським Союзом, Пакет цифрової економіки ЄС-Філіппіни, підтримає цифрову трансформацію країни за рахунок внеску ЄС у розмірі 20 млн євро, а також додаткового фінансування з боку Фінляндії та Франції, зосередившись на 5G, кібербезпеці, штучному інтелекті та цифровій зв'язності…» ***(Ranier Allan Ronda. DICT vows better cybersecurity to attract investors // Philstar Global Corp. (https://www.philstar.com/headlines/2025/11/21/2488828/dict-vows-better-cybersecurity-attract-investors). 21.11.2025).***

***

«За даними постачальника послуг з управління IT ManageEngine, філіппінські компанії повинні терміново посилити свої заходи з кібербезпеки, оскільки швидка цифровізація та впровадження штучного інтелекту (ШІ) значно збільшують їхню вразливість до кібератак. Регіональний віце-президент ManageEngine Арун Кумар зазначив, що, хоча країна швидко просуває цифрову трансформацію та ШІ, багато місцевих компаній все ще не мають достатніх засобів захисту кібербезпеки, оскільки «не заклали правильні основи»…

Він наголосив на необхідності підходу до цифрової трансформації, що ставить на перше місце кібербезпеку, та рекомендував компаніям впровадити належне управління доступом, проводити регулярні оцінки вразливості та підвищувати обізнаність співробітників. Це попередження підкреслюється у звіті Microsoft Digital Defense Report, в якому Філіппіни входять до 20 країн, що найбільше постраждали від зловмисних кібератак у першій половині 2025 року. Кумар також попередив, що штучний інтелект дає шахраям можливість легко здійснювати складні атаки, і порадив компаніям боротися з цим, впроваджуючи системи захисту на основі штучного інтелекту та посилюючи навчання співробітників. Це узгоджується з даними Cisco, які вказують, що хоча 85% філіппінських компаній минулого року стикалися з кібератаками, пов'язаними з штучним інтелектом, лише 6% з них вважалися достатньо зрілими, щоб захиститися від них. ManageEngine, оптимістично налаштована щодо розширення своєї присутності в країні, робить ставку на зростаючу цифрову економіку та ринок центрів обробки даних, щоб стимулювати попит на свої комплексні рішення з управління IT на основі штучного інтелекту…» ***(Beatriz Marie D. Cruz. PHL cybersecurity must keep pace with AI, digital growth // BusinessWorld Publishing***

(https://www.bworldonline.com/corporate/2025/11/21/713719/phl-cybersecurity-must-keep-pace-with-ai-digital-growth-manageengine/). 21.11.2025).

***

«Широке поширення цифрових технологій в Індії залучило мільйони громадян, підприємств та критичної інфраструктури до мережі Інтернет, але також спричинило сплеск кіберзлочинності. За даними урядової організації CERT-In, кількість зареєстрованих інцидентів зросла з 1,39 мільйона у 2022 році до 1,59 мільйона у 2023 році і перевищила 2,04 мільйона у 2024 році, що підкреслює як масштаб, так і складність атак. Експерти стверджують, що необхідні активні заходи з боку уряду: посилення законодавства у сфері кібербезпеки, інвестиції в сучасні засоби захисту, тісніша координація між державними та центральними органами, а також загальнонаціональні кампанії з підвищення обізнаності населення, що сприяють ранньому формуванню цифрової грамотності…

Засновник CyberPeace Вініт Кумар стверджує, що лише поєднання більш жорстких заходів стримування та освіти громадян допоможе відновити довіру. Основні правила безпеки для окремих осіб залишаються критично важливими: використовуйте надійні, унікальні паролі з багатофакторною автентифікацією; оновлюйте все програмне забезпечення та антивірусні інструменти; з підозрою ставтеся до небажаних посилань і вкладень; блокуйте пристрої та використовуйте VPN у публічних мережах Wi-Fi; створюйте резервні копії даних, обмежуючи дозволи для додатків. Снеха Каткар з Quick Heal додає, що шахрайство на основі штучного інтелекту та крадіжка особистих даних у даркнеті роблять особисті дані новою валютою злочинності.

Зрештою, для забезпечення цифрового майбутнього Індії необхідна постійна співпраця між урядом, промисловістю та громадянським суспільством, постійне оновлення законодавчої бази та колективна прихильність до кібергігієни, щоб технологічна демократизація не відбувалася за рахунок безпеки…» ***(Cybersecurity in India: How awareness, and vigilance can stop cybercriminals // The Indian Express [P] Ltd. (https://www.financialexpress.com/life/technology-cybersecurity-in-india-how-awareness-and-vigilance-can-stop-cybercriminals-4045297/). 16.11.2025).***

***

«…На конференції «Cyber Secure Bharat: Fortifying India's Digital Future» (Кібербезпека в Індії: зміцнення цифрового майбутнього Індії) в Гувахаті фахівці з кібербезпеки попередили, що Індія повинна значно збільшити інвестиції в інструменти, навчання та оборонну інфраструктуру, оскільки сучасні конфлікти все частіше ведуться в комп'ютерних мережах. Бригадний генерал Вівек Верма (у відставці) з Об'єднаного інституту служб Індії заявив, що мета уряду підготувати 500 000 фахівців з кібербезпеки протягом п'яти років є недостатньою, і закликав інтегрувати кібердослідження в шкільні програми, військові академії та створити спеціальний кадровий резерв для кіберслужб. Він порівняв щорічні витрати Індії на військову штучну інтелігенцію, які становлять приблизно 50 мільйонів доларів США, з витратами Китаю (1,8 мільярда доларів

США) та проектом Maven Міністерства оборони США, назвавши цю різницю небезпечною «асиметрією»…

Генеральний директор NIELIT М. М. Тріпаті заявив, що «світ штучного інтелекту проти штучного інтелекту» вимагає висококваліфікованих фахівців з кіберкриміналістики та власних систем сертифікації. Він наголосив на необхідності використання існуючих лабораторій та запуску висококласних програм навчання для студентів завдяки більш тісній співпраці між урядом, науковими колами та промисловістю…» ***(Experts call for better tools, training and cyber defence systems // Nagaland Post (https://nagalandpost.com/experts-call-for-better-tools-training-and-cyber-defence-systems/). 21.11.2025).***

***

«Малайзія запустить своє перше спеціалізоване командування з кібернетичної та електромагнітної оборони (BSEP) у грудні, що стане важливим кроком на шляху до створення «розумних збройних сил», оголосив заступник міністра оборони Адлі Захарі. BSEP буде виконувати функцію центрального центру збройних сил для кібернетичних та електромагнітних операцій і буде впроваджуватися поетапно в рамках 13-го плану Малайзії з метою створення до 2030 року повністю боєздатних кібернетичних сил. Цей крок підтримує концепцію «Сил майбутнього», яка наголошує на передовій доктрині, цифрових структурах та високотехнологічних ресурсах. Адлі зазначив, що спеціальне кіберкомандування зміцнить національну оборону, дозволить проводити превентивні операції та поглибить співпрацю з регіональними партнерами у боротьбі зі все більш складними кіберзагрозами…

Міністерство також впроваджує штучний інтелект у вісім пріоритетних сфер, починаючи з наземного, повітряного та морського спостереження. Можливості штучного інтелекту будуть поширені на військові дрони, кіберзахист, системи розумної зброї, безпілотні транспортні засоби, застосування зелених технологій, комунікації, розвідку, тренажери та логістику, і все це з метою підвищення операційної ефективності за допомогою використання активів на основі даних. Відображаючи тенденції у Сполучених Штатах, Малайзія має намір забезпечити, щоб персонал оборони оволодів навичками експлуатації дронів.

Для підтримки цих технологічних змін у січні буде запроваджено національну політику у сфері оборонної промисловості. Координована Національною радою з питань оборонної промисловості, вона об'єднає університети, дослідницькі агентства та міністерства, такі як Міністерство науки, технологій та інновацій, з метою консолідації промислових потужностей, пов'язаних з обороною, розвитку вітчизняної експертизи та використання існуючих переваг у різних секторах…» ***(Cyber and Electromagnetic Defence Command to be set up // Star Media Group Berhad (https://www.thestar.com.my/news/nation/2025/11/20/cyber-and-electromagnetic-defence-command-to-be-set-up). 20.11.2025).***

***

«Шрі-Ланка переглядає свою систему кіберзахисту в рамках Національної стратегії цифрової економіки, в якій кібербезпека визначена

одним з основних пріоритетів. Проект реформ Національного закону про кібербезпеку передбачає створення вищого органу з кібербезпеки (CSA), надання Шрі-Ланкійському центру реагування на інциденти (SLCERT) більш широких повноважень з реагування на інциденти та встановлення комплексної правової та адміністративної системи для «надійної цифрової екосистеми», як заявив заступник міністра цифрової економіки Еранга Віпараратне на нещодавній Національній конференції з кібербезпеки…

Країна вже піднялася на другий рівень Глобального індексу кібербезпеки МСЕ; нова Національна стратегія кібербезпеки спрямована на досягнення першого рівня за допомогою чотирьох основних напрямків: (1) створення надійної правової/регуляторної системи, включаючи остаточне прийняття Закону про кібербезпеку та створення Органу з регулювання кібербезпеки; (2) підготовка кваліфікованих кадрів у сфері кібербезпеки; (3) програми підвищення обізнаності громадськості та готовності уряду; та (4) розширення можливостей SLCERT та більш широка співпраця зацікавлених сторін.

Основні інвестиції включають Національний центр кібербезпеки (NCSOC), який здійснює моніторинг критично важливих урядових мереж. Кабінет міністрів схвалив підключення 37 важливих відомств — імміграційної служби, казначейства, охорони здоров'я, комунальних служб тощо — з метою об'єднання всіх критично важливих структур до грудня 2026 року. SLCERT також управляє Національним центром сертифікації цифрових сертифікатів і виділяє людський фактор — причину 95 % інцидентів — як головну вразливість. Наразі підготовлено понад 5000 державних службовців, а також заплановано подальші програми за підтримки галузі…

Спільно CSA, посилений SLCERT, моніторинг NCSOC та загальнонаціональне навчання мають на меті забезпечити цифрову трансформацію Шрі-Ланки та зміцнити міжнародну довіру до її цифрової економіки, що розвивається». ***(Duruthu Edirimuni Chandrasekera. Sri Lanka advances in global cybersecurity ranking // Biometrics Research Group, Inc. (https://www.biometricupdate.com/202511/sri-lanka-advances-in-global-cybersecurity-ranking). 23.11.2025).***

***

«Швидка цифровізація Індії призвела до подвоєння кількості зареєстрованих інцидентів у сфері кібербезпеки з 1 мільйона у 2022 році до 2,2 мільйона у 2024 році, при цьому громадяни втратили приблизно 700 мільярдів рупій (791 мільйон доларів США) через онлайн-шахрайство лише за перші п'ять місяців 2025 року. Значна частина цього зростання пов'язана з шахрайством, яке використовує відомі бренди для завоювання довіри споживачів. Тактика включає використання схожих доменів і додатків, пірамідні схеми, фальшиві пропозиції про працевлаштування або франшизу, посилання з шкідливим програмним забезпеченням, великомасштабні піратські портали та фішинг з використанням штучного інтелекту. Group-IB зафіксувала 304-відсотковий стрибок шахрайства з використанням підроблених брендів з 2022 року, а експерти попереджають, що ринки з низьким рівнем цифрової обізнаності є основними цілями…

Влада створила кілька каналів реагування. CERT-In та Національний центр кіберкоординації займаються технічними інцидентами, а Індійський центр координації боротьби з кіберзлочинністю (I4C) та Національний портал повідомлень про кіберзлочини дозволяють жертвам та власникам інтелектуальної власності подавати кримінальні скарги; нова функція «Повідомити про підозрілого» прискорює запити на блокування шахрайських доменів. Однак правоохоронні органи стикаються з труднощами, коли шахрайство поширюється на багатьох сайтах та соціальних платформах…

Тому індійські суди розробили широкі цивільно-правові засоби захисту. У справі UTV Software (2019) Вищий суд Делі запровадив «динамічні судові заборони», що дозволяють правовласникам блокувати нові дзеркальні сайти без нових судових позовів. Пізніші рішення додали «динамічні+» судові заборони (що охоплюють майбутні твори) та «суперлативні» судові заборони (блокування в режимі реального часу на декількох носіях). Суди регулярно наказують реєстраторам доменів, інтернет-провайдерам, банкам і телекомунікаційним компаніям призупиняти роботу сайтів, що порушують авторські права, заморожувати рахунки та розкривати дані про реєстраторів. Вони протистояли загальним «омнібусним» заборонам на використання слів, що є торговими марками, але розглядають механізми для обмеження оманливих реєстрацій, і зараз очікується низка судових позовів від великих брендів…

Щоб зменшити збитки, регуляторні органи та власники брендів повинні: швидко реагувати на порушення прав доменів; впровадити моніторинг на основі штучного інтелекту для виявлення типографських помилок, підроблених додатків та соціальних шахраїв; інформувати споживачів про офіційні канали; та вимагати співпраці між NIXI, банками, телекомунікаційними компаніями та правоохоронними органами. Зміни в законодавстві повинні посилити відповідальність посередників, вимагати прозорої реєстрації доменів та інтегрувати списки відомих торговельних марок у банківську систему та систему UPI для запобігання шахрайству. Тільки скоординована екосистема — надійна технічна інфраструктура, оперативні суди та міжвідомча співпраця — може йти в ногу з витонченими кіберзлочинцями та захищати як споживачів, так і права інтелектуальної власності». ***(Urfee Roomi, Anuja Chaudhury. The intersection of IP rights and cybersecurity as growing integration of tech and business increases risk of cyberfraud // Law Business Research (https://www.iam-media.com/index.php/guide/india-managing-the-ip-lifecycle/2026/article/the-intersection-of-ip-rights-and-cybersecurity-growing-integration-of-tech-and-business-increases-risk-of-cyberfraud). 25.11.2025).***

***

Інші країни

«Національне управління з кібербезпеки Саудівської Аравії (NCA) тепер пропонує фінансові заохочення для інформаторів, які викривають порушення кібербезпеки. Інформатори, чиї повідомлення призводять до остаточного рішення,

можуть отримати 1% від суми штрафу або до 50 000 саудівських ріалів (близько 13 000 доларів США), залежно від того, яка сума є меншою. Комітет NCA розгляне кожну справу і визначить розмір винагороди. До порушень, що підпадають під дію програми, належать: надання послуг з кібербезпеки без ліцензії, порушення умов ліцензії, ігнорування національних стандартів безпеки, фальсифікація інформації, запитуваної NCA, торгівля незатвердженими засобами безпеки або перешкоджання роботі офіційних інспекторів… Винагорода виплачується тільки після винесення судового рішення або закінчення строку оскарження, і тільки в тому випадку, якщо інформація, надана інформатором, виявилася вирішальною. Винятки застосовуються до співробітників NCA та їхніх близьких родичів, державних службовців, чиї посадові обов'язки вже передбачають подання таких повідомлень, а також до випадків, за які вже було виплачено винагороду; інформатори також повинні зберігати конфіденційність інформації. Ця програма є частиною більш широких зусиль Королівства, спрямованих на посилення відповідальності, захист своєї цифрової інфраструктури та зміцнення свого становища регіонального лідера в галузі кіберуправління…» ***(Khitam Al Amir. Saudi Arabia offers SR50,000 reward for whistleblowers of cybercrimes // Al Nisr Publishing LLC (https://gulfnews.com/world/gulf/saudi/saudi-arabia-offers-sr50000-reward-for-whistleblowers-of-cybercrimes-1.500339610). 09.11.2025).***

***

«Сербія значно вдосконалила свою систему кібербезпеки завдяки новому Закону про інформаційну безпеку, який набрав чинності 31 жовтня 2025 року. Хоча Сербія не є членом ЄС, цей закон тісно узгоджується з принципами Директиви ЄС NIS2, що свідчить про значне розширення попередніх правил кібербезпеки країни…

Закон значно розширює сферу його застосування, охоплюючи широкий спектр секторів — від традиційних галузей, таких як енергетика та фінанси, до нововключених, таких як виробництво харчових продуктів, автомобілебудування та управління відходами. Регульовані суб'єкти класифікуються як «пріоритетні» або «важливі», причому обидві категорії підпадають під однакові основні зобов'язання, хоча пріоритетні суб'єкти підлягають більш високим штрафам. Примітною особливістю є те, що секторальне застосування закону, як видається, за замовчуванням поширюється на малі та мікропідприємства, доки не буде надано додаткових роз'яснень у вигляді виконавчих положень.

Постраждалі організації повинні виконувати комплексний перелік проактивних обов'язків. Основні зобов'язання включають реєстрацію в органах влади, впровадження надійних заходів безпеки та управління ризиками ланцюга поставок шляхом перевірки постачальників послуг та оновлення контрактів. Важливо, що компанії повинні підготувати як офіційний Закон про оцінку ризиків, так і Закон про безпеку ІКТ-систем до кінця квітня 2027 року, які повинні переглядатися щорічно. Вимоги щодо повідомлення про інциденти також є суворими: про інциденти необхідно повідомляти органи влади протягом 24 годин з моменту їх виявлення, а в деяких випадках — також і користувачів, яких вони стосуються…

Хоча повні деталі будуть вказані в імплементаційних нормативних актах, які очікуються до 31 жовтня 2026 року, компаніям рекомендується негайно розпочати підготовку. Наступні необхідні кроки включають визначення їх класифікації відповідно до нового закону, перегляд існуючих заходів кібербезпеки, внесення змін до контрактів з постачальниками та встановлення внутрішніх процедур для повідомлення про інциденти та майбутніх обов'язкових заходів безпеки». ***(Goran Radoševic and Anja Gatarić. From NIS2 to Serbia: How the New Information Security Law Impacts Your Business // Karanovic & Partners (https://www.karanovicpartners.com/news/from-nis2-to-serbia-how-the-new-information-security-law-impacts-your-business/). 11.2025).***

***

«Пакистан завершив розробку проекту Національного закону про кібербезпеку, який передбачає створення центрального органу з кібербезпеки для координації та забезпечення захисту у всіх секторах критичної інформаційної інфраструктури (CII). Запланований орган є основою Національної політики кібербезпеки 2021 року, яка є частиною Програми розвитку цифрової економіки, що також охоплює такі проекти, як безпечний рівень обміну даними, цифрова ідентифікація та електронні послуги для громадян… Наразі уряд офіційно визначив інформаційні системи NADRA, FBR та телекомунікаційного сектору як CII відповідно до PECA-2016 та видав керівні принципи щодо виявлення та захисту інших критичних систем; наступною на черзі для визначення є служба імміграції та паспортів. Доки не буде створено новий орган, 14-членна Рада CERT, до складу якої входять представники міністерств інформаційних технологій, оборони, внутрішніх справ та закордонних справ, а також оператори телекомунікаційних послуг, наукові кола та громадянське суспільство, продовжує займатися реагуванням на інциденти та координацією між державним і приватним секторами відповідно до Правил CERT 2023…» ***(Pakistan to Get First Dedicated Cybersecurity Authority to Boost National Defense // ProPakistani.PK (https://propakistani.pk/2025/11/21/pakistan-to-get-first-dedicated-cybersecurity-authority-to-boost-national-defense/#google_vignette). 21.11.2025).***

***

«…ОАЕ запустили «Глобальну програму лідерства в галузі передових технологій, штучного інтелекту та кібербезпеки», щоб продемонструвати свої передові практики та розбудувати міжнародний потенціал у цих сферах. Програма, організована Управлінням з обміну досвідом уряду при Міністерстві у справах кабінету міністрів у партнерстві з Радою з кібербезпеки ОАЕ, зібрала 21 генерального директора та виконавчого директора з 14 країн — від Барбадосу та Південної Африки до В'єтнаму та Казахстану — в Еміратах для проведення низки візитів, семінарів та зустрічей з 30 експертами з Еміратів…

Протягом декількох днів учасники вивчали підхід ОАЕ до забезпечення цифрової трансформації, захисту критичної інфраструктури та швидких технологічних інновацій, одночасно вдосконалюючи власні лідерські та управлінські навички. Заступник міністра Абдулла Нассер Лута заявив, що ця

ініціатива відповідає стратегії ОАЕ щодо використання передових технологій та кібербезпеки як основи модернізації уряду та глобального партнерства. Голова кібербезпеки ОАЕ д-р Мохамед Хамад Аль-Кувейтський додав, що інвестиції в людський капітал є центральним елементом будь-якої надійної системи цифрової безпеки і що програма зміцнює міжнародне співробітництво у боротьбі з зростаючими кіберзагрозами». ***(Government leaders from 14 countries explore UAE's experience in advanced technologies, cybersecurity // WAM (https://www.wam.ae/en/article/bmso8dw-government-leaders-from-countries-explore-uae%E2%80%99s). 19.11.2025).***

***

«Прогнозується, що ринок кібербезпеки ОАЕ зросте більш ніж удвічі — з 620 млн доларів США у 2024 році до приблизно 1,29 млрд доларів США до 2030 року, зростаючи на 12,8 % CAGR під впливом аналітики на основі штучного інтелекту, архітектури Zero-Trust та потужних урядових ініціатив, таких як Національна стратегія кібербезпеки та Федеральна рада з кібербезпеки. На цьому тлі Intersec 2026 (12–14 січня в Дубайському світовому торговому центрі) проведе «InCyber Briefing», спрямований на керівників служб інформаційної безпеки та лідерів у сфері цифрових ризиків. Програма запропонує практичні рамки щодо управління штучним інтелектом, готовності до постквантової ери, стійкості ланцюгів постачання та звітності про кіберризики…

Головний доповідач Лукман Кондет, директор з кібербезпеки в Нью-Йоркському університеті в Абу-Дабі, використає притчу про «сільського оракула», щоб проілюструвати нагляд за ШІ: скористатися інтелектом ШІ, не відмовляючись від людського судження. Він виступає за модель «трьох ліній захисту» — операційні команди, що тестують ШІ, команди з ризиків/відповідності, що вимірюють упередженість і точність, та аудитори, що перевіряють дотримання правил — і прогнозує, що управління ШІ стане безперервною «інфраструктурою», вбудованою в архітектуру підприємства, подібно до сучасних засобів контролю конфіденційності та безпеки…

З понад 1400 експонентами з більш ніж 60 країн на площі 67 000 м² та очікуваними 50 000 відвідувачів, 27-а виставка Intersec стане найбільшою за всю історію її проведення. Виставка проходить під патронатом Його Високості шейха Мансура бін Мохаммеда бін Рашида Аль Мактума та за підтримки цивільної оборони Дубая і SIRA». ***(UAE's US$1.29 billion cybersecurity market sets stage for strategic AI dialogue at Intersec's InCyber Briefing // ROMA Publications Ltd. (https://premierconstructionnews.com/2025/11/24/uaes-us1-29-billion-cybersecurity-market-sets-stage-for-strategic-ai-dialogue-at-intersecs-incyber-briefing/). 24.11.2025).***

***

«Нова платформа електронних віз Сомалі, запущена у вересні, зазнала витоку даних, в результаті якого була розкрита інформація про мандрівників, які користуються електронною системою дозволів на подорож (e-TAS). Після появи перших повідомлень у соціальних мережах, які спочатку були спростовані

владою, Агентство з питань імміграції та громадянства (HSJ) визнало, що «виявило незаконний витік даних», і негайно ізолювало уражені системи…

Уряд сформував національну робочу групу з представників органів безпеки, міжнародних експертів-криміналістів та посадових осіб, відповідальних за захист даних, щоб визначити масштаби, джерело та наслідки порушення. Після розслідування буде опубліковано детальний звіт, а всі, хто постраждав, будуть повідомлені безпосередньо через офіційні канали. Тим часом HSJ попередила громадськість про дезінформацію та заявила, що посилює свої захисні заходи за допомогою сучасних стандартів захисту даних та багатофакторної автентифікації.

Посольства США та Великої Британії раніше попередили своїх громадян про потенційні ризики при використанні служби електронних віз Сомалі. Система цифрових віз є частиною ширшої програми управління кордонами (PISCES), що підтримується США, та більш широкої програми цифрової трансформації Сомалі, яка також включає національну схему цифрової ідентифікації, що підтримується Світовим банком, з метою реєстрації 15 мільйонів людей до 2029 року…» ***(Ayang Macdonald. Somalia government probes digital visa platform data breach // Biometrics Research Group, Inc. (https://www.biometricupdate.com/202511/somalia-government-probes-digital-visa-platform-data-breach). 18.11.2025).***

***

«…Глобальний індекс шахрайства за 2025 рік, складений Sumsub і Statista, показує, що Африка, особливо Нігерія, залишається вкрай вразливою до цифрового та фінансового шахрайства. З 112 країн Нігерія посіла 110-те місце, а Танзанія (108-те) і Уганда (107-те) також опинилися внизу рейтингу. Загальний показник вразливості Африки до шахрайства, що становить 3,84, є найгіршим серед усіх регіонів, що відображає слабку координацію політики, обмежене правозастосування та низьку обізнаність громадськості. На противагу цьому, Маврикій є найкращим в Африці, посідаючи 22-е місце у світі, тоді як Ботсвана, Марокко, Туніс і Південна Африка демонструють помірну стійкість…

У світовому рейтингу за рівнем захисту від шахрайства лідирують Люксембург, Данія, Фінляндія, Норвегія та Нідерланди, тоді як шахрайські схеми на основі штучного інтелекту набирають обертів у всьому світі. Експерти стверджують, що африканські уряди повинні поєднати свої зусилля з цифрової інклюзії з більш потужними системами верифікації на основі штучного інтелекту, гармонізацією політики та транскордонною співпрацею, щоб запобігти підриву довіри до цифрової та фінансової інфраструктури континенту». ***(Juliet Umeh. Cybersecurity: Africa's fraud crisis deepens // Vanguard Media Limited (https://www.vanguardngr.com/2025/11/cybersecurity-africas-fraud-crisis-deepens/). 26.11.2025).***

***

«Кіберризики випередили кліматичні зміни як головну проблему для французьких страховиків, що зумовлено хвилею все більш дорогих атак, таких як збиток у розмірі 2 млрд євро, який зазнала компанія Jaguar у 2025 році. Зловмисники, які прагнуть отримати гроші або геополітичний вплив, тепер регулярно порушують роботу корпорацій, лікарень та урядів, а збитки від втрати даних часто є незворотними. Проте розрив у зрілості залишається: великі підприємства інвестують у надійні засоби контролю та купують високі кіберліміти, тоді як малі та середні підприємства, обмежені бюджетом та усвідомленням ризиків, мають незначне або взагалі не мають покриття. Ця вразливість «найслабшої ланки» ставить під загрозу цілі ланцюги постачання та ускладнює страхування; складні, нестандартні анкети відлякують малі підприємства, а ціни розходяться (ставки для великих французьких корпорацій у 2024 році впали на 18 %, на відміну від премій для малих та середніх підприємств). Страховики повинні спростити процедуру укладення договорів — сканування ризиків на основі штучного інтелекту може замінити паперову роботу — і перейти від чистого відшкодування до «стійкості як послуги»…

До інциденту оператори повинні діяти як охоронці безпеки: проводити контрольні перевірки, проводити навчальні тренування, перевіряти постачальників та відстежувати цифрові сліди (хмара, MSP, OT/IT-посилання). Після інциденту вони повинні організувати швидке відновлення за допомогою заздалегідь перевірених команд з криміналістики, юриспруденції, PR та взаємодії з регуляторними органами.

Регулювання прискорює ці зміни. Директива ЄС NIS2 та Закон про кіберстійкість 2024 року встановлюють більш суворі вимоги до управління ризиками та забезпечення безперебійної роботи для критично важливих операторів та фінансових установ, включаючи самі страхові компанії. Таким чином, страхові компанії перетворюються з пасивних носіїв ризиків на стратегічних партнерів, які будують колективний цифровий імунітет, необхідний як для стабільності ринку, так і для системної кіберзахисту…» ***(The Cyber Insurance Shortfall: Why all Businesses Should Have Cyber Attack Cover // Insurance Edge (https://insurance-edge.net/2025/11/20/the-cyber-insurance-shortfall-why-all-businesses-should-have-cyber-attack-cover/). 20.11.2025).***

***

«Опитування GlobalData щодо страхування малих та середніх підприємств у Великобританії на 2025 рік показує, що лише 40% британських малих та середніх підприємств мають кіберстрахування, що залишає значну частину економіки фінансово вразливою, оскільки атаки стають все частішими та дорожчими. Рівень страхування різко зростає з розміром підприємства — лише 13% приватних підприємців мають страхування проти 63% підприємств із 50–249 працівниками, — але навіть деякі великі корпорації, такі як Jaguar Land Rover, залишаються незастрахованими. Головним стримуючим фактором (на який вказують 40% тих, хто не купує страхування) є переконання, що їхня

компанія навряд чи стане об'єктом атаки; ще 16% вважають, що існуючих заходів захисту достатньо…

Тим часом, Асоціація британських страховиків повідомляє, що виплати за кіберпретензіями в 2024 році потроїлися до 197 мільйонів фунтів стерлінгів, а середня вартість претензій зросла з 113 000 до 276 000 фунтів стерлінгів, що значною мірою було спричинено шкідливим програмним забезпеченням. Гучні порушення в Harrods, Marks & Spencer та JLR у 2025 році свідчать про посилення загрози…

Без страхового покриття підприємства ризикують понести всі витрати на криміналістичне розслідування, відновлення даних, юридичні послуги, штрафи регуляторних органів, втрату доходів та кризове управління — витрати, які можуть змусити невеликі фірми закритися. Брокери залишаються ключовими фігурами: 27% застрахованих МСП придбали страхове покриття за порадою брокера, а 26% — після повідомлень у ЗМІ про атаки. Тому страховики повинні інформувати клієнтів і пропонувати доступні, індивідуальні поліси, особливо для МСП з обмеженою маржею, які все ще вважають кіберстрахування необов'язковою витратою». ***(UK cyber insurance adoption is low yet cyberattacks are escalating // GlobalData Plc (https://www.lifeinsuranceinternational.com/analyst-comment/uk-cyber-insurance-adoption-low-yet-cyberattacks-escalating/?cf-view). 21.11.2025).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«У травні 2025 року, одночасно з фізичними ударами «Операції Сіндур» (Operation Sindoor) по терористичній інфраструктурі, кібермережі Індії зазнали складних, точно спланованих фішингових атак і атак з використанням шкідливого програмного забезпечення, що стало яскравим прикладом гібридної війни в Південній Азії. Дослідження, проведене Індійським технологічним інститутом у Бомбеї, дозволило встановити, що за цими вторгненнями стоїть APT36 (Transparent Tribe) — пакистанська група кібершпигунів, яка діє з 2013 року…

Цифрова атака розпочалася ще до військових ударів, з використанням фішингових електронних листів, замаскованих під офіційні повідомлення про терористичний напад у Пахалгамі. Коли жертви відкривали шкідливий документ Office, він запускав Crimson RAT (троян для віддаленого доступу) — шкідливе програмне забезпечення, яке надавало зловмисникам повний віддалений контроль для викрадення облікових даних, запису натискань клавіш та витоку даних на сервери в Росії, Німеччині та Індонезії. Важливо, що шкідливе програмне забезпечення було скомпільовано за день до теракту в Пахалгамі, що свідчить про попередню координацію між терористичною операцією та кіберкампанією…

Відтворивши атаку в контрольованому середовищі за допомогою системи телеметрії кінцевих точок Osquery, дослідники реконструювали ланцюжок зараження, зазначивши, що APT36 використовувала надійні бінарні файли Microsoft («живучи з того, що є») для досягнення прихованості та швидкості. На основі цього аналізу команда IIT-Bombay розробила систему виявлення за допомогою інтерфейсу

SQL Osquery, яка позначає поведінку Crimson RAT і може бути інтегрована в існуючі системи EDR/XDR. У дослідженні робиться висновок, що сучасний конфлікт охоплює «код, командування та пізнання», що робить комплексну кіберготовність необхідністю, а не лише доповненням до національної оборони». ***(Reinforcements for the cyber frontline // THG PUBLISHING PVT LTD. (https://www.thehindubusinessline.com/business-tech/reinforcements-for-the-cyber-frontline/article70233666.ece). 03.11.2025).***

***

«…Ізраїльські сили оборони (IDF) нещодавно віддали наказ про вилучення приблизно 700 автомобілів китайського виробництва, переважно моделей Chery Tiggo 8 Pro, з парку автомобілів для старших офіцерів до початку 2026 року, виходячи з оцінки національної безпеки, згідно з якою ці автомобілі становлять неприйнятний ризик шпигунства. Ця радикальна міра, яка стала наслідком невдалих спроб «стерилізувати» мультимедійні системи автомобілів для запобігання передачі даних, була необхідною через висновок, що потенціал витоку розвідданих, який може поставити під загрозу військові операції, не може бути повністю усунутий…

Експерти з безпеки класифікують сучасні підключені автомобілі як «мобільні інтелектуальні платформи» через їх закриті операційні системи, широкі можливості бездротового підключення та набір камер, мікрофонів і GPS/телематичних пристроїв. Ці компоненти постійно збирають і передають конфіденційні дані, включаючи геолокацію, біометричну інформацію та візуальні деталі військових пересувань або секретних об'єктів, потенційно на зовнішні сервери в Китаї без згоди водія…

Рішення Ізраїлю відображає аналогічні обмеження в США та Великобританії і підкреслює системну проблему кібербезпеки: будь-який мережевий пристрій є потенційною вразливістю. Загроза не обмежується китайськими автомобілями, оскільки більшість автовиробників не впроваджують надійні функції безпеки, такі як наскрізне шифрування для величезних потоків даних, що надходять з їхніх транспортних засобів. Дії IDF підкреслюють, що протоколи безпеки повинні кардинально змінитися, щоб відповісти на цю нову реальність, в якій традиційний периметр безпеки розчинився, вимагаючи обов'язкових, системних стандартів кібербезпеки, включаючи шифрування для всіх мережевих платформ транспортних засобів незалежно від виробника, а не покладаючись виключно на заборони для конкретних брендів…» ***(Jack Poller. Why Israel Just Banned 700 Chinese Cars from Its Military—And What It Means for Security // Techstrong Group Inc. (https://securityboulevard.com/2025/11/why-israel-just-banned-700-chinese-cars-from-its-military-and-what-it-means-for-security/). 04.11.2025).***

***

«Незалежне Бюджетне управління Конгресу (CBO), яке надає законодавцям фінансові прогнози та аналітичні матеріали щодо політики, стало жертвою хакерської атаки, яка, як вважається, пов'язана з іноземним супротивником. CBO заявляє, що негайно локалізувало злом, додало нові засоби

моніторингу та контролю безпеки і продовжує свою роботу для Конгресу, поки триває розслідування. Хоча офіційні особи не уточнили, до чого саме отримали доступ зловмисники, офіс зберігає конфіденційні економічні прогнози, бюджетні дані та внутрішню переписку з персоналом Конгресу, які можуть надати стратегічну інформацію зовнішній розвідці… Бюджетний комітет Сенату та Комітет з питань внутрішньої безпеки Палати представників підтримують контакт з CBO та Агентством з кібербезпеки та безпеки інфраструктури, щоб відстежувати заходи з мінімізації наслідків. Цей інцидент нагадує торішнє вторгнення іноземних хакерів в електронну пошту Конгресової дослідницької служби та підкреслює більш широку тенденцію до атак з боку державних суб'єктів на мережі уряду США. Законодавці попереджають, що цей ризик є особливо тривожним, оскільки значна частина федерального уряду залишається частково закритою…» ***(David DiMolfetta. CBO systems accessed in 'security incident' possibly tied to foreign hackers // Government Media Executive Group LLC. (https://www.nextgov.com/cybersecurity/2025/11/cbo-systems-accessed-security-incident-possibly-tied-foreign-hackers/409379/). 06.11.2025).***

***

«Міністр безпеки Великобританії Ден Джарвіс і MI5 опублікували суворе публічне попередження про те, що китайські агенти систематично націлюються на парламент, політичні партії, кандидатів на виборах, державних службовців, підприємства та університети шляхом таємного втручання, кібероперацій та професійних мережевих платформ…

У відповідь на це уряд оголосив про комплексний пакет контрзаходів:

Нове законодавство у вигляді законопроекту про вибори, що посилює правила щодо іноземних політичних пожертв та зміцнює повноваження національної безпеки проти втручання.

Обов'язкові інструктажі з питань безпеки для всіх політичних партій та індивідуальні рекомендації для кандидатів щодо виявлення та повідомлення про підозрілі спроби впливу.

Активні кампанії, спрямовані на те, щоб зробити LinkedIn та подібні платформи ворожою територією для іноземних агентів.

Знищення проксі-компаній та підставних організацій, які використовуються ворожими державами.

170 мільйонів фунтів стерлінгів на заміну всіх зашифрованих систем урядового зв'язку

Негайне вилучення китайського обладнання для спостереження з усіх важливих об'єктів урядової власності Великобританії по всьому світу

Продовження наступальних дій проти хакерських угруповань, що базуються в Китаї

130 мільйонів фунтів стерлінгів на посилення антитерористичної діяльності поліції та Національного агентства з питань безпеки, щоб допомогти британським компаніям захистити інтелектуальну власність від крадіжок, що фінансуються державою

Розширення консультаційної служби з питань економічної безпеки, яка вже захищає передові галузі виробництва

Термінова зустріч з ректорами університетів для протидії іноземному втручанню в академічну сферу…

Ці заходи є найагресивнішим і найскоординованішим кроком Великобританії на сьогоднішній день, спрямованим на протидію впливу Пекіна на все суспільство та шпигунській кампанії проти демократичних інститутів і економічних активів Великобританії». ***(UK measures to counter China's threat to lawmakers, business, universities // Reuters (https://www.reuters.com/world/uk/uk-measures-counter-chinas-threat-lawmakers-business-universities-2025-11-18/). 18.11.2025).***

***

«Підрозділ Amazon, що займається аналізом загроз, попереджає, що хакери, пов'язані з іранською державою, все частіше використовують кібероперації для підготовки до реальних атак — це явище називається «кібернетичне кінетичне націлювання». Замість того, щоб розглядати цифрові вторгнення та фізичні атаки як окремі сфери, групи, пов'язані з Ісламською революційною гвардією Ірану (Imperial Kitten/Tortoiseshell) та Міністерством розвідки і безпеки (MuddyWater), проводять детальну онлайн-розвідку для наведення ракет та інших кінетичних дій…

• З грудня 2021 року по січень 2024 року Imperial Kitten проникла в автоматичну ідентифікаційну систему корабля, а згодом отримала доступ до бортової системи відеоспостереження. 27 січня 2024 року група запросила дані AIS для конкретного судна; через кілька днів бойовики Хуті (без успіху) обстріляли це саме судно в Червоному морі.

• У травні 2025 року MuddyWater створила інфраструктуру, яка через місяць була використана для перегляду прямих трансляцій з камер відеоспостереження в Єрусалимі. Кібердиректорат Ізраїлю заявив, що зловмисники намагалися переглядати зображення з громадських камер під час масштабного ракетного обстрілу Іраном 23 червня, щоб підвищити точність ударів…

Актори направляють трафік через VPN-сервіси, щоб приховати його походження, підкреслюючи, що шпигунські вторгнення слугують стартовими майданчиками для кінетичних атак. Amazon стверджує, що такі комбіновані кампанії стирають традиційну межу між кібервійною та фізичною війною, вимагаючи інтегрованих засобів захисту, які розглядають цифрові та кінетичні загрози як частини єдиного поля бою». ***(Ravie Lakshmanan. Iran-Linked Hackers Mapped Ship AIS Data Days Before Real-World Missile Strike Attempt // The Hacker News (https://thehackernews.com/2025/11/iran-linked-hackers-mapped-ship-ais.html). 20.11.2025).***

***

«…Група APT31, пов'язана з Китаєм, була визнана відповідальною за серію тривалих кібершпигунських атак, спрямованих проти російського IT-сектору в період з 2024 по 2025 рік, зокрема проти компаній, що виступають підрядниками та інтеграторами для державних органів… Щоб залишатися невиявленими протягом тривалого часу, іноді починаючи з перших зломів у 2022 році, група стратегічно використовувала легальні російські хмарні сервіси, такі як

Yandex Cloud, для управління та витоку даних, змішувала свою діяльність із звичайним трафіком, працюючи у вихідні та святкові дні, а також розміщувала корисні навантаження на профілях у соціальних мережах. Їхні атаки часто починалися з фішингових листів, що містили архіви, які запускали завантажувачі, такі як CloudyLoader, для початку компрометації…

APT31 використовувала широкий і постійно оновлюваний арсенал інструментів для забезпечення стійкості, розвідки та крадіжки даних, включаючи утиліти для вилучення паролів браузерів, такі інструменти, як Tailscale VPN і Microsoft dev tunnels для створення зашифрованих тунелів, а також спеціальні бекдори, такі як COFFProxy і CloudSorcerer, які використовували хмарні сервіси для комунікації. Цей витончений підхід, що поєднував загальнодоступні та спеціальні інструменти, налаштовані для імітації легальних додатків, дозволив групі систематично збирати конфіденційну інформацію, включаючи паролі поштових скриньок, і протягом багатьох років залишатися непомітною в інфраструктурі жертв…» ***(Ravie Lakshmanan. China-Linked APT31 Launches Stealthy Cyberattacks on Russian IT Using Cloud Services // The Hacker News (https://thehackernews.com/2025/11/china-linked-apt31-launches-stealthy.html). 22.11.2025).***

***

«На початку листопада 2025 року Knownsec, одна з найбільших китайських компаній з кібербезпеки, що має прямі зв'язки з урядом, зазнала катастрофічного витоку даних, в результаті якого було оприлюднено понад 12 000 секретних документів.

Цей інцидент виявив масштаби та складність кібероперацій, що фінансуються державою, включаючи детальну інформацію про кіберзброю, внутрішні хакерські інструменти та вичерпний список цілей глобального спостереження.

Цей витік став значним поворотним моментом у розумінні технічних можливостей та геополітичного масштабу організованих кібершпигунських операцій на державному рівні». ***(Chinese Cybersecurity Firm Data Breach Exposes State-Sponsored Hackers Cyber Weapons and Target List // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/chinese-cybersecurity-firm-data-breach-exposes-state-sponsored-hackers-cyber-weapons-and-target-list/). 17.11.2025).***

***

«У щорічному звіті Microsoft про кібербезпеку за 2025 рік Бельгія посідає одне з перших місць серед країн, які найчастіше стають об'єктом хакерських атак, що підтримуються державою. У звіті зазначається, що минулого року суб'єкти, пов'язані з Росією, спрямували близько 5 % своїх глобальних кібероперацій на бельгійські мережі. Порушення роботи компаній Proximus, Scarlet та Університетської лікарні Гента ілюструють цю тенденцію. Барт Аснот з Microsoft Belgium пояснює таку увагу до Бельгії стратегічним розташуванням НАТО, інституцій ЄС та Євроконтролю, називаючи країну «серцем Європи». Більшість дій національних держав пов'язані з проросійськими «хактивістськими» групами, які

використовують розподілені атаки типу «відмова в обслуговуванні» для спричинення короткочасних перебоїв у роботі та надсилання політичних повідомлень, а не для проникнення в системи…

Незважаючи на це, шпигунство становить лише 4% атак, спрямованих на Бельгію; переважна частка — 81% — припадає на кіберзлочинців, які керуються фінансовими мотивами. Фінансові послуги, IT-провайдери, освіта та наукові дослідження залишаються головними цілями злочинців. У звіті також відзначається різке зростання кількості фішингових атак із використанням штучного інтелекту: завдяки штучному інтелекту зловмисники можуть за лічені секунди створювати високо персоналізовані приманки, що сприяє зростанню середньої кількості спроб атак на паролі до майже 7000 на секунду, що на 30% більше, ніж у минулому році». ***(Beyza Binnur Donmez. Belgium increasingly targeted by state-backed cyberattacks: Report // Anadolu Ajansı (www.aa.com.tr/en/europe/belgium-increasingly-targeted-by-state-backed-cyberattacks-report/3738573). 09.11.2025).***

***

«У 2025 році Іран значно посилив свої наступальні кібердіяльності, керуючись стратегією просування своїх військових і політичних цілей, одночасно протидіючи більш технологічно розвиненим супротивникам. Ключовою особливістю його операцій є «подвійне використання цілей», що передбачає викрадення розвідданих, які служать як військовим потребам, так і більш широким політичним цілям… Прикладом цього є такі групи, як UNC1549 (відстежувана CrowdStrike під назвою «Imperial Kitten»), яка проводить шпигунські кампанії за допомогою spear-phishing проти аерокосмічних, оборонних та урядових організацій у таких країнах, як США, Ізраїль та ОАЕ. Замість того, щоб здійснювати руйнівні атаки, ці групи зосереджуються на таємному підтриманні довгострокового доступу до мережі для викрадення даних, що дозволяє Ірану прискорити розвиток військових технологій та обійти міжнародні санкції…

Хоча Іран займається широким спектром зловмисних дій — від втручання у вибори до використання програм-вимагачів — його основна кібердіяльність зосереджена на Ізраїлі та США, особливо після посилення геополітичної напруженості та американських авіаударів у 2025 році. Експерти відзначають, що останні військові невдачі, ймовірно, посилили необхідність Тегерана використовувати кібероперації для збору розвідданих про плани супротивників, проєктування впливу за межі своїх кордонів та зміцнення свого ослабленого політичного та військового становища…» ***(Alexander Culafi. Inside Iran's Cyber Objectives: What Do They Want? // TechTarget, Inc. (https://www.darkreading.com/cybersecurity-operations/iran-cyber-objectives). 21.11.2025).***

***

«…Arctic Wolf повідомила, що RomCom, хакерська група, пов'язана з російською розвідкою, у вересні 2025 року здійснила атаку на американську інженерну фірму виключно тому, що ця компанія надавала послуги американському муніципалітету, який підтримує побратимські відносини з

українським містом. Хоча Arctic Wolf запобігла будь-яким оперативним порушенням, цей інцидент підкреслює розширення кіберкампаній Москви проти організацій, які допомагають Україні — навіть опосередковано — шляхом покарання, шпигунства або порушення роботи організацій, пов'язаних із мережею підтримки Києва…

Ця атака відбулася після попереджень ФБР та CISA про те, що агенти, пов'язані з Росією, досліджують інфраструктуру США з метою перешкоджання гуманітарній та військовій допомозі Україні. Нещодавні кампанії також вразили такі гуманітарні організації, як Червоний Хрест та ЮНІСЕФ, використовуючи складні фішингові тактики, маскуючись під українських чиновників, що демонструє готовність Росії націлюватися на уряди, НУО та приватні компанії, які підтримують військові зусилля України». ***(DAVID KLEPPER. Russian hackers target US engineering firm because of work done for Ukrainian sister city // Courthouse News Service (https://www.courthousenews.com/russian-hackers-target-us-engineering-firm-because-of-work-done-for-ukrainian-sister-city/). 25.11.2025).***

***

Створення та функціонування кібервійськ

«Національна гвардія Пенсільванії перетворила свої кіберможливості на об'єднані сили швидкого реагування, які підтримують мережі як США, так і штату, одночасно поглиблюючи 32-річне партнерство з Литвою у сфері кібербезпеки. Створений у 2011 році як невелика команда підтримки мережі, кіберпідрозділ Гвардії зараз складається з трьох взаємодоповнюючих підрозділів — Елементу оборонних кібероперацій (DCOE) та Елементу місії команди кіберзахисту Армійської гвардії, а також 112-го ескадрону кібероперацій Повітряної гвардії, що надає йому гнучкі людські ресурси для захисту систем Міністерства оборони та допомоги агентствам Пенсильванії у відновленні після атак програм-вимагачів та інших атак… За останнє десятиліття ці команди провели понад 60 оцінок вразливості для державних, окружних та критично важливих інфраструктурних об'єктів, ще 10 оцінок заплановано, а майже 70 знаходяться в списку очікування. Вони також проводять просвітницькі програми, такі як «Wi-Fighter», яка пропонує школам кібервиклики типу «захопи прапор»…

На міжнародному рівні кібервійська Пенсільванії тренуються разом із литовськими колегами в рамках Програми партнерства штатів Національного бюро гвардії, беруть участь у навчаннях, таких як Cyber Shield і литовська Amber Mist, обмінюються інформацією про загрози та допомагають будувати Литовський регіональний центр кіберзахисту. Співпраця поєднує американський досвід у процесах дотримання вимог із литовським оперативним досвідом. У перспективі Національна гвардія планує створити штатну державну команду з оцінки кібербезпеки та розширити функції фахівців, щоб відповідати зростаючим кіберзагрозам у країні та за кордоном…» ***(Pennsylvania National Guard strengthens cyber defense at home and abroad // U.S.***

Army(https://www.army.mil/article/289050/pennsylvania_national_guard_strengthens_cyber_defense_at_home_and_abroad). 17.11.2025).

***

«Міністерство оборони Литви оголосило про загальнонаціональний план створення 44 центрів кібербезпеки протягом найближчих трьох з половиною років, що дозволить розширити можливості цифрової оборони далеко за межі столиці. Координовані Національним центром кібербезпеки (NKSC), кожна область матиме регіональний центр, який буде контролювати місцеві мережі, виявляти та реєструвати інциденти, а також зміцнювати вразливі системи. Модель базується на пілотному центрі в регіоні Шяуляй, який має запрацювати до кінця року і в якому працюватимуть чотири фахівці, що обслуговуватимуть сім муніципалітетів. Згідно з цією схемою, NKSC надаватиме обладнання, програмне забезпечення та навчання, а муніципалітети забезпечуватимуть приміщення та оплачуватимуть роботу персоналу. Взаємопов'язані центри забезпечать єдину систему виявлення загроз та реагування на інциденти по всій Литві, а також посилять координацію під час великих кіберподій, що значно підвищить кіберстійкість державного сектору…» ***(Lithuania to roll out 44 local cybersecurity operations centers to boost national defense // Anadolu Ajansı (https://www.aa.com.tr/en/europe/lithuania-to-roll-out-44-local-cybersecurity-operations-centers-to-boost-national-defense/3745790). 17.11.2025).***

***

«Велика Британія запустила Міжнародні оборонні кіберспортивні ігри (IDEG) — багатонаціональну ініціативу, в рамках якої військовослужбовці з понад 40 країн-союзників змагатимуться в іграх, щоб відточити критично важливі цифрові бойові навички, необхідні для сучасної війни. Офіційно визнані Великою Британією військовим видом спорту в 2024 році, IDEG мають на меті зміцнити кіберстійкість і бойову готовність шляхом розвитку таких навичок, як відстеження множинних загроз, швидке прийняття рішень під тиском і керування дронами. На ініціативу значний вплив мали уроки України, де ігри-симулятори з використанням дронів продемонстрували значне підвищення точності наведення операторів та ефективності виконання місій…

Фінал змагань заплановано на жовтень 2026 року в Національній ігровій та кіберспортивній арені в Сандерленді, де відбудуться турніри з прямою трансляцією та стратегічні саміти з питань кібербезпеки та штучного інтелекту. За підтримки великих оборонних компаній IDEG позиціонує Велику Британію як лідера у використанні ігрових технологій для підготовки збройних сил до цифрових бойових дій майбутнього, реагуючи на понад 90 000 кібератак, що щорічно спрямовані проти країни…» ***(UK Military Esports Games Boost Cyber Skills // Mirage.News (https://www.miragenews.com/uk-military-esports-games-boost-cyber-skills-1575630/). 22.11.2025).***

***

«Стартап під назвою Twenty (XX), заснований колишніми військовими хакерами та фахівцями з кібербезпеки, виграв стратегічну ставку на те, що Пентагон надасть пріоритет наступальним кібероперaціям, отримавши контракти на суму до 12,6 мільйона доларів з Кіберкомандуванням США та ВМС США. Компанія, названа на честь британської контррозвідувальної операції часів Другої світової війни, має на меті використовувати штучний інтелект, щоб допомогти військовим хакерам автоматизувати та прискорити вторгнення в мережі супротивників. Це відбувається в той час, коли Національна кіберстратегія адміністрації Трампа явно переходить від переважно оборонної позиції до активного переслідування хакерів з національних держав, підкріпленого пакетом витрат у розмірі 1 мільярда доларів на наступальні операції…

Twenty, яка також залучила 38 мільйонів доларів у рамках раунду фінансування серії A під керівництвом Caffeinated Capital за участю In-Q-Tel, є першим стартапом, що спеціалізується виключно на кібервійні та зосереджується на створенні інструментів штучного інтелекту для військових хакерів. Її технологія призначена для перетворення робочих процесів, які «раніше вимагали тижнів ручної праці, на автоматизовані, безперервні операції», допомагаючи аналітикам виявляти вразливі місця в мережах супротивника та обробляти величезні обсяги даних про цілі. Користуючись цією стратегічною зміною, генеральний директор Джо Лін застерігає, що «сліпе використання штучного інтелекту є програшною пропозицією», підкреслюючи необхідність відповідального впровадження та ширшої суспільної дискусії про автономність систем озброєння. Зростання стартапу збігається з посиленням занепокоєння щодо загроз з боку супротивників, прикладом чого є китайські хакери, які використовують моделі штучного інтелекту для автоматизації вторгнень, та визнана нестача персоналу, через яку кібервійська США значно поступаються чисельністю…» ***(Margi Murphy. US Military Hackers Go on Offense With Help From Cyber Startup // Bloomberg L.P. (https://www.bloomberg.com/news/articles/2025-11-20/cyber-warfare-startup-nabs-contracts-to-give-us-military-hackers-ai-tools). 20.11.2025).***

***

«Національний центр телекомунікаційної безпеки Пакистану (NTSOC) зафіксував найнапруженіший період у своїй історії, відреагувавши на понад 2800 сповіщень про порушення безпеки та виявивши понад 3000 кібератак на урядові та телекомунікаційні системи. В останньому звіті висвітлено кілька тривожних тенденцій: понад 300 випадків витоку даних, що зачепили організації державного сектору та критичної інфраструктури, а також виявлення близько 4000 скомпрометованих облікових даних електронної пошти або мережі, що належать працівникам урядових та телекомунікаційних організацій. Більшість вторгнень були пов'язані зі спробами спірфішингу та несанкціонованого доступу…

Спільно з місцевими інтернет-провайдерами NTSOC заблокував понад 200 зловмисних дій, що походили з Пакистану, перервавши трафік-зонди та спроби експлуатації, які могли бути використані як стартові майданчики для більш масштабних атак. Центр також працював цілодобово під час індійсько-пакистанського «цифрового конфлікту» в травні 2025 року, допомагаючи

стримувати атаки, спрямовані на телекомунікаційну інфраструктуру Пакистану, та демонструючи важливість моніторингу загроз у режимі реального часу…

Незважаючи на різке зростання кількості атак, оборонна позиція Пакистану покращується: країна піднялася з 79-го на 40-те місце в глобальному рейтингу кібербезпеки, що, на думку офіційних осіб, пов'язано з поліпшенням обміну інформацією про загрози, модернізацією інфраструктури моніторингу та новими національними кібер-рекомендаціями. Щоб ще більше посилити захист, Телекомунікаційне управління Пакистану опублікувало комплексну стратегію протидії DDoS-атакам, стандартизувавши протоколи реагування для критичної національної інфраструктури.

NTSOC продовжує сканувати фішингові кампанії, шкідливий трафік та індикатори витоку даних у даркнеті, одночасно надаючи консультації як державному, так і приватному секторам. Влада заявляє, що наступними пріоритетами є розширення штату фахівців з кібербезпеки та модернізація інфраструктури, щоб засоби захисту могли йти в ногу з дедалі більш витонченими зловмисниками, які націлені на зростаючий цифровий слід Пакистану…» ***(Rizwana Omer. PTA Blocks Over 3,000 Cyberattacks as Pakistan Climbs to 40th in Global Cybersecurity Ranking // PhoneWorld (https://www.phoneworld.com.pk/pta-ntsoc-blocks-3000-cyber-attacks-pakistan-cybersecurity-ranking/). 20.11.2025).***

***

Кіберзахист критичної інфраструктури

«Нові звіти, отримані на підставі запитів про доступ до інформації, показують, що з січня 2024 року британські об'єкти питного водопостачання стали об'єктом п'яти успішних кібератак, що є рекордом за будь-який дворічний період, згідно з даними Інспекції питного водопостачання. Хоча ці інциденти не порушили постачання безпечної води, вони успішно порушили роботу критично важливих організацій, підкресливши серйозну потенційну загрозу, яку зловмисні хакери становлять для суспільства. Загроза є багатогранною: окрім державних суб'єктів, які націлені на критичну інфраструктуру, поширеними є атаки з фінансовою мотивацією, такі як вимога викупу у 2024 році на суму понад 3 мільйони фунтів стерлінгів від Southern Water за витік даних… Це відображається в глобальному масштабі, коли хактивісти втручаються в онлайн-системи, що контролюють водопостачання, енергопостачання та сільськогосподарські об'єкти, порушення роботи яких може мати летальні наслідки. Експерти попереджають, що будь-яка атака на критичну інфраструктуру має на меті привернути увагу ЗМІ та порушити роботу громадських служб, підкреслюючи, що організації повинні бути пильними як щодо загроз з боку розвинених держав, так і щодо опортуністичних, менш витончених атак, оскільки ці інциденти фактично є «випробуванням ґрунту» для потенційних масштабних порушень…» ***(Ellen Jennings-Trace. Experts warn UK's basic infrastructure at risk after hackers target drinking water suppliers // Future US,***

Inc. (https://www.techradar.com/pro/security/experts-warn-uks-basic-infrastructure-at-risk-after-hackers-target-drinking-water-suppliers). 04.11.2025).

***

«…На 8-му Форумі з кібербезпеки в Брюсселі європейські лідери в галузі енергетики, технологій та безпеки дійшли згоди, що захист критичної інфраструктури став суспільним обов'язком, а не лише технічним завданням. Війна в Україні підкреслила, як кібератаки на енергомережі можуть спричинити загальнонаціональну недовіру, економічний параліч та геополітичний тиск. Регулюючі органи, такі як Європейська комісія та ENISA, наполягали на тому, що політика сама по собі не може протистояти цій загрозі; стійкість залежить від постійної міжгалузевої координації, можливості бачити в режимі реального часу промислові мережі та спільного використання інформації про загрози операторами, постачальниками та урядами…

Форум також висвітлив загрозливу вразливість: швидко зростаюча мережа енергетичних пристроїв для споживачів — зарядні пристрої для електромобілів, домашні акумулятори, фотоелектричні інвертори — які до 2030 року можуть сукупно досягати сотень гігават контрольованої потужності. Без вбудованої безпеки кожне підключення до домашньої мережі стає точкою входу для масштабних збурень. Доповідачі стверджували, що сучасна оборона тому переходить від «будівництва вищих стін» до досягнення глибокої інфраструктурної розвідки — картографування ворожих доменів, кореляції ворожої інфраструктури та нейтралізації кампаній до того, як вони досягнуть операційних систем. В епоху, коли кожний вольт, пакет і датчик мають значення, захист електромереж, водопостачання та транзитних ліній є фундаментальним для збереження довіри громадськості та безпеки людей…» ***(David Ratner. Securing the Modern Grid: Why Infrastructure Intelligence is Required for Critical Infrastructure // HYAS Infosec Inc. (https://www.hyas.com/blog/securing-the-modern-grid-why-infrastructure-intelligence-is-required-for-critical-infrastructure). 04.11.2025).***

***

«Eviden, бренд групи Atos, що спеціалізується на передових обчислювальних технологіях та кібербезпеці, виграв проект Європейського центру компетенції та мережі з кібербезпеки (ECCC), спрямований на посилення захисту та стійкості критичної інфраструктури Європи. В рамках цієї ініціативи Eviden очолить CIPHER (Cybersecurity Intelligence, Protection and Holistic Enterprise Resilience), консорціум із 13 членів із семи країн ЄС, до якого входять оператори інфраструктури, дослідницькі організації та малі та середні підприємства у сфері кібербезпеки. CIPHER надасть постачальникам основних послуг стандартизовану платформу для співпраці з метою тестування, перевірки та сертифікації їхнього рівня безпеки, тим самим допомагаючи їм відповідати більш суворим вимогам щодо управління та ризик-менеджменту, передбаченим директивою NIS 2…

Eviden розробить та інтегрує два основні компоненти платформи, що базуються на штучному інтелекті: (1) автоматизований механізм оцінки вразливості,

який безперервно сканує системи, включаючи інтерфейси Wi-Fi, 4G та 5G, на предмет неправильних налаштувань та відомих недоліків, збагачує результати даними про загрози та визначає пріоритетність ризиків; та (2) автоматизовану систему тестування на проникнення, яка координує роботу відкритих і спеціальних інструментів для виконання масштабованих симуляцій реальних атак у мережах, додатках і радіошарах, передаючи результати до механізму оцінки ризиків і модуля рекомендацій. Усі агенти штучного інтелекту відповідатимуть вимогам Закону ЄС про штучний інтелект та GDPR, а проект відповідатиме етичним і екологічним принципам ЄС, включаючи практики циркулярної економіки та енергоефективності, щоб мінімізувати вплив ІКТ на довкілля та підвищити загальну кіберстійкість Європи». ***(Eviden selected by the European Cybersecurity Competence Center and Network for its solutions for testing the cyber resistance of critical systems // yahoo!finance (https://finance.yahoo.com/news/eviden-selected-european-cybersecurity-competence-100000437.html). 20.11.2025).***

***

«Критична інфраструктура — енергетика, водопостачання, транспорт, охорона здоров'я, виробництво — працює на системах OT/ICS, які зараз є головними цілями кібератак. Національні держави, угруповання, що займаються вимаганням викупу, та хактивісти можуть використовувати застаріле обладнання, плоскі мережі та власні протоколи, щоб спричинити фізичні порушення та поставити під загрозу громадську безпеку. Уряди відреагували на це більш жорсткими правилами: Закон ЄС про кіберстійкість та NIS2, майбутній законопроект Великобританії про кібербезпеку та стійкість, рекомендації CISA/NIST США та ініціативи Всесвітнього економічного форуму вимагають від операторів перейти від формального дотримання вимог до повної кіберстійкості…

Справжня стійкість означає більше, ніж просто брандмауери; вона охоплює чотири можливості:

Передбачення: постійний аналіз загроз, оцінка ризиків, специфічних для операційних технологій, планування сценаріїв.

Стійкість: глибока оборона, сегментація та захищені системи, що забезпечують безперебійну роботу основних процесів під час атак.

Відновлення: перевірені плани реагування на інциденти та відновлення, що відповідають вимогам промислової безпеки.

Адаптація: навчання після інцидентів, постійне навчання та культура постійного вдосконалення…

Для досягнення цієї мети організації повинні створити три взаємодоповнюючі основи:

• Комплексна видимість – неінтрузивне виявлення та картографування всіх IT- та OT-активів, їх конфігурації, залежностей та ролі в критичних процесах.

• Постійне виявлення – цілодобовий моніторинг вразливостей, аномалій у поведінці та інформації про загрози в конкретному секторі з використанням штучного інтелекту, налаштованого для OT, щоб мінімізувати помилкові тривоги.

• Практичні висновки – інформаційні панелі ризиків, які перетворюють технічні висновки на операційні пріоритети, направляючи проактивні виправлення та швидку реакцію з урахуванням бізнес-інтересів…

Ці основи забезпечують проактивну оборону, швидше стримування та обґрунтоване прийняття рішень на виконавчому рівні. У міру посилення глобального регулювання та ускладнення атак, впровадження цього циклу «видимість-виявлення-дія» стає необхідним для забезпечення безперебійного енергопостачання, чистоти води, функціонування транспорту та системи охорони здоров'я — незалежно від того, наскільки ворожим стає кіберсередовище». ***(Anton Shipulin. Building Cyber Resilience is Imperative for Critical Infrastructure in a Contested Digital World // AI Journal (https://aijourn.com/building-cyber-resilience-is-imperative-for-critical-infrastructure-in-a-contested-digital-world/). 21.11.2025).***

***

«У 2025 році критична національна інфраструктура Великобританії — енергетичні мережі, водопровідні станції, транспорт, охорона здоров'я — стикається з безпрецедентним кібертиском: одне дослідження налічує 13 атак щосекунди, багато з яких здійснюються групами, що фінансуються державою. Успішна атака може призвести до відключення електроенергії, затримки пасажирів, витоку даних споживачів і збитків на сотні мільйонів. Цифровізація, хоча і є необхідною для ефективності та сталого розвитку, розширює площу атаки; підключені пристрої OT/ICS успадковують вразливість від IT-мереж…

Основні слабкі ланки:

• Ланцюги постачання. Хакери все частіше зламують системи постачальників програмного забезпечення, хостингових компаній та інших третіх сторін, а потім проникають у мережі операторів. EU NIS2 та майбутній британський законопроект про кібербезпеку та стійкість змусять постачальників розкривати вразливі місця та виконувати більш суворі вимоги щодо безпеки.

• Люди. Фішинг все ще є причиною 85 % порушень, а генеровані штучним інтелектом депфейки роблять соціальні інженерні афери все більш переконливими. Розділення IT та OT і постійне навчання персоналу мають вирішальне значення…

Цифрові засоби захисту:

• Штучний інтелект для добра: моделі машинного навчання стежать за аномаліями та рекомендують швидкі заходи для їх усунення.

• Цифрові двійники: перевірені віртуальні копії проводять тести на проникнення та моделюють гіпотетичні сценарії, що дозволяє постійно оптимізувати засоби захисту як під час експлуатації, так і на етапі проектування.

• Стандарти, такі як IEC 62443, та практики безпечного проектування пропонують еталон для апаратного забезпечення, вбудованого програмного забезпечення та процесів інтеграції, забезпечуючи управління виправленнями, зміцнення та контроль облікових даних…

Справжня кіберстійкість вимагає комплексного підходу, що охоплює людей, процеси та технології, безперервну пильність та дотримання мінливих нормативних вимог. Інтегровані рішення, підкріплені сертифікатами та підтримкою спеціалізованих служб, допомагають операторам передбачати, протистояти,

відновлюватися та адаптуватися до постійно мінливих атак на системи, що забезпечують функціонування суспільства». ***(Dale Geach. The hidden fight to secure our critical infrastructure // Siemens (https://www.siemens.com/uk/en/company/stories/the-hidden-fight-to-secure-our-critical-infrastructure.html). 11.2025).***

***

«Канадські системи водопостачання, водовідведення та протипаводкового захисту стикаються з наростаючою хвилею кіберзагроз, попередив Канадський центр кібербезпеки в оцінці, опублікованій у листопаді 2025 року. Хакери — як угруповання, що керуються жадобою наживи, так і групи, що фінансуються державами з країн, які агентство вже згадувало раніше (Китай, Росія, Іран, Північна Корея) — все частіше проникають і, в деяких випадках, вже займають мережі операційних технологій, що контролюють насоси, тиск, дозування хімікатів та шлюзи. В одному з недавніх інцидентів зловмисники змінили значення тиску на муніципальному заводі, погіршивши якість послуг…

Програми-вимагачі вважаються найнебезпечнішими: злочинці знають, що муніципалітети, швидше за все, швидко заплатять, щоб відновити критично важливі послуги. Але Кіберцентр стверджує, що іноземні розвідувальні служби «майже напевно» отримали таємний доступ до канадської водопровідної інфраструктури і можуть саботувати її під час кризи, наприклад, переповнюючи резервуари або отруюючи процеси очищення…

Вразливість пов'язана з підключеними до Інтернету системами управління, які комунальні підприємства впровадили для зручності та економії коштів, але часто недостатньо захищають. Агентство закликає операторів:

• Видалити або обмежити підключення до Інтернету, де це можливо;
• Змінити стандартні паролі та посилити захист пристроїв ОТ;
• Картографувати ризики ланцюга поставок;
• Сегментувати або повністю відокремити мережі управління від ІТ-мереж та публічних мереж…

«Водопровідні системи зараз стикаються з загрозами, на які вони не були розраховані», — заявив керівник Кіберцентру Раджив Гупта. Без рішучих дій навіть невеликі громади можуть зазнати руйнівних перебоїв у постачанні послуг або фізичних збитків». ***(Christopher Nardi. Cyber criminals increasingly targeting Canadians' water, cyber defence agency says // Postmedia Network Inc. (https://ottawacitizen.com/news/politics/cyber-criminals-increasingly-targeting-canadians-water-cyber-defence-agency-says). 25.11.2025).***

***

Кібезахист об’єктів промисловості

«…Критичною проблемою в захисті операційних технологій (ОТ) та промислових систем управління (ICS) є гостра нестача даних про реальні

кібератаки, що заважає ефективному реагуванню та аналізу. На відміну від IT, де стандартом є криміналістичні журнали, дані OT часто є тимчасовими; інструкції виконуються, а потім зникають, що робить криміналістичну експертизу після інциденту майже неможливою без спеціалізованих інструментів моніторингу, які вже встановлені. Цей дефіцит даних створює серйозну проблему, особливо з огляду на те, що державні суб'єкти заздалегідь позиціонують себе в мережах критичної інфраструктури…

Навіть коли дані збираються, складність промислових процесів і загальна незрілість у сфері безпеки OT ускладнюють їх аналіз, оскільки багато операторів все ще не мають базового уявлення про активи у своїх мережах. Хоча компанії, що займаються безпекою OT, публікують звіти про загальні тенденції, вони зобов'язані дотримуватися конфіденційності клієнтів і не можуть ділитися детальною оперативною інформацією… Експерти стверджують, що відсутність публічної інформації може перебільшувати сприйняття загрози, оскільки порушення, пов'язані з IT, часто помилково класифікуються як прямі атаки на OT. Щоб вирішити цю проблему, лідери галузі закликають до створення централізованої анонімної системи обміну даними про атаки на OT, наголошуючи на необхідності кращої координації та стандартизації обміну інформацією між існуючими міжгалузевими платформами, а не створення нових». ***(Shaun Waterman. For OT Cyber Defenders, Lack of Data Is the Biggest Threat // Information Security Media Group, Corp. (https://www.govinfosecurity.com/for-ot-cyber-defenders-lack-data-biggest-threat-a-29959). 07.11.2025).***

***

«Сучасні виробничі ланцюги поставок — це тісно пов'язані між собою мережі IT-, OT- та хмарних систем, що охоплюють десятки постачальників, логістичних компаній та заводів. Ці зв'язки створюють ідеальні точки входу для зловмисників, які часто зламують недостатньо захищені мережі дрібних постачальників, а потім переходять до середовищ більших виробників, де погано контрольовані, не оновлені OT-пристрої можуть порушити виробництво або безпеку.

Виявлення та реагування на мережеві атаки (NDR) — це нова категорія кібербезпеки, яка є особливо важливою для захисту сучасних виробничих ланцюгів постачання, що стають дедалі більш цифровими, взаємопов'язаними та вразливими. На відміну від виявлення та реагування на кінцевих точках (EDR), яке зосереджується на окремих пристроях, NDR забезпечує комплексну видимість шляхом моніторингу та аналізу всього мережевого трафіку — в IT, операційних технологіях (OT) та хмарних середовищах — для виявлення підозрілої поведінки, яка часто походить від менш захищених дрібних постачальників і може поширюватися на більших виробників…

Архітектура NDR базується на шести ключових характеристиках: комплексна видимість мережі; автоматичне виявлення загроз за допомогою штучного інтелекту та поведінкового аналізу; пошук загроз у режимі реального часу; автоматичні засоби реагування, такі як ізоляція сегментів; інтеграція з існуючими засобами безпеки; прозорі та зрозумілі результати. Це робить систему надзвичайно ефективною у

виявленні прихованих загроз, таких як компрометація облікових даних користувачів або захоплення облікових записів, шляхом виявлення незначних аномалій, таких як незвичайні моделі трафіку з пристроїв ОТ, несанкціоновані спроби зовнішнього підключення або нестабільна робота обладнання…

Аналізуючи мережевий трафік в режимі реального часу, NDR може виявляти зловмисну діяльність, яку традиційні інструменти пропускають, включаючи вторгнення на ранній стадії від скомпрометованих постачальників, приховані комунікації команд і контролю, а також потенційне програмне забезпечення для вимагання викупу, перш ніж воно порушить виробництво. Ця можливість є критично важливою у виробництві, де хвилини простою можуть коштувати мільйони. В кінцевому підсумку, NDR підвищує оперативну стійкість, забезпечуючи швидше виявлення та локалізацію загроз у всьому цифровому ланцюжку поставок, захищаючи як виробничі приміщення, так і взаємопов'язані логістичні системи, що забезпечують безперебійність виробництва…» ***(Subo Guha. Redefining Supply Chain Cyber Resilience With Network Detection and Response // Keller International Publishing Corp (https://www.supplychainbrain.com/blogs/1-think-tank/post/42641-redefining-supply-chain-cyber-resilience-with-network-detection-and-response). 20.11.2025).***

***

«Швидке занурення виробництва в Індустрію 5.0 — робототехніку, автоматизацію на основі штучного інтелекту, розумні заводи та глобально пов'язані ланцюги поставок — зробило кібербезпеку однією з найважливіших бізнес-функцій. Сучасні атаки більше не спрямовані лише на викрадення даних; вони порушують роботу операційних технологій (ОТ), виводять з ладу виробничі лінії та використовують вразливість ланцюгів поставок як зброю. Кількість випадків використання програм-вимагачів проти промислових організацій зросла на 87 % минулого року, а середні виплати у виробництві зараз перевищують 1,5 мільйона доларів. Кожен підключений до мережі робот, датчик або постачальник віддаленого доступу стає ще одними дверима для супротивників, як показують приклади зупинки Nucor у травні 2025 року та дефіциту дитячого харчування у 2022 році…

Щоб перейти від реагування на проблеми до справжньої стійкості, виробники повинні:

• Проводити масштабні оцінки безпеки ОТ, що охоплюють як застаріле обладнання, так і системи нового покоління.

• Забезпечити цілісність ланцюга поставок, використовуючи моніторинг на основі штучного інтелекту та суворий доступ на основі ролей для всіх сторонніх сервісних служб.

• Застосовувати архітектури мережі Zero-Trust та SASE/SD-WAN за замовчуванням, щоб кожен користувач, пристрій та додаток постійно проходили повторну автентифікацію.

• Перекласти кіберризики на оперативну мову — години простою, втрачені доходи, шкода репутації — і зробити їх ключовими показниками ефективності (KPI) для правління…

Перехід європейської пекарні на SD-WAN, який усунув перебої в роботі 12 заводів і централізував моніторинг безпеки, демонструє переваги: майже нульовий час простою та простіше управління. Такі проактивні проекти перетворюють кібербезпеку з «страхового поліса» на основну промислову інфраструктуру, необхідну для економічної стійкості Америки та світу в цілому, оскільки виробництво стає все більш цифровим і взаємопов'язаним». ***(Vaibhav Dutta. Protecting productivity: the imperative of cybersecurity in manufacturing // Future US, Inc. (https://www.techradar.com/pro/protecting-productivity-the-imperative-of-cybersecurity-in-manufacturing). 21.11.2025).***

***

«…Промислові середовища управління залишаються вкрай вразливими не тільки через елітних зовнішніх хакерів, а й головним чином через інсайдерів — співробітників, підрядників або скомпрометовані облікові дані — чиї помилки або злісні дії можуть призвести до зупинки критично важливих процесів. Ключові моменти від фахівців з безпеки ОТ:

• Переважають людські помилки. Помилки операторів становлять 80-90 % промислових аварій; недбалі співробітники спричиняють приблизно 56 % порушень. Привілейований персонал ОТ (та сторонні постачальники) часто повторно використовують стандартні паролі, неправильно налаштовують брандмауери або підключають несанкціоновані USB-накопичувачі, що спричиняє дорогі простої та інциденти з безпекою.

• Типи співробітників. Існує три широкі категорії: необережні користувачі, зловмисні співробітники та викрадені або розкриті облікові дані. Мотиви варіюються від поспіху та недостатньої підготовки до фінансової вигоди, невдоволення або державного примусу. В ОТ ставки вищі: одна помилка може зупинити виробництво або поставити під загрозу життя людей, а не тільки призвести до витоку даних…

• Вразливість ланцюга поставок. Зовнішні постачальники, які дистанційно обслуговують PLC та HMI, часто мають такий самий доступ, як і персонал, але слабшу кібердисципліну, що збільшує ризик з боку інсайдерів.

• Нагляд проти довіри. Жорсткий контроль може створити «культуру поліцейського нагляду», що породжує обурення та ухилення від виконання обов'язків. Ефективні програми поєднують цільовий аналіз поведінки з чіткою політикою, орієнтованим на безпеку ведення журналів, підтримкою психічного здоров'я та культурою, в якій співробітники можуть без страху повідомляти про помилки…

• Можливості та обмеження штучного інтелекту. Системи аналізу поведінки можуть виявляти аномальні входи в систему або зміни в програмованих логічних контролерах швидше, ніж люди, але помилкові спрацьовування, шумні телеметричні дані та зловмисники, які розуміють, як працюють ці інструменти, обмежують їхню ефективність. Штучний інтелект повинен доповнювати, а не замінювати надійні засоби контролю процесів та експертну оцінку.

• Найкращі практики.

– Забезпечте повну видимість активів ОТ/ІТ та сегментуйте мережі.

– Застосовуйте принцип мінімальних привілеїв та рольового доступу, особливо для підрядників.

– Включіть усвідомлення внутрішніх загроз до управління, навчань «червоної команди» та тестування управління змінами.

– Створіть культуру поваги та безпеки, щоб «хороші люди залишалися хорошими» і відчували себе в безпеці, висловлюючи свої занепокоєння…

• Прогалини в законодавстві. Такі рамки, як NIST CSF, IEC 62443 та нові закони (NIS2, директиви CISA) торкаються внутрішніх загроз, але все ще недооцінюють людський фактор; організації повинні інтегрувати поведінкові ризики в планування безпеки та стійкості підприємства…

Внутрішній нагляд в ОТ повинен забезпечувати баланс між надійними технічними засобами контролю та аналітикою поведінки, з одного боку, і формуванням довіри, чіткими процедурами та спільною культурою безпеки, з іншого боку, щоб обмежити найбільше джерело промислових кіберризиків». ***(Anna Ribeiro. Rising cost of trust as insider behavior becomes a weak link in critical infrastructure cyber defense // Industrial Cyber (https://industrialcyber.co/features/rising-cost-of-trust-as-insider-behavior-becomes-a-weak-link-in-critical-infrastructure-cyber-defense/). 23.11.2025).***

***

Кіберзахист закладів охорони здоров'я

«Лідери галузі охорони здоров'я США вважають кібербезпеку стратегічною необхідністю для бізнесу, а не лише функцією IT або дотримання нормативних вимог, згідно з опитуванням Ernst & Young LLP (EY US) та KLAS Research (KLAS) «US Healthcare Cyber Resilience Survey», в якому взяли участь 100 керівників. 81% опитаних вважають, що включення кібербезпеки до основної стратегії покращує операційну ефективність та результати. Таку думку формує зростання впливу кіберзагроз: 72% респондентів повідомили про помірні або серйозні фінансові збитки від інцидентів за останні два роки, 60% зазнали операційних перебоїв, а 59% зіткнулися з клінічними наслідками, такими як затримки в лікуванні та підрив довіри пацієнтів. В середньому, протягом минулого року організації стикалися з п'ятьма різними типами загроз, серед яких лідирували фішинг, порушення з боку третіх осіб та шкідливе програмне забезпечення, що підкреслює, чому понад 70% зазнали значних фінансових, операційних або клінічних збитків…

Відповідно змінюються і пріоритети. 68% планують збільшити інвестиції в управління ідентифікацією та доступом в умовах загроз, пов'язаних з штучним інтелектом, і складних екосистем постачальників, а 52% вважають навчання та підвищення кваліфікації персоналу ключовим фактором для реалізації цінності кібербезпеки. У звіті викладено шість основних напрямків діяльності керівництва: узгодження кібербезпеки з бізнес-цілями; оновлення посібників з цифрової ідентифікації для вирішення питань, пов'язаних зі штучним інтелектом та нелюдськими ідентичностями; використання кібербезпеки як засобу для штучного

інтелекту, автоматизації та позалікарняного догляду; вирішення проблеми нестачі талановитих кадрів; перехід від формального дотримання вимог до стратегічного управління ризиками; та перегляд системи контролю ризиків, пов'язаних із третіми сторонами. У дослідженні робиться висновок, що надійна кібербезпека є необхідною для впевненої модернізації — вона сприяє безпечному впровадженню штучного інтелекту та дистанційного медичного обслуговування, захищає конфіденційні дані, забезпечує безперервність медичного обслуговування та зберігає довіру пацієнтів…» ***(EY US-KLAS healthcare cybersecurity survey reveals cyber capability enablement a top business priority // Cision US Inc. (https://www.prnewswire.com/news-releases/ey-us-klas-healthcare-cybersecurity-survey-reveals-cyber-capability-enablement-a-top-business-priority-302602895.html). 03.11.2025).***

***

«Лікарі та медсестри по всій Канаді тихо використовують загальнодоступні інструменти генеративного штучного інтелекту, такі як ChatGPT, Claude, Copilot і Gemini, для складання клінічних записок, перекладу виписок із лікарні та узагальнення даних про пацієнтів. Оскільки ці чат-боти працюють на іноземних серверах, будь-які дані про пацієнтів, введені в них, залишають безпечну мережу лікарні, створюючи ризик «тіньового штучного інтелекту», який обходить брандмауери, системи реєстрації та канадські закони про конфіденційність…

Правила локалізації даних, такі як PIPEDA, були написані задовго до появи генеративної ШІ. Хоча лікарні повинні захищати особисту медичну інформацію, чинні закони майже не згадують про моделі машинного навчання або офшорну обробку даних. Навіть якщо імена видалені, поєднання діагнозів, дат і місць може дозволити повторно ідентифікувати осіб, особливо якщо дані зберігаються або кешуються державним постачальником ШІ, політика зберігання даних і розташування серверів якого є непрозорими…

Таким чином, Shadow AI приєднується до фішингу та програм-вимагачів як одна з основних внутрішніх загроз: випадкові витоки інформації з боку співробітників, які мають добрі наміри. Міжнародні дослідження показують, що приблизно кожен п'ятий лікар загальної практики у Великобританії вже використовує такі інструменти; неофіційні дані свідчать про подібну ситуацію в Канаді. Кожне окреме використання може виглядати нешкідливим, але в сукупності вони утворюють неконтрольований відтік даних, який, на думку страховиків, може стати наступною великою сліпою плямою.

Фахівці з кібербезпеки стверджують, що організації охорони здоров'я потребують трирівневого реагування:

Аудит та розкриття інформації про використання ШІ в ході регулярних перевірок безпеки, розглядаючи це як будь-який ризик, пов'язаний з використанням власних пристроїв.

Пропонування сертифікованих «безпечних для ШІ» шлюзів — затверджених послуг генеративного ШІ, які обробляють дані виключно в канадських центрах обробки даних під суворим контролем та зберіганням.

Інформування персоналу про те, що навіть невеликі фрагменти тексту, вставлені в публічні моделі, можуть порушити конфіденційність…

Ці кроки не заборонять генеративну ШІ, але приведуть повсякденну практику у відповідність до регуляторних вимог і захистять конфіденційність пацієнтів, перш ніж серйозне порушення змусить провести реформи. Без таких заходів найнебезпечніша кіберзагроза для системи охорони здоров'я Канади може прийти зсередини: доброзичливі клініцисти можуть ненавмисно передавати конфіденційні дані глобальним ШІ-системам, що знаходяться поза контролем держави…» ***(Silent cyber threats: How shadow AI could undermine Canada's digital health defenses // This Week In AI (https://thisweekinai.news/2025/11/18/silent-cyber-threats-how-shadow-ai-could-undermine-canadas-digital-health-defenses/). 18.11.2025).***

***

Захист персональних даних та соціальні мережі

«…У зв'язку зі стрімким зростанням вартості порушень безпеки даних, оцінки захисту даних (DPA) стали важливим превентивним інструментом для виявлення та зменшення ризиків кібербезпеки. Закон штату Техас про конфіденційність та безпеку даних (TDPSA), який набирає чинності 1 липня 2024 року, зобов'язує підприємства, що обробляють персональні дані в штаті, проводити DPA, перетворюючи їх із простої форми перевірки відповідності вимогам на стратегічний актив… Закон вимагає від контролерів проводити такі оцінки для видів діяльності з високим рівнем ризику, таких як цільова реклама, продаж персональних даних та обробка конфіденційної інформації, змушуючи підприємства зважувати переваги обробки даних та потенційну шкоду для споживачів. Завдяки обов'язковому проведенню оцінок впливу на захист даних (DPA) закон TDPSA допомагає організаціям проактивно виявляти та усувати вектори кібератак, що призводить до покращення реагування на інциденти, скорочення часу на усунення порушень та значної економії коштів. Ця вимога відповідає зростаючій національній тенденції, оскільки багато інших штатів прийняли подібні закони, спрямовані на зміцнення захисту даних та побудову більш стійкої цифрової економіки в умовах дедалі більш ворожої загрози…» ***(Lynn Rohland. Data Protection Assessments: A New Arsenal for Combating Cyberattacks // Gray Reed Advisory Services LLC. (https://www.grayreedadvisory.com/post/data-protection-assessments-a-new-arsenal-for-combating-cyberattacks). 06.11.2025).***

***

«…Національні закони про локалізацію даних, які вимагають зберігання даних громадян в межах країни, поширюються по всьому світу під гаслом захисту приватного життя та безпеки. Однак ці закони, прийняті такими державами, як Китай, ЄС, Індія та Саудівська Аравія, також обумовлені економічним націоналізмом і можуть створити значні прогалини в кібербезпеці для транснаціональних компаній…

Цей конфлікт ілюструється зростаючим технологічним партнерством між Китаєм і Саудівською Аравією. Сотні китайських компаній, таких як Alibaba і Huawei, виходять на саудівський ринок і мусять дотримуватися суворих законів обох країн щодо захисту даних, часто створюючи окремі паралельні IT-системи. Таке дублювання не тільки виснажує ресурси, але й фрагментує нагляд за кібербезпекою, ускладнюючи централізований моніторинг та реагування на інциденти…

Основна проблема полягає в тому, що конфлікти у сфері дотримання нормативних вимог можуть створювати операційні вразливості. Компанії можуть стикатися з нечіткими межами відповідальності, бути змушені покладатися на затверджених урядом сторонніх постачальників з привілейованим доступом або використовувати непотрібне проміжне програмне забезпечення для управління транскордонними потоками даних. Це може призвести до «неконтрольованих потоків даних» і відсутності місцевих прав на аудит, де, як стверджує експерт Ісмаїл Ахмед, «справжня загроза полягає не тільки в коді, а й у «задніх дверях» у контракті». Для вирішення цієї проблеми потрібен новий підхід, який виходить за межі традиційної периметральної безпеки та дозволяє проактивно управляти системними ризиками, що виникають внаслідок геополітичної та регуляторної невідповідності…» ***(Nate Nelson. Do National Data Laws Carry Cyber-Risks for Large Orgs? // TechTarget, Inc. (https://www.darkreading.com/cybersecurity-operations/national-data-laws-cyber-risks-large-orgs). 20.11.2025).***

***

Масштабні витоки персональних даних

«Шведський орган з захисту приватних даних (IMY) розпочав розслідування щодо постачальника IT-систем Miljödata після кібератаки, в результаті якої були викрадені особисті дані 1,5 мільйона осіб, що становить приблизно половину населення Швеції. Компанія Miljödata, яка обслуговує близько 80% шведських муніципалітетів, повідомила про інцидент, що стався 25 серпня, під час якого зловмисники викрали дані та вимагали 1,5 біткойна. Цей злом спричинив перебої в роботі в багатьох регіонах, а група хакерів Datacarry пізніше взяла на себе відповідальність за цей інцидент, опублікувавши викрадену інформацію, що включає конфіденційні дані, такі як урядові посвідчення, імена та адреси, в даркнеті…

IMY надає пріоритет розслідуванню можливих порушень GDPR, зосередившись на заходах безпеки Miljödata та практиках обробки даних містом Гетеборг, муніципалітетом Ельмхульт та регіоном Вестманланд, приділяючи особливу увагу даним, що належать дітям, особам із захищеною ідентичністю та колишнім працівникам. Керівник IMY Дженні Бард підкреслила, що масштабний витік даних викликає серйозні питання щодо рівня безпеки та типів персональних даних, що зберігаються в уражених системах, і наголосила на необхідності виявлення недоліків, які можуть зменшити ризик подібних інцидентів у майбутньому…» ***(Bill Toulas. Data breach at major Swedish software supplier impacts 1.5 million // Bleeping Computer® LLC***

(https://www.bleepingcomputer.com/news/security/data-breach-at-major-swedish-software-supplier-impacts-15-million/). 04.11.2025).

***

«Японський медіагігант Nikkei зазнав витоку даних після того, як шкідливе програмне забезпечення заразило комп'ютер співробітника, скомпрометувавши платформу обміну повідомленнями Slack компанії та розкривши особисту інформацію понад 17 000 співробітників і ділових партнерів. Експерт з безпеки Mayank Kumar з DeepTempo охарактеризував цю атаку як сучасний цикл атаки, що переходить від скомпрометованого кінцевого пристрою до високоцінного додатка SaaS, основною метою якого є крадіжка дійсних облікових даних… Опинившись всередині Slack, зловмисники «живуть за рахунок ресурсів», імітуючи законних співробітників, що дозволяє їм обходити традиційні засоби безпеки на основі сигнатур, такі як SIEM, NDR (завдяки зашифрованому трафіку) та UEBA (якщо активність була «низькою і повільною»). Кумар підкреслив, що цей інцидент демонструє необхідність еволюції засобів виявлення загроз безпеки від розпізнавання відомого шкідливого програмного забезпечення до виявлення зловмисних намірів у міру їх виникнення, навіть у аутентифікованих користувачів, зазначивши, що викрадений пароль не повинен призводити до катастрофічного порушення безпеки. Це порушення є другим серйозним інцидентом безпеки для Nikkei за останні роки після втрати 29 мільйонів доларів у результаті атаки на бізнес-електронну пошту в 2019 році…» ***(Tim Sandle. Nikkei struck by cyberattack after employee error // DIGITAL JOURNAL INC. (https://www.digitaljournal.com/tech-science/nikkei-struck-by-cyberattack-after-employee-error/article). 04.11.2025).***

***

«Компанія Illuminate Education, що займається освітніми технологіями, виплатить штраф у розмірі 5,1 мільйона доларів за звинуваченнями в тому, що її неналежні заходи безпеки призвели до масштабного витоку даних у 2021 році. В результаті витоку були розкриті конфіденційні дані мільйонів студентів у 49 штатах, включаючи імена, расові ознаки, кодовані медичні стани та статус спеціальної освіти…

Згідно з прес-релізом генеральних прокурорів Каліфорнії, Коннектикуту та Нью-Йорка, порушення безпеки включали невидалення облікових даних колишніх співробітників (які хакер використовував для доступу), відсутність моніторингу систем на предмет підозрілої активності та зберігання резервних баз даних в тій самій мережі, що й активні, що дозволило їх також зламати. Компанію також звинуватили у наданні неправдивих відомостей у своїй політиці конфіденційності.

В рамках угоди компанія Illuminate погодилася посилити свою безпеку шляхом вдосконалення контролю доступу, впровадження моніторингу в режимі реального часу та розділення резервних і активних баз даних. Згодом компанія була придбана Renaissance, яка заявила, що інтегрувала продукти Illuminate у свою власну надійну програму кібербезпеки…» ***(Suzanne Smalley. Edtech company fined $5.1 million for poor data security practices leading to hack // Recorded Future News***

(https://therecord.media/ed-tech-company-fined-5-million-data-breach-security-practices). 06.11.2025).

***

«15 жовтня 2025 року Британське управління з питань інформації (ICO) наклало штраф у розмірі 14 мільйонів фунтів стерлінгів на Capita Group (8 мільйонів фунтів стерлінгів на Capita plc як контролера та 6 мільйонів фунтів стерлінгів на її дочірню компанію Capita Pension Services Limited як обробника) за серйозні порушення статей 5(1)(f) та 32 Британського GDPR після масштабної кібератаки в березні 2023 року. В результаті атаки були викрадені персональні дані понад шести мільйонів осіб з більш ніж 300 пенсійних програм, включаючи дані особливої категорії, відомості про судимості та фінансову інформацію…

Цей штраф у розмірі 14 мільйонів фунтів стерлінгів — один з найбільших, які коли-небудь накладалися ICO за інцидент у сфері кібербезпеки — спочатку становив 58 мільйонів фунтів стерлінгів, але був значно зменшений після того, як Capita визнала порушення, погодилася не подавати апеляцію та отримала додаткову знижку, щоб уникнути «подвійного покарання» двох компаній групи за ті самі основні порушення…

ICO виявило низку системних недоліків, які зробили порушення особливо серйозним:

відсутність управління привілейованим доступом (PAM), багаторівневої системи облікових записів та контролю мінімальних привілеїв, що дозволило швидко розширити привілеї та здійснити латеральне переміщення;

відомі вразливості, які не були усунені, що ICO назвало «особливо серйозним» та доказом того, що Capita свідомо прийняла ризик;

58-годинна затримка у реагуванні на високопріоритетне попередження про безпеку, яке було подано протягом десяти хвилин після початкового порушення;

недостатнє тестування на проникнення, при цьому ICO наголошує, що сканування вразливостей не є заміною і що зрілі організації повинні мати комплексні програми тестування на проникнення, засновані на ризиках, пропорційні чутливості оброблюваних даних…

У рішенні неодноразово згадуються провідні стандарти (рекомендації NCSC, CIS Controls IG3, ISO 27001, NIST CSF, MITRE ATT&CK) і чітко зазначено, що ICO оцінюватиме організації відповідно до цих стандартів, їхніх внутрішніх політик і цілей реагування на тривоги, а також «сучасного рівня» практик безпеки. До великих, досвідчених організацій, таких як Capita, застосовуються відповідно вищі стандарти.

Важливо, що ICO відхилило аргумент Capita про те, що виправлення ситуації після інциденту робить штраф непотрібним, заявивши, що все ще необхідні значні поліпшення і що виправлення ситуації після факту може саме по собі бути доказом попередньої неспроможності. Материнська компанія Capita plc також була визнана безпосередньо відповідальною, незважаючи на те, що дочірня компанія встановлювала загальні для всієї групи політики безпеки, підкресливши, що

внутрішньогрупові домовленості не отримують особливого поблажливого ставлення і повинні розглядатися на умовах рівноправності…

Цей випадок свідчить про явне посилення позиції ICO щодо кіберінцидентів, особливо в тих випадках, коли йдеться про великі обсяги конфіденційних даних і коли організації не вжили заходів щодо відомих ризиків. Він також показує, що раннє визнання відповідальності та укладення угоди можуть призвести до значного зменшення штрафів. Для керівників служб інформаційної безпеки, технічних директорів та правлінь компаній це має однозначне значення: надійне управління, суворе впровадження визнаних технічних засобів контролю (зокрема PAM, швидке оповіщення та комплексне тестування на проникнення) та проактивне ставлення до ризиків, а не їх прийняття, є тепер обов'язковими вимогами згідно з британським GDPR». ***(Andrew Moir, Peter Dalton and Miriam Everett. ICO fines Capita £14 million for data breaches // Herbert Smith Freehills Kramer LLP (https://www.hsfkramer.com/notes/cybersecurity/2025-posts/ico-fines-capita-14m-for-data-breaches#page=1). 14.11.2025).***

***

«Служба доставки їжі DoorDash зазнала витоку даних, який торкнувся мільйонів користувачів у США, Канаді, Австралії та Новій Зеландії, після того, як співробітник став жертвою соціальної інженерії, що надала хакеру доступ до внутрішніх систем компанії. Серед викрадених даних — імена, фізичні адреси, номери телефонів та адреси електронної пошти, хоча компанія заявляє, що конкретна інформація різниться залежно від користувача, і наполягає, що конфіденційні дані не були викрадені…

Однак експерти з кібербезпеки заперечують це, попереджаючи, що такі особисті дані надають злочинцям безліч можливостей для цілеспрямованого фішингу, атак з відновленням облікових записів та спаму. Цей випадок викликав додаткову критику через 19-денну затримку в повідомленні клієнтів, протягом якої постраждалі не знали, що їхня інформація була розкрита. Цей інцидент підкреслює зростаючу загрозу соціальної інженерії, яка базується на маніпулюванні людськими помилками, а не технічними недоліками, і стала основною причиною вторгнень у корпоративні мережі, склавши 36% порушень за останній рік, згідно з даними Palo Alto Networks, що ставить DoorDash в один ряд з іншими великими компаніями, які нещодавно постраждали від таких тактик…» ***(David Curry. DoorDash Hit by Cybersecurity Breach, Millions of Users Potentially Exposed // TechnologyAdvice (https://www.techrepublic.com/article/news-doordash-breach-november-2025/). 17.11.2025).***

***

«Іспанська авіакомпанія Iberia почала повідомляти клієнтів про те, що хакери отримали доступ до одного з її сторонніх постачальників і викрали кеш даних про постійних пасажирів. Ця атака, яка є частиною більш широкої хвилі вторгнень, пов'язаних з компаніями, що використовують програмне забезпечення для підтримки клієнтів Salesforce, могла призвести до витоку імен, адрес електронної пошти та номерів програм лояльності, але не даних кредитних карток або паролів.

Інші авіакомпанії, які постраждали від цієї ж кампанії, включають Qantas, Air France і KLM…

Iberia заявляє, що активувала свої протоколи безпеки, як тільки було виявлено вторгнення, і вжила заходів для його локалізації та запобігання повторенню. Хоча фінансові дані не були викрадені, вкрадена інформація може бути використана в фішингових шахрайствах, які спонукають пасажирів розкривати додаткові особисті дані або встановлювати шкідливе програмне забезпечення.

Ця інформація з'явилася через тиждень після того, як на хакерському форумі з'явилася непідтверджена інформація про те, що 77 ГБ внутрішніх технічних документів Iberia виставлено на продаж. Iberia, що входить до складу IAG, якій також належать British Airways, Aer Lingus і Vueling, не прокоментувала цю інформацію…» ***(Mateusz Maszczynski. Spanish Flag Carrier Iberia Admits It's Fallen Victim To A Cyber Attack And Customer Data Has Been Compromised // paddleyourownkanoo.com(https://www.paddleyourownkanoo.com/2025/11/23/spanish-flag-carrier-iberia-admits-its-fallen-victim-to-a-cyber-attack-and-customer-data-has-been-compromised/). 23.11.2025).***

***

Кібербезпека та хмарні технології

«…Згідно з останнім звітом ReliaQuest, ризики, пов'язані з ідентифікацією, становлять найбільшу загрозу безпеці хмарних середовищ підприємств, складаючи 44% дійсних сповіщень про порушення безпеки хмарних середовищ і 33% усіх сповіщень, що генеруються інструментами безпеки. Хакери віддають перевагу атакам на основі ідентифікації, оскільки вони покладаються на дешеві облікові дані з даркнету, можуть легко уникнути традиційних механізмів виявлення та пропонують численні можливості для підробки особи…

У міру перенесення активів підприємств у хмару управління ідентифікацією стало «справжнім сучасним периметром», що вимагає проактивної позиції, яка виходить за межі мережі, включаючи сканування даркнету на предмет скомпрометованих облікових даних співробітників. У звіті підкреслюється, що понад половина підтверджених сповіщень, пов'язаних з ідентифікацією, стосуються підвищення привілеїв, і наголошується, що використання законних, надмірно широких привілеїв є «набагато більш прихованим» методом, ніж використання сканерів вразливостей. Компанія ReliaQuest представила сувору статистику, згідно з якою 99% хмарних ідентифікаторів мають надмірні привілеї, і закликала організації перейти на модель «нульових постійних привілеїв», яка управляє правами користувачів за допомогою аутентифікації «just-in-time». Цей різкий сплеск сповіщень, пов'язаних з ідентифікацією, створює «подвійне навантаження» для команд безпеки, перевантажуючи їх шумом і водночас стаючи основною причиною підтверджених порушень, що призводить до зростання операційних витрат, оскільки для відрізнення нешкідливої діяльності від зловмисних загроз потрібна ручна оцінка…» ***(Eric Geller. Identity-based attacks need more attention in cloud security***

strategies // TechTarget, Inc. (https://www.cybersecuritydive.com/news/cloud-security-identity-attacks-reliaquest/804621/). 04.11.2025).

***

«Нелюдські ідентифікатори (Non-Human Identities, NHI) — облікові записи машин, ключі, токени та сертифікати, що аутентифікують системи одна перед одною — стали наріжним каменем безпеки хмарних технологій. Складаючись із «секретів» (зашифрованих облікових даних) та дозволів, наданих службами призначення, NHI функціонують як паспорти та візи для програмних компонентів… Оскільки сучасні архітектури покладаються на величезну кількість тимчасових служб, контейнерів та автоматизації, організації повинні управляти NHI протягом усього їхнього життєвого циклу: виявляти та класифікувати секрети; забезпечувати доступ з мінімальними привілеями; контролювати поведінку на предмет аномалій; обертати та виводити з експлуатації облікові дані; а також швидко виявляти та усувати вразливості. Цей комплексний підхід усуває постійні розриви між безпекою та НДДКР шляхом вбудовування управління ідентифікацією машин у DevOps та інженерію платформ, а не покладаючись на фрагментовані точкові інструменти, такі як автономні сканери секретів.

Ефективне управління NHI зменшує ризик порушення, покращує дотримання вимог (завдяки впровадженню політик та аудиторським слідом), підвищує ефективність завдяки автоматизації (наприклад, доступ «точно вчасно», ротація секретів), покращує видимість та контроль завдяки централізованому нагляду, а також знижує операційні витрати завдяки усуненню ручних, схильних до помилок робочих процесів… Найбільше виграють сектори, що працюють з конфіденційними даними — фінансові послуги, охорона здоров'я, туризм та команди SOC/DevOps, але кожна організація, що надає перевагу хмарним технологіям, отримує стійкість, розглядаючи NHI як першокласні об'єкти безпеки. Сучасні рішення все частіше використовують AI/ML для контекстного моніторингу, виявлення відхилень від нормального використання та запуску цільових реакцій, тоді як функції платформи, такі як динамічне видавання секретних даних (наприклад, підходи на основі сховищ), мінімізують постійні привілеї та зменшують радіус ураження…

Впровадження цієї системи супроводжується певними викликами: інтеграція платформ із застарілою інфраструктурою, узгодження вимог до управління та регулювання (GDPR, HIPAA, PCI-DSS) із комплексним веденням журналів та звітності, а також управління змінами шляхом постійного навчання та залучення зацікавлених сторін. Організації повинні встановити чіткі політики щодо ролей, обов'язків, контролю доступу, реагування на інциденти та можливості аудиту, а також провести аналіз витрат і вигод, зваживши початкові інвестиції та зменшення кількості випадків шахрайства, втрати даних та оптимізацію операцій. У міру зростання хмарних та периферійних екосистем, а також перетворення ідентичності на фактичний периметр, пріоритетність безагентних, адаптивних та інтегративних рішень NHI — у поєднанні з мінімальними привілеями, нульовими постійними привілеями та контекстно-орієнтованими засобами контролю — перетворює ідентичності машин із пасивів на безпечну основу для сумісних, масштабованих та

стійких хмарних середовищ…» ***(Angela Shreiber. Are Your Cloud Secrets Truly Protected? // Techstrong Group Inc. (https://securityboulevard.com/2025/11/are-your-cloud-secrets-truly-protected-2/). 02.11.2025).***

***

«CrowdStrike під керівництвом генерального директора Джорджа Курца перепозиціонує себе як «гіпермасштабований постачальник послуг безпеки» — новий тип компанії, побудований на основі хмарної платформи Falcon та революційної моделі передплати під назвою Falcon Flex. Ця стратегія, яка віддзеркалює успіх гігантів публічної хмари, таких як AWS, покликана значно прискорити зростання як CrowdStrike, так і її партнерів по каналах збуту, спростивши масштабування засобів захисту…

Цей підхід базується на двох принципах. По-перше, платформа Falcon — це єдина архітектура, що працює виключно в хмарі та використовує один програмний агент для розгортання понад 30 різних модулів безпеки, від захисту кінцевих точок до ідентифікації та безпеки хмари. Ця модель «одноразового збору та багаторазового використання» дозволяє миттєво додавати нові можливості. По-друге, модель передплати Falcon Flex дозволяє клієнтам заздалегідь визначити рівень витрат, а потім поступово використовувати різні продукти, що забезпечує гнучкість і економію коштів. Це стало потужним фактором зростання, що дозволило таким партнерам, як SHI і GuidePoint Security, досягти мільярдних обсягів продажів і перетворити багатомільйонні угоди на контракти вартістю понад 100 мільйонів доларів…

Поєднуючи уніфіковану технологічну платформу з гнучкою бізнес-моделлю, схожою на гіпермасштабовану, CrowdStrike прагне стати «операційною системою кібербезпеки». Ця стратегія виявляється надзвичайно ефективною, розширюючи присутність компанії з великих підприємств на ринок малого та середнього бізнесу і позиціонуючи її як лідера наступної ери безпеки, включаючи використання штучного інтелекту…» ***(Kyle Alspach. 'Flexing' Its Muscle: CrowdStrike CEO Kurtz Says It's The First 'Hyperscaler Of Security' // The Channel Company (https://www.crn.com/news/cover-story/flexing-its-muscle-crowdstrike-ceo-kurtz-says-it-s-the-first-hyperscaler-of-security). 20.11.2025).***

***

«Оскільки хмарна інфраструктура стає основою корпоративних IT-систем, забезпечуючи критично важливі робочі навантаження для понад 94% великих організацій, кількість кіберінцидентів, пов'язаних із хмарними активами, значно зросла. За даними Unit42, майже 29% розслідувань у 2024 році були пов'язані з хмарними або SaaS-системами. Ця зміна вимагає спеціалізованого підходу до цифрової криміналістики, відомого як хмарні розслідування, який використовує аудиторські сліді, такі як AWS CloudTrail та Azure Activity Logs, для реконструкції інцидентів, відображення поведінки зловмисників та виявлення порушень, які часто спричинені неправильною конфігурацією або зловживанням ідентифікаційними даними. Реальні приклади, такі як порушення безпеки в Capital One та Uber, підкреслюють критичну важливість аналізу журналів провайдерів,

ролей IAM та активності API для відстеження шляхів атак, що використовують конкретні вразливості хмарних технологій…

Однак розслідування в хмарі стикаються з унікальними викликами порівняно з традиційною криміналістикою, зокрема через мінливість середовищ з автоматичним масштабуванням, де тимчасові докази можуть миттєво зникнути, а також через складність нормалізації даних на мультихмарних платформах з різними форматами журналів. Щоб подолати ці перешкоди, команди з безпеки все частіше використовують автоматизовані інструменти, системи CSPM та уніфіковані платформи XDR, які оптимізують збір доказів і корелюють дані в AWS, Azure та GCP. У майбутньому, у міру розвитку автоматизації та машинного аналізу для обробки величезних обсягів даних журналів, хмарні розслідування стануть незамінною опорою сучасної кібербезпеки, необхідною для підтримки операційної стійкості та відповідності вимогам у гібридному, мультихмарному світі…» ***(Cloud Investigations: The New Backbone of Modern Cybersecurity // Demand Media BPM (https://ittech-pulse.com/our-tech-insights/cloud-investigations-the-new-backbone-of-modern-cybersecurity/). 17.11.2025).***

***

«Хмарні обчислення кардинально змінили підхід до кібербезпеки порівняно з традиційними внутрішніми центрами обробки даних, де системи, межі та активи, що підлягають захисту, були чітко визначені. У хмарі організації працюють у спільному, менш відчутному середовищі, де інфраструктура частково контролюється зовнішніми постачальниками, що ускладнює застосування та моніторинг заходів безпеки… Основні цілі залишаються незмінними — конфіденційність, цілісність і доступність даних та послуг — але для їх досягнення потрібно приділити особливу увагу трьом ключовим напрямкам: надійний захист даних у спільних середовищах, посилення конфігурацій хмарних середовищ для мінімізації ризиків та забезпечення достатньої видимості й простежуваності, незважаючи на абстрактність і спільну інфраструктуру. Хмарні послуги не є безпечними «за замовчуванням», тому неправильні налаштування, слабкий контроль доступу та погано керовані авторизації можуть залишити критичні ресурси незахищеними, а зменшені можливості реєстрації або моніторингу порівняно з локальними системами можуть затуманити шляхи атак…

Ще одна істотна відмінність полягає у зміні периметра: замість чітко обмеженої внутрішньої мережі хмарні системи розширюються назовні, постійно взаємодіючи із зовнішніми службами та користувачами, що змушує команди з безпеки постійно перевіряти, звідки походять з'єднання та чи є вони законними. Водночас відповідальність за безпеку тепер розділяється з хмарними провайдерами, які забезпечують безпечну базу, але не охоплюють усі рівні, тому клієнти повинні розробляти надійні архітектури та застосовувати власні засоби контролю. Сама хмарна кібербезпека швидко еволюціонувала: спочатку вона викликала недовіру і використовувалася лише для некритичних робочих навантажень, а організації намагалися відтворити традиційні моделі безпеки. У міру того, як провайдери посилювали власні засоби захисту, стало зрозуміло, що багато ризиків пов'язані не стільки з витонченими експлойтами, скільки з неправильною конфігурацією

клієнтів, що підкреслює необхідність вбудовувати безпеку в хмарні архітектури з самого початку. Сьогодні широке поширення автоматизації та використання шаблонів, «планів» і, все частіше, штучного інтелекту дозволяє розгортати середовища з попередньо визначеними стандартами безпеки, що дає командам можливість швидко керувати властивим хмарі «хаосом» без створення вузьких місць і зосередитися більше на стратегічному управлінні ризиками, ніж на ручній конфігурації…» ***(Daniel Consentini. How are cybersecurity and the cloud related? // Telefónica S.A. (https://www.telefonica.com/en/communication-room/blog/cybersecurity-cloud-related/). 19.11.2025).***

***

«У міру того як підприємства впроваджують мультихмарні архітектури на базі AWS, Azure та Google Cloud, складність забезпечення безпеки випередила традиційні моделі захисту, що робить кіберстійкість стратегічним завданням на 2026 рік. Тому кіберстійкість — здатність передбачати загрози, протистояти атакам, швидко відновлюватися та підтримувати роботу критично важливих служб — стала вимогою на рівні правління...

Основні виклики в області безпеки мультихмарних середовищ

• Фрагментація ідентичності: кожна хмара має власну систему управління ідентифікацією та доступом (IAM), що призводить до непослідовності політик і робить її головним об'єктом атак зловмисників.

• Ізольована видимість і повільна реакція на інциденти: розрізнені журнали перетворюють виявлення на ручну роботу, що займає години.

• Плоскі моделі довіри та статичні засоби контролю, які не можуть слідувати за динамічними робочими навантаженнями.

• Зростання кількості атак на основі ідентичності — у 2024 році Google зафіксував їх зростання на 400 % — та порушень безпеки в мультихмарних середовищах, які коштують на 32 % дорожче, ніж інциденти в однохмарних середовищах…

Вимоги до стійкої архітектури:

1 / Постійна перевірка ідентичності, застосування мінімальних привілеїв та надійна багатофакторна автентифікація (MFA).

2 / Мікросегментацію мережі та доступ на основі моделі «нульової довіри» у хмарних середовищах для стримування зловмисників.

3 / Наскрізне шифрування даних, маскування та моніторинг витоку даних.

4 / Безпеку додатків на рівні API, середовища виконання та SDLC.

5 / Автоматизовані сценарії, тестування хаосу та міжхмарне відновлення після збою для швидкого відновлення…

Штучний інтелект є одночасно загрозою і засобом захисту. Підприємства використовують аналітику на основі машинного навчання для виявлення аномалій і автоматичного їх усунення, тоді як зловмисники використовують штучний інтелект для прискорення фішингу та виявлення вразливостей. Спостережуваність у поєднанні зі штучним інтелектом забезпечує ситуаційну обізнаність у режимі реального часу в усіх хмарних середовищах.

Zero Trust став основним принципом: не довіряти жодному з'єднанню, застосовувати політику для кожного користувача, пристрою та ресурсу, а також постійно перевіряти.

З організаційної точки зору, компанії повинні перенести акцент з контрольних списків відповідності на вимірюване зниження ризиків, інтегрувати інструменти TPRM та GRC, а також забезпечувати щомісячні брифінги для керівництва. Малі підприємства покладаються на постачальників послуг з управління безпекою; великі підприємства поєднують внутрішні SOC з інструментами на базі штучного інтелекту…

Результати першопрохідців: глобальний постачальник медичних послуг скоротив кількість інцидентів, пов'язаних з ідентифікацією в хмарі, на 70 % і вдвічі скоротив час відновлення після впровадження уніфікованих рівнів ідентифікації, політики нульової довіри та автоматизованого реагування.

Прогнози аналітиків на 2026 рік:

• Кількість атак на мультихмару зросте на 30 %.

• Автоматизоване реагування вдвічі зменшить вплив порушень.

• SOC на базі штучного інтелекту вирішують інциденти на 40 % швидше.

• Кіберстійкість стає ключовим показником ефективності (KPI) для керівництва…» ***(Mohana Chandorkar. Cyber Resilience in a Multi-Cloud World: Redefining Security Architecture for 2026 // ReadITQuik (https://readitquik.com/security-2/cyber-resilience-in-a-multi-cloud-world-redefining-security-architecture-for-2026/). 21.11.2025).***

***

Кібербезпека Інтернету речей. Штучний інтелект

«…Цифрові ідентичності стрімко поширюються всередині організацій під впливом агентів штучного інтелекту та інших нелюдських облікових записів, і цей сплеск змінює характер кіберризиків. Глобальне опитування показує:

• Кількість нелюдських ідентичностей (NHI) зараз перевищує кількість співробітників у співвідношенні 82 до 1.

• 90 % керівників підприємств вважають атаки на основі ідентичності своєю головною проблемою в галузі безпеки; 58 % керівників служб безпеки очікують, що половина порушень безпеки в наступному році буде пов'язана з агентами штучного інтелекту.

• 89 % компаній вже використовують штучний інтелект на основі агентів у своїх системах ідентифікації, а майже всі інші планують зробити це протягом дванадцяти місяців.

• 87 % переоцінюють або замінюють свої платформи IAM; 58 % вказують на прогалини в безпеці навколо NHI.

• 89 % наймуть фахівців з безпеки ідентифікації протягом наступного року…

Впевненість у швидкому відновленні роботи знижується: лише 28 % вважають, що зможуть відновити роботу протягом 12 годин після порушення безпеки ідентифікаційних даних, що на 43 % менше, ніж торік, а 58 % зараз очікують

на дводенне або більш тривале відключення. Програми-вимагачі продовжують діяти — 89 % тих, хто постраждав, заплатили викуп…

Експерти попереджають, що зловмисники все частіше «входять в систему, а не зламують її», використовуючи викрадені або отримані за допомогою соціальної інженерії облікові дані. Тому стійкість залежить від надійного управління ідентифікацією, суворого контролю доступу як для людей, так і для агентів штучного інтелекту, а також від комплексного плану відновлення після інцидентів». ***(Shannon Williams. AI-driven agents spark new identity crisis for cyber security // TechDay (https://securitybrief.asia/story/ai-driven-agents-spark-new-identity-crisis-for-cyber-security). 19.11.2025).***

***

«Агентний ШІ стає наступним великим технологічним проривом, виводячи штучну інтелігенцію за межі чат-ботів і перетворюючи її на автономних виконавців рішень, здатних навчатися, міркувати і діяти самостійно. До 2028 року очікується, що третина корпоративних додатків буде містити агентний штучний інтелект (у порівнянні з <1% у 2024 році), а до 15% рутинних рішень на робочому місці будуть прийматися автономно — це зміна, яка може змінити обличчя кібербезпеки…

Агентні системи штучного інтелекту, що відрізняються від традиційних моделей машинного навчання своєю здатністю працювати ітеративно, адаптуватися до контексту та вдосконалюватися завдяки досвіду, добре підходять для вирішення постійних проблем безпеки. Вони можуть трансформувати центри безпеки (SOC), самостійно досліджуючи рутинні сповіщення, зменшуючи «втому від сповіщень» та скорочуючи вікно вразливості. Вони також покращують тестування на проникнення, виявляючи типові проблеми у великому масштабі, та покращують управління вразливостями, стандартизуючи звіти та рекомендуючи заходи з усунення недоліків, тим самим масштабуючи операції з безпеки попри нестачу талановитих фахівців.

Однак автономність агентного ШІ створює нові критичні ризики, якими керівники підприємств повинні ретельно управляти. Ці ризики включають швидке введення, коли зловмисні інструкції, вбудовані в зовнішні дані, можуть спонукати автономних агентів заподіяти більшої шкоди; ризики доступу до даних та конфіденційності через обробку великих наборів даних; а також джейлбрейкінг, коли зловмисники переконують ШІ ігнорувати обмеження безпеки. Для зменшення ризиків необхідний постійний моніторинг, надійні захисні механізми, ефективне управління даними та постійна робота «червоної команди» для стрес-тестування систем. Застосовуючи агентний ШІ з чітким управлінням та людським наглядом на критичних етапах, організації можуть значно посилити свої захисні можливості, перейти до безперервного управління загрозами та запобігти збільшенню асиметрії між зловмисниками та захисниками…» ***(Michiel Prins. The rise of agentic AI in cybersecurity // Future US, Inc. (https://www.techradar.com/pro/the-rise-of-agentic-ai-in-cybersecurity). 03.11.2025).***

***

«Розумні будівлі, оснащені сотнями підключених до Інтернету датчиків, контролерів і застарілих систем автоматизації, стали головними цілями кібератак. У міру розширення ринку з прогнозованим середньорічним темпом зростання 17 % власники поспішають встановлювати пристрої Інтернету речей, які часто не мають базових засобів безпеки, що збільшує площу атаки. Результат: у 4 кварталі 2022 року було зареєстровано понад 10 мільйонів атак на IoT, а атаки типу «відмова в обслуговуванні» на вразливі пристрої зараз домінують у статистиці інцидентів. До типових слабких місць належать системи автоматизації будівель без оновлень, незахищені мережі та погано сегментовані парки IoT; після проникнення зловмисники можуть перейти до саботажу освітлення, систем опалення, вентиляції та кондиціонування, димових сигналізацій, ліфтів або систем спостереження, що призводить до простоїв, фізичних небезпек, шкоди репутації та багатомільйонних збитків…

Оскільки навіть одне неправильно налаштоване обладнання може зруйнувати навіть найкраще розроблену систему захисту, експерти закликають регулярно проводити симуляції кібератак, щоб виявити приховані прогалини раніше, ніж це зроблять злочинці. Вправи «червоної» та «фіолетової» команд, моделі глибокого підкріплення навчання на основі штучного інтелекту та повноцінні лабораторії кібербезпеки дозволяють захисникам випробовувати реальні тактики без шкоди для операцій. Ефективні симуляції починаються з повного інвентаризації активів, чітких індикаторів компрометації, врахування фізичних та цифрових ризиків, а також включення сценаріїв людських помилок, що є критично важливим, враховуючи, що люди є причиною 95 % порушень…

Часті реалістичні навчання покращують виявлення, вдосконалюють сценарії реагування на інциденти та спрямовують інвестиції на найризикованіші системи, в результаті перетворюючи найбільшу слабкість розумної будівлі — її взаємопов'язаність — на захищену сильну сторону». ***(Ellie Gabel. Simulating Cyberattacks to Strengthen Defenses for Smart Buildings // Techstrong Group Inc. (https://securityboulevard.com/2025/11/simulating-cyberattacks-to-strengthen-defenses-for-smart-buildings/). 07.11.2025).***

***

«У новому звіті IDC «2026 FutureScape: Worldwide Security and Trust» (Майбутнє 2026 року: глобальна безпека та довіра) стверджується, що генеративний та «агентний» штучний інтелект переосмислить поняття корпоративної безпеки протягом наступних п'яти років. Основні прогнози включають:

• До 2028 року агенти штучного інтелекту будуть сортувати 80% сповіщень у більшості центрів безпеки, динамічно створюючи сценарії дій для 85% цих інцидентів.

• До 2027 року фішинг із використанням синтетичної ідентичності — атаки, що поєднують реальні та сфабриковані штучним інтелектом особисті дані — торкнеться 80% організацій. 15% корпоративних ПК будуть працювати на програмному забезпеченні для виявлення глибоких підробок.

• Кількісна оцінка кіберризиків у реальному часі стане нормою: до середини 2028 року 30% платформ виявлення будуть додавати до кожного сповіщення оцінку збитків у доларах, а 40% підприємств використовуватимуть автономні платформи агентів для перетворення показників безпеки у фінансові ризики для бюджетування, проведення комплексних перевірок при злиттях і поглинаннях та звітування перед правлінням…

• Поширюватимуться вимоги щодо суверенної штучної інтелектуальної власності: до 2027 року третина урядів вимагатиме від чутливих секторів використання архітектур «всередині країни» з розширеним пошуком і генерацією (RAG), що змусить підприємства відстежувати специфікації штучного інтелекту на предмет вразливості та дотримання ліцензійних вимог.

• До 2027 року 40% компаній з рейтингу Global 2000 замовлять оцінку квантових ризиків, а до 2029 року 70% великих підприємств перейдуть на приватні хмарні обчислювальні середовища для захисту даних, що використовуються великими мовними моделями, розміщеними в хмарі…

В цілому, прогнози показують, що керівники служб інформаційної безпеки переходять від фрагментарних заходів контролю до стратегій безпеки, що базуються на штучному інтелекті, фінансово обґрунтованих і відповідають вимогам суверенітету, розроблених для того, щоб йти в ногу з атаками, що використовують штучний інтелект, і загрозами квантових технологій…» ***(Tim Sandle. Majority of security operations 'will be run by AI agents' within three years // DIGITAL JOURNAL INC. (https://www.digitaljournal.com/tech-science/majority-of-security-operations-will-be-run-by-ai-agents-within-three-years/article). 07.11.2025).***

***

«Кібератаки зараз відбуваються кожні 39 секунд і коштують американським компаніям в середньому 10,2 мільйона доларів за кожну з них; 70 відсотків з них спрямовані проти малих і середніх підприємств, а 60 відсотків цих жертв закриваються протягом шести місяців. Особливо небезпечним сучасний ландшафт загроз робить штучний інтелект: ШІ дозволяє злочинцям автоматично генерувати бездоганні фішингові повідомлення, підробляти голоси керівників з точністю 98%, орендувати набори програм-вимагачів з ШІ та кожні кілька хвилин переписувати шкідливе програмне забезпечення, щоб уникнути виявлення — настільки ефективно, що 80% інцидентів із програм-вимагачів зараз містять компонент ШІ…

Однак штучний інтелект також може змістити баланс сил на користь захисників. Організації, які використовують платформи безпеки на основі штучного інтелекту, скорочують цикл порушення безпеки на 108 днів і економлять близько 1,9 мільйона доларів на кожен інцидент завдяки більш точному виявленню аномалій, меншій кількості помилкових сповіщень і швидшій автоматизованій реакції…

Щоб не відставати, великі та малі підприємства повинні:

• регулярно проводити аудити безпеки та цикли оновлення;

• встановлювати системи поведінкового аналізу на основі штучного інтелекту та засоби контролю на основі моделі «нульової довіри» (MFA, мікросегментація);

• виводити з експлуатації застарілі системи, застосовувати суворі режими резервного копіювання/незмінності та вести повні інвентаризації даних;

• постійно навчати співробітників, зосереджуючись на виявленні фішингу та депфейків, створених за допомогою штучного інтелекту;

• розробляти та відпрацьовувати план реагування на інциденти відповідно до NIST/SANS та використовувати штучний інтелект для криміналістичного аналізу після порушення безпеки…

Штучний інтелект прискорює атаки, але він також надає інструменти для їх виявлення, локалізації та відновлення з такою ж швидкістю — якщо організації зараз інвестують в інтелектуальні багаторівневі системи захисту та культуру пильності…» ***(Lynn Rohland. AI-Powered Cyberattacks Are Here: How They Are Supercharging Ransomware Attacks and How You Can Mitigate Them // Gray Reed Advisory Services LLC. (https://www.grayreedadvisory.com/post/ai-powered-cyberattacks-are-here-how-they-are-supercharging-ransomware-attacks-and-how-you-can-miti). 06.11.2025).***

***

«Перетворення електромобілів (EV) на підключені, програмно-визначені екосистеми мобільності перетворило сучасну силову установку на критичну кіберфізичну систему, що створює ризики, де цифрові вразливості можуть перетворитися на фізичну небезпеку. Хоча виробники досягли значних успіхів у забезпеченні безпеки інформаційно-розважальних систем, контролери двигунів та інвертори залишаються незахищеними. Завдяки таким важливим функціям підключення, як оновлення через бездротовий канал (OTA) та хмарне прогнозне технічне обслуговування, зловмисники можуть потенційно проникнути в ці системи, щоб маніпулювати крутним моментом, вимкнути рекуперативне гальмування або спричинити перегрів, перетворюючи кіберінцидент на пряму загрозу безпеці пасажирів…

Ця загроза швидко зростає, про що свідчить повідомлення про збільшення на третину кількості кіберінцидентів в автомобільній галузі, спрямованих проти постачальників, телематичних систем та мереж зарядних станцій. Недавні порушення підкреслюють вразливість галузі: у 2024 році вразливість порталу Kia дозволила виконувати несанкціоновані віддалені команди, а дешеві симулятори безключового доступу використовувалися для викрадення автомобілів. Крім того, кібератака 2025 року на серверну інфраструктуру Jaguar Land Rover зупинила виробництво, продемонструвавши, що ризики поширюються не тільки на автомобілі, а й на логістичні та IT-системи, які їх підтримують…

Щоб зменшити ці небезпеки, потрібна комплексна стратегія захисту, яка охоплює апаратне та програмне забезпечення, а також ланцюг постачання. Механізми захисту повинні включати безпечні процеси завантаження, цифрове підписання прошивки та апаратні модулі безпеки (HSM) для захисту ключів шифрування. Архітектура мережі повинна відокремлювати критичні функції силового агрегату від зовнішніх інтерфейсів, а системи виявлення вторгнень (IDS) повинні контролювати аномальну поведінку. Крім того, для оновлень OTA та інфраструктури зарядки необхідно застосовувати надійну аутентифікацію. Зрештою, у міру того, як електромобілі все більше інтегруються в енергомережу та розумні

міста, захист основних компонентів, таких як інвертори, від кіберзагроз є надзвичайно важливим для забезпечення фізичної безпеки та надійності майбутньої мобільності». ***(Cybersecurity risks inside the powertrain: why EVs need defence at the motor level // GlobalData Plc (https://www.just-auto.com/analyst-comment/cybersecurity-risks-inside-the-powertrain-why-evs-need-defence-at-the-motor-level/?cf-view&cf-closed). 20.11.2025).***

***

«Зростаюча роль штучного інтелекту в кібербезпеці посилила дискусії щодо його наступальних можливостей, які нещодавно розпалилися після опублікування звіту Anthropic, в якому стверджувалося, що атака за допомогою штучного інтелекту була «на 90 % автономною» — твердження, яке IBM X-Force інтерпретує як підкреслення критичних змін у ландшафті загроз. Поточні можливості штучного інтелекту в області нападу є в основному побічним продуктом моделей, навчених на загальних наборах даних кодування, але зараз відбувається перехід: організації та супротивники активно створюють спеціальні набори даних для завдань, таких як виявлення вразливостей, мережеві атаки та створення зброї. Ця зміна переводить штучний інтелект від простої демократизації кіберможливостей для менш кваліфікованих учасників до забезпечення складних, експоненціально більш ефективних операцій, коли ці спеціалізовані моделі поєднуються з вдосконаленими наборами даних…

Зростає розрив між відкритим і закритим кодом штучного інтелекту, де досвідчені зловмисники використовують приватні, необмежені моделі, навчені на основі власних даних про атаки, щоб обійти захисні бар'єри, властиві публічним системам. Ці закриті системи дозволяють зловмисникам автоматизувати складні завдання, включаючи управління інфраструктурою, таке як ротація доменів і налаштування корисного навантаження, що дозволяє швидко масштабувати стійкі кампанії. Крім того, поява мультимодальних моделей, здатних інтерпретувати текст, код, зображення та журнали, дозволить ШІ автоматизувати складні розвідку та прийняття рішень, створюючи адаптивні загрози, які можуть картографувати середовища та організовувати багатоетапні атаки з надлюдською швидкістю…

Майбутні кібероперації, ймовірно, будуть поєднувати зусилля людей та штучного інтелекту, причому автономні агенти будуть займатися дослідженням вразливостей, розробкою експлойтів та напівавтономними атаками. Зловмисники вже застосовують такі стратегії, як розбиття шкідливих завдань на нешкідливі фрагменти, щоб обійти сучасні фільтри безпеки штучного інтелекту, що доводить недостатність простих оперативних перевірок. Щоб протистояти цим еволюціонуючим загрозам — від сучасних програм-вимагачів до автоматизованої інфраструктури — спільнота кібербезпеки повинна надати пріоритет дослідженням у галузі оборонного штучного інтелекту, стратегічному діалогу та відповідальному розробленню систем, здатних передбачати та пом'якшувати глибокі можливості наступального штучного інтелекту наступного покоління». ***(Michelle Alvarez, Chris Thompson. Understanding the future of offensive AI in cybersecurity // Ibm***

(https://www.ibm.com/think/x-force/understanding-future-of-offensive-ai-in-cybersecurity). 19.11.2025).

***

«Після виявлення кіберкампанії, в рамках якої група, спонсорована китайським урядом, використовувала штучний інтелект Claude Code від Anthropic для автономного злому приблизно 30 цілей, експерти попереджають, що штучний інтелект створив нову еру кібервійни, яка вимагає захисту на основі штучного інтелекту. Цей інцидент продемонстрував, що загальнодоступний штучний інтелект може діяти як «мультиплікатор сили», виконуючи приблизно 80-90% тактичних операцій — від розвідки до аналізу даних — зі швидкістю, неможливою для людини, що фактично дозволяє одному оператору організовувати численні атаки…

Ця зміна означає, що навіть середньокваліфіковані супротивники тепер можуть здійснювати атаки безпрецедентного масштабу та швидкості, що можна порівняти з «цифровим пострілом з рушниці», який загрожує багатьом вразливим мережам. Хоча ці агенти штучного інтелекту ще не настільки досконалі, щоб проникнути в найбезпечніші системи з повітряним розривом, такі як системи ядерного командування та контролю, вони значно підвищують продуктивність хакерських команд, зберігаючи свої найсучасніші інструменти для найскладніших цілей.

За словами колишнього глави Агентства національної безпеки та Кіберкомандування США Пола Накасоне та інших експертів, головним викликом є те, що оборона повинна наздогнати розвиток технологій. Очікується, що протягом наступних шести місяців буде зроблено значний поштовх до розвитку «агентних кіберзахисних систем», які зможуть автоматично протидіяти цим атакам на основі штучного інтелекту. Однак протистояння алгоритмів один одному з надлюдською швидкістю несе значні ризики, включаючи ненавмисну ескалацію, особливо якщо такі автоматизовані системи будуть націлені на критичну інфраструктуру, таку як системи ядерного командування. Консенсус є очевидним: щоб захиститися від атак на основі штучного інтелекту, захисники повинні терміново інтегрувати штучний інтелект у свої системи, щоб відповідати новій швидкості та масштабу загрози…»
(Sydney J. Freedberg Jr. Chinese use of Claude AI for hacking will drive demand for AI cyber defense, say experts // Breaking Media, Inc. (https://breakingdefense.com/2025/11/chinese-use-of-claude-ai-for-hacking-will-drive-demand-for-ai-cyber-defense-say-experts/). 20.11.2025).

***

«Штучний інтелект змінює кібербезпеку по обидва боки фронту, озброюючи зловмисників швидшими та розумнішими інструментами, а захисникам надаючи нові способи виявлення та блокування загроз. Зараз кіберзлочинці використовують ШІ для автоматизації фішингу за допомогою високо персоналізованих електронних листів, що генеруються великими мовними моделями, для створення переконливих аудіо- та відеоматеріалів з використанням технології deepfake для шахрайства, а також для розробки самонавчального

шкідливого програмного забезпечення, яке адаптується під час атаки. Дослідження SoSafe 2025 року показало, що 87% організацій зазнали кібератаки на основі ШІ протягом попереднього року, і ця цифра, як очікується, зростатиме в міру вдосконалення технології. Водночас команди з безпеки все частіше покладаються на штучний інтелект для виявлення загроз у режимі реального часу, моніторингу на основі поведінки та автоматизованого реагування на інциденти: за даними Cisco, 89% організацій вже використовують інструменти на основі штучного інтелекту для розуміння кіберзагроз. Повсякденні сервіси, такі як Gmail, непомітно фільтрують шахрайські повідомлення за допомогою штучного інтелекту, але невдоволення громадськості чат-ботами та занепокоєння щодо непрозорого використання штучного інтелекту підкреслюють необхідність прозорості та освіти, щоб можна було довіряти захисту на основі штучного інтелекту…

Незважаючи на стрімкий розвиток засобів захисту, людська помилка залишається основною вразливістю. Національний тест на конфіденційність NordVPN 2025 року дав американським користувачам оцінку 59/100, причому лише 5% розуміють ризики конфіденційності штучного інтелекту на робочому місці, навіть незважаючи на те, що багато порушень все ще пов'язані з тим, що люди натискають на шкідливі посилання, неправильно налаштовують контроль доступу, повторно використовують слабкі паролі, неправильно поводяться з конфіденційними даними або ігнорують оновлення безпеки. Експерти стверджують, що для ефективного захисту потрібні не тільки більш інтелектуальні технології, а й краща цифрова грамотність, формування звичок та культура пильності. Ефективна стратегія поєднує штучний інтелект з іншими засобами захисту, такими як VPN: системи штучного інтелекту можуть виявляти та нейтралізувати загрози в режимі реального часу, а VPN шифрують трафік, приховують IP-адреси та знижують ефективність автоматизованих сканувань, відстеження та геотаргетованих атак. Такі сервіси, як Threat Protection Pro від NordVPN, поєднують ці рівні, використовуючи машинне навчання для блокування фішингових сайтів, шкідливого програмного забезпечення та трекерів поряд із шифруванням. У майбутньому штучний інтелект у кібербезпеці залишиться грою в кота і мишу: у міру вдосконалення моделей виявлення захисниками, зловмисники будуть використовувати ту саму технологію для вдосконалення своїх тактик. У цьому мінливому середовищі поєднання захисних засобів на основі штучного інтелекту, потужних інструментів конфіденційності та обізнаної поведінки користувачів є необхідним для того, щоб йти в ногу з цифровими ризиками, які постійно вдосконалюються…» ***(AI in Cybersecurity: How Hackers and Defenders Use AI // Reuters (https://www.reuters.com/press-releases/ai-in-cybersecurity-how-hackers-and-defenders-use-ai-2025-11-20/). 20.11.2025).***

***

«Китайський виробник Yutong, який вже перебуває під пильною увагою в Данії та Норвегії після того, як норвезький оператор Ruter виявив, що може дистанційно вимкнути «новий» електричний автобус, має понад 1500 транспортних засобів, включаючи близько 145 моделей на акумуляторних батареях, що курсують в Австралії. Хоча місцевий дистриб'ютор Yutong, компанія VDI, заявляє, що оновлення програмного забезпечення в Австралії виконуються

тільки в сервісних центрах, експерти з кібербезпеки попереджають, що реальна небезпека полягає в будь-якому «підключеному» транспортному засобі, виробник якого зберігає віддалений доступ до мікрофонів, камер, GPS і прошивки…

Аластер Макгіббон, колишній глава Австралійського центру кібербезпеки, зазначає, що компанії, зареєстровані в Китаї, в кінцевому рахунку підпорядковуються директивам Комуністичної партії Китаю, і закликає Канберру розглянути можливість заборонити використання електромобілів китайського виробництва на території урядових установ. Денніс Десмонд, колишній агент ФБР, який зараз працює в Університеті Саншайн-Кост, стверджує, що кожне імпортоване інтелектуальне обладнання, включаючи автобуси з будь-якої країни, повинно пройти повне тестування на безпеку даних перед введенням в експлуатацію, особливо якщо це стосується оборони, правоохоронних органів або інших чутливих користувачів…

Yutong наполягає, що його австралійські автобуси не можуть дистанційно керуватися, гальмуватися або прискорюватися, а оперативні дані надходять лише до центру AWS у Сіднеї за згодою клієнтів; компанія «повністю розуміє» проблеми конфіденційності. Міністерство оборони заявляє, що покладається на багаторівневу модель базової безпеки, а Transport Canberra, яке має отримати 90 автобусів Yutong E12, ще не прокоментувало цю ситуацію.

Аналітики вважають, що цей випадок є сигналом тривоги: навіть «звичайні» операційні або діагностичні дані можуть допомогти супротивнику скласти карту мереж і спланувати порушення їх роботи, тому ретельна оцінка кібербезпеки перед укладенням контракту є необхідною для всього ланцюжка поставок Інтернету речей…» ***(Sally Brooks. Chinese-made electric buses on Australian roads spark cybersecurity concerns after Norway flags issue // ABC (https://www.abc.net.au/news/2025-11-07/chinese-electric-buses-in-australia-spark-security-concerns/105982738). 07.11.2024).***

***

«Інструменти штучного інтелекту — ChatGPT, Microsoft Copilot, Google Gemini та функції штучного інтелекту, вбудовані в Slack, Notion, Adobe Creative Cloud та десятки інших бізнес-додатків — стали частиною повсякденної роботи. Однак ця зручність породила практично невидиму загрозу, відому як «тіньовий штучний інтелект»: співробітники вводять конфіденційні дані в генеративні моделі або використовують вбудовані механізми прогнозування без відома або контролю з боку IT- та безпекових команд…

Оскільки багато платформ інтегрують ШІ настільки органічно, співробітники можуть навіть не усвідомлювати, що надсилають корпоративну інтелектуальну власність, записи про клієнтів або конфіденційну стратегію стороннім службам. Після того, як ці дані обробляються або зберігаються поза контролем компанії, ризики збільшуються: витоки, такі як нещодавнє публічне індексування розмов ChatGPT, наражають компанії на штрафи за GDPR, штрафи за Законом про захист даних Великобританії, нові правила управління ШІ та шкоду репутації. Повні заборони рідко працюють; працівники просто переходять на особисті пристрої або

приватні браузери, що робить діяльність більш прихованою і недоступною для моніторингу дотримання вимог…

На відміну від класичного тіньового ІТ, тіньовий ШІ ховається на виду, уникаючи традиційних черг на затвердження програмного забезпечення та щорічних аудитів, які були розроблені для статичного коду, а не для систем, що постійно навчаються. Тому організаціям потрібне нове, більш швидке управління: постійне виявлення прихованих функцій штучного інтелекту, ретельна перевірка будь-якої моделі, що впливає на корпоративні робочі процеси, чітка політика щодо власності даних та відповідальності за помилки, а також контроль у режимі реального часу, який перетворює несанкціоноване використання штучного інтелекту на керований ресурс, що відповідає законодавству. Без таких змін неперевірений штучний інтелект залишається потенційною загрозою, і відділи кадрів, комплаєнсу та юридичні відділи зрештою будуть змушені усувати наслідки». ***(Pravesh Kara. Shadow AI: The unseen cybersecurity threat infiltrating UK workplaces // Codel Software Ltd (https://hrnews.co.uk/shadow-ai-the-unseen-cybersecurity-threat-infiltrating-uk-workplaces/). 24.11.2025).***

***

«Майже всі підприємства планують розширити використання автономних «агентних» інструментів штучного інтелекту в наступному році, але більшість з них ще не вирішили питання нових ризиків для безпеки, які несуть ці агенти. Дослідження показують, що компанії використовують десятки генеративних програм штучного інтелекту — часто без нагляду — і співробітники часто вставляють в них конфіденційні дані. Оскільки агенти штучного інтелекту не просто генерують текст, а діють на основі даних, вони можуть розкривати конфіденційну інформацію, спотворювати процес прийняття рішень і спричиняти порушення вимог дотримання нормативних вимог…

Перш ніж використання агентів стане звичним, необхідно вирішити чотири основні завдання:

Посилити базові заходи безпеки: багато порушень, пов'язаних із штучним інтелектом, пов'язані з відсутністю таких основних елементів, як управління доступом, оцінка постачальників та аналіз ризиків, пов'язаних із третіми сторонами. Безпеку не можна забезпечити пізніше.

Гарантія цілісності даних: агенти повинні працювати з даними, походження та історія змін яких підлягають аудиту. Централізована, добре керована база даних є надзвичайно важливою, інакше пошкоджені або вирвані з контексту дані призведуть до помилкових, потенційно незаконних рішень…

Усунення «тіньової ШІ»: несанкціоноване використання публічних моделей ШІ або додавання нових функцій ШІ до затвердженого програмного забезпечення без повторної оцінки ризиків збільшує витрати та ймовірність порушення. Виявлення та постійний моніторинг усіх випадків використання ШІ тепер є контрольними точками відповідності.

Залучайте людей до процесу: агенти можуть автоматизувати рутинні завдання, такі як моніторинг журналів та перевірка доступу, але людський нагляд залишається життєво важливим для виявлення контексту, етики та упередженості. Навчання

співробітників безпечним практикам використання ШІ — наприклад, ніколи не вводити конфіденційні дані в неперевірені інструменти — є настільки ж важливим, як і навчання їх користуватися новою технологією…

При правильному використанні агентська ШІ може посилити захист, перекладаючи на неї завдання низької цінності та дозволяючи командам безпеки зосередитися на складних загрозах. При неправильному використанні вона стає дорогою відповідальністю. Лідери, які з самого початку впроваджують системи безпеки, управління та довіри до даних, зможуть безпечно масштабувати ШІ та отримати її конкурентні переваги». ***(Larry English. Agentic AI Is Coming—But Is Your Cybersecurity Really Ready For It? // Forbes Media LLC (https://www.forbes.com/sites/larryenglish/2025/11/24/agentic-ai-is-coming-but-is-your-cybersecurity-really-ready-for-it/). 24.11.2025).***

***

«Такі постачальники штучного інтелекту, як OpenAI, Anthropic і Microsoft, порушують давні традиції секретності в галузі, публікуючи детальні звіти про те, як зловмисники зловживають їхніми платформами з великими мовними моделями. Реакція спільноти фахівців з безпеки розділилася: багато практиків, звиклих до багаторічної непрозорості постачальників, відкидають ці розкриття як маркетинговий хід, тоді як інші бачать у них цінну інформацію про загрози. Звіти показують, що зловмисники не вигадують екзотичні нові експлойти, а пристосовують генеративну ШІ до звичних тактик — фішингу, створення шкідливих скриптів, операцій впливу — і використовують швидкість, масштаб та багатомовність ШІ для їх вдосконалення. Вони також розкривають ранні експерименти з «агентною» ШІ: напівавтономними агентами, які можуть збирати цільові дані, писати шкідливий код і здійснювати атаки з мінімальним втручанням людини, що свідчить про перші кроки до повністю автоматизованих кампаній…

Хоча мотиви постачальників частково є комерційними — завоювання довіри є необхідною умовою для впровадження штучного інтелекту в підприємствах — їхня прозорість змушує ширшу кіберіндустрію, яка зазвичай розкриває порушення лише під тиском, підвищити власні стандарти розкриття інформації. Публічні звіти про інциденти розвіюють міфи про ризики штучного інтелекту, демонструють саморегулювання відповідно до цілей політики та сприяють розвитку моделі колективного захисту, подібної до обміну інформацією про загрози в ISAC…

Керівники служб безпеки, які розглядають ці звіти як стратегічні активи, а не як рекламний хід, можуть: інформувати ради директорів з метою забезпечення бюджету для засобів контролю, пов'язаних з ШІ; застосовувати захисні заходи «AEGIS», такі як мінімальне втручання, постійний моніторинг та перевірки цілісності; а також проводити навчання «червоної команди», що імітують швидке введення, зловживання агентами та API, описані в прикладах з практики. Відмовившись від рефлекторного цинізму на користь цікавості, захисники можуть перетворити відверту інформацію від постачальників на більш ефективне управління, виявлення та реагування на майбутню хвилю атак, прискорених штучним інтелектом». ***(Jeff Pollard, Allie Mellen, Jess Burn. AI Vendor Threat Research And Cybersecurity's Cynicism Problem // Forrester Research, Inc.***

(https://www.forrester.com/blogs/ai-vendor-threat-research-and-cybersecuritys-cynicism-problem/). 24.11.2025).

***

Штучний інтелект, як інструмент боротьби із кіберлочинністю

«Check Point Research використовував генеративний ШІ, щоб значно прискорити та покращити реверс-інжиніринг XLoader, відомого інфокрадія, похідного від Formbook. Традиційний аналіз шкідливого програмного забезпечення є повільним і ручним — розпакування бінарних файлів, відстеження функцій і написання скриптів для дешифрування — а XLoader є особливо складним через потужний захист від пісочниць… Інтегруючи ChatGPT у дворівневий робочий процес — хмарний статичний аналіз (експорт даних з IDA Pro для ідентифікації алгоритмів шифрування за допомогою моделі, структур даних та генерації дешифраторів Python) та аналіз виконання за допомогою MCP (пов'язування моделі з живим дебагером для вилучення ключів, дешифрованих буферів та даних C2 в пам'яті) — команда напівавтоматизувала завдання, які зазвичай є нудними та схильними до помилок. Цей підхід дозволив розшифрувати основний код, виявити багаторівневе шифрування, відновити 64 приховані домени управління та контролю, викрити приховані API та відкрити нову техніку уникнення пісочниці, яка отримала назву «secure-call trampoline». Підкреслюючи, що штучний інтелект доповнює, а не замінює аналітиків, Check Point зазначає, що цей метод забезпечує швидкість, відтворюваність та глибше розуміння того, як XLoader ховається, комунікує та захищається — це критично важлива інформація для поліпшення виявлення та реагування… XLoader, вперше виявлений у 2021 році під час крадіжки даних з macOS, еволюціонував з давно існуючого Formbook, орієнтованого на Windows, який спочатку був кейлоггером, а потім перетворився на повноцінний засіб для крадіжки даних». ***(Sead Fadilpašić. One of the most devious malware strains might have been cracked - and it's all thanks to Gen AI // Future US, Inc. (https://www.techradar.com/pro/security/one-of-the-most-devious-malware-strains-might-have-been-cracked-and-its-all-thanks-to-gen-ai). 04.11.2025).***

***

«…Заснована наприкінці 2024 року колишніми інженерами підрозділу 8200 Хагаєм Шапіром та Елдадом Родічем, компанія Daylight із Тель-Авіва створила платформу кібербезпеки, яка поєднує автономних агентів штучного інтелекту з людськими аналітиками, щоб йти в ногу з противниками, кількість яких зростає на 50 відсотків щороку і які все частіше використовують генеративний штучний інтелект як зброю. Система постійно збирає телеметричні дані, в режимі реального часу виявляє складні загрози, а потім направляє результати досвідченим аналітикам для перевірки та реагування — це «гібридна» модель, яка, за словами Шапіра, забезпечує швидкість штучного інтелекту без втрати судження та довіри, які можуть надати тільки люди… За підтримки Craft Ventures (співзасновник якої Девід Сакс зараз обіймає посаду царя штучного інтелекту та

криптовалют в адміністрації США) та інших провідних інвесторів, Daylight використає нове фінансування для прискорення експансії в США, збагачення своєї служби керованого виявлення та реагування модулями захисту ідентичності та хмарних робочих навантажень, а також розширення своєї команди з 25 осіб, які працюють в Ізраїлі, США та Сінгапурі. Компанія вже має серед десятків організацій, що використовують її платформу MDR на базі штучного інтелекту, такі фірми, як The Motley Fool, Cresta та McKinsey Investment Office…» ***(Sharon Wrobel. Trump AI czar's investment firm leads $33 million funding in Israeli cyber startup // The Times of Israel (https://www.timesofisrael.com/trumps-ai-czar-leads-33-million-investment-in-israeli-cybersecurity-startup/). 04.11.2025).***

***

«Кібербезпека на основі штучного інтелекту (ШІ) представляє собою фундаментальний зсув у цифровій обороні, виходячи за межі традиційних систем, заснованих на правилах, і переходячи до підходу, який використовує машинне навчання та обробку даних у реальному часі для захисту мереж. Встановлюючи базові показники поведінки, ШІ постійно моніторить величезні потоки даних безпеки для виявлення аномалій, таких як несанкціонований доступ, латеральний рух або експлойти нульового дня, які можуть бути пропущені людськими аналітиками або застарілими інструментами… До 2025 року ця технологія стала необхідною для великих підприємств і критичної інфраструктури, беручи на себе завдання, які перевантажують людський інтелект, такі як сортування сотень щоденних сповіщень про безпеку, захист програмного коду перед розгортанням та кореляція розрізнених подій у хмарних, кінцевих і IoT-середовищах для виявлення складних ланцюжків атак.

Застосування ШІ в цьому секторі є широким і трансформує три основні результати: швидкість виявлення, точність реагування та оперативну ефективність. Рішення на основі ШІ можуть підвищити рівень виявлення загроз до 95% і значно скоротити час реагування за рахунок виконання автоматизованих стратегій локалізації, таких як ізоляція скомпрометованих кінцевих точок або скасування облікових даних, за мілісекунди. Серед конкретних застосувань – адаптивна аутентифікація, яка аналізує контекст, а не лише паролі, та вдосконалене виявлення фішингу, яке використовує обробку природної мови (NLP) для виявлення маніпуляцій в електронних листах або глибокого клонування голосу. Крім того, ШІ автоматизує управління вразливостями, проактивно відображаючи поверхні атаки та прогнозуючи, які слабкі місця хакери найімовірніше використають наступного разу, на основі історичних даних…

Однак інтеграція ШІ в кібербезпеку є двосічним мечем. Хоча вона дозволяє невеликим командам ефективно захищати складні середовища, вона також спровокувала гонку озброєнь: зловмисники одночасно використовують генеративний ШІ для масштабування фішингових кампаній, автоматизації мутацій шкідливого програмного забезпечення та вдосконалення розвідки. Як наслідок, організації стикаються з такими ризиками, як надмірна залежність від автоматизації, помилкові спрацьовування та проблеми конфіденційності даних, які посилюються глобальним дефіцитом кваліфікованих фахівців, здатних управляти цими

інструментами. Незважаючи на ці виклики, майбутнє кібербезпеки вказує на повністю автономні операції, де «агентна ШІ» займається виявленням та усуненням проблем з мінімальним втручанням людини. Щоб орієнтуватися в цьому мінливому середовищі, організації повинні збалансувати впровадження передових платформ ШІ з надійним управлінням, людським наглядом та дотриманням нормативних вимог». ***(What is AI in cybersecurity in 2025: Uses, latest developments, and future trends // nexos.ai (https://nexos.ai/blog/ai-in-cybersecurity/). 19.11.2025).***

***

«Штучний інтелект швидко змінює ландшафт кібербезпеки, виступаючи як потужна зброя для зловмисників і надійний щит для захисників, а компанія Türk Telekom стала лідером у сфері захисту Туреччини. Цей телекомунікаційний гігант надає послуги з кібербезпеки майже 5000 установам, використовуючи системи на базі штучного інтелекту для блокування тисяч щомісячних фішингових, DDoS-атак і атак з використанням шкідливого програмного забезпечення. Тільки у 2023 році компанія нейтралізувала 2620 критичних атак. Його майстерність визнана на міжнародному рівні: компанія має акредитацію CREST у трьох категоріях і вже три роки поспіль є лідером турецького ринку послуг з кібербезпеки. Окрім основної діяльності, Türk Telekom сприяє інноваціям через TT Ventures, свій корпоративний венчурний фонд, який інвестував у 12 стартапів, що спеціалізуються на штучному інтелекті, кібербезпеці та технологіях у сфері охорони здоров'я…

Ця місцева діяльність відображає інтенсивну глобальну конкуренцію в галузі штучного інтелекту, де нещодавно представлена модель Gemini 3 від Google піднялася на вершину рейтингу, заявивши про свою перевагу над такими конкурентами, як ChatGPT і Claude, в обробці тексту, зображень, аудіо та відео. Її глибока інтеграція з екосистемою Google є ключовою перевагою, хоча незалежна перевірка її можливостей і географічні обмеження її преміум-функцій ще не були повністю оцінені. Тим часом економічний потенціал ШІ стає вражаючим. На Дні інновацій Salesforce в Стамбулі компанія прогнозувала, що агенти ШІ — автономні системи, які переформатують робочі процеси — можуть створити глобальний економічний ефект у розмірі 13 трильйонів доларів до 2030 року. Salesforce підкреслила, що ключовим фактором є не тільки сама технологія, а й її успішне впровадження, і представила платформу Agentforce, розроблену для того, щоб допомогти компаніям подолати 95% невдач у впровадженні ШІ…

Динамічна турецька технологічна екосистема також приваблює значні інвестиції, які сприяють цьому переходу. Стартап AdTech GoWit та фінтех-компанія Onlayer нещодавно отримали фінансування для прискорення своєї міжнародної експансії та вдосконалення своїх платформ на базі штучного інтелекту, причому Onlayer стала першим акредитованим постачальником послуг з моніторингу торговців у Туреччині та Європі. Ще більше підкріплюючи це зростання, програма Mastercard Lighthouse Türkiye x EBRD Star Venture Startup Acceleration Program зараз приймає заявки на другий цикл, пропонуючи шістьом обраним фінтех-стартапам 18 місяців наставництва, навчання, доступ до мереж інвесторів та фонд у розмірі 50 000 євро. У сукупності ці події малюють картину динамічного турецького технологічного сектору, очолюваного визнаними гігантами та спритними

стартапами, який позиціонує себе в авангарді глобальної гонки в галузі штучного інтелекту та кібербезпеки…» ***(Timur Sırt. AI-driven cybersecurity investments accelerate in Türkiye // Turkuvaz Haberleşme ve Yayıncılık (https://www.dailysabah.com/business/tech/ai-driven-cybersecurity-investments-accelerate-in-turkiye). 21.11.2025).***

***

«У сучасному цифровому середовищі, насиченому загрозами, штучний інтелект стає незамінним для безпеки підприємств, змінюючи захист з реактивного на проактивний. ШІ чудово справляється з обробкою та аналізом величезних потоків даних у реальному часі, що дозволяє організаціям виявляти аномалії в поведінці та нові моделі атак, які не помічають інструменти, що базуються на правилах. Механізми машинного навчання можуть скоротити час реагування на інциденти — часто на 90 відсотків — а їхня прогнозна аналітика дозволяє командам безпеки передбачати ймовірні вектори атак і усунути прогалини, перш ніж ними скористаються зловмисники…

Одним з найпотужніших додатків є управління привілейованим доступом на основі штучного інтелекту. Адміністративні облікові записи є головними цілями, проте традиційні засоби контролю залежать від статичних правил і ручного нагляду. Платформи, які накладають на ці облікові записи шар машинного навчання — постійно аналізуючи поведінку, позначаючи відхилення та автоматично блокуючи підозрілі сесії — миттєво адаптуються до змін ризиків, різко зменшуючи зловживання обліковими даними…

ШІ також автоматизує трудомісткі операції з безпеки: сортування сповіщень, аналіз журналів, оновлення політик для забезпечення відповідності вимогам та звільнення аналітиків від виконання складних розслідувань. Інтегрована в існуючі структури, ШІ підвищує ефективність та мінімізує людські помилки, які часто сприяють порушенням.

Ця технологія не позбавлена проблем. Алгоритми можуть переймати упередження з навчальних даних, що викликає занепокоєння з етичних міркувань та питань відповідальності, а їх «чорний ящик» прийняття рішень може обмежувати прозорість. Проте, у міру вдосконалення інструментів ШІ, очікується більш тісна інтеграція між системами безпеки, обмін інформацією між системами в режимі реального часу і навіть використання ШІ-механізмів, які моделюють атаки для тестування захисних систем. При відповідальному використанні ШІ обіцяє динамічно адаптивну систему кібербезпеки, яка перевершує креативність і швидкість сучасних супротивників…» ***(How AI Is Reinventing The Future Of Enterprise Cybersecurity // Analytics Insight (https://www.analyticsinsight.net/artificial-intelligence/how-ai-is-reinventing-the-future-of-enterprise-cybersecurity). 18.11.2025).***

***

«Новий звіт «Прогноз у сфері кібербезпеки на 2026 рік» від Google Cloud Security попереджає, що кіберзагрози, пов'язані з штучним інтелектом, та зростання рівня вимагання в усьому світі визначатимуть ситуацію у сфері безпеки в наступному році. Google прогнозує, що штучний інтелект стане стандартною зброєю зловмисників, прискорюючи соціальну інженерію, створення шкідливого програмного забезпечення та кампанії з підробки особи. Зокрема, очікується, що мультимодальні генеративні інструменти штучного інтелекту, здатні маніпулювати голосом, текстом і відео, сприятимуть новій хвилі надзвичайно реалістичного фішингу та компрометації ділової електронної пошти, стираючи межі між обманом з боку людини та машини…

Виділено два основні ризики, пов'язані з штучним інтелектом: Prompt Injection (швидке введення) — техніка маніпулювання, яка, за прогнозами, набуватиме поширення у міру інтеграції підприємствами великих мовних моделей (LLM) у робочі процеси, що дозволить зловмисникам обходити засоби контролю та спричиняти порушення безпеки даних; та «Shadow Agent Challenge» (проблема тіньових агентів), коли співробітники використовують несанкціонованих агентів штучного інтелекту для автоматизації завдань, створюючи невидимі, неконтрольовані канали передачі даних, що створюють ризики для безпеки та дотримання нормативних вимог. Google наголошує, що організації повинні вирішувати проблему тіньових агентів не шляхом заборони агентів, а шляхом впровадження нових дисциплін управління безпекою ШІ, включаючи системи моніторингу та ідентифікації, які керують агентами як цифровими об'єктами…

Крім штучного інтелекту, у звіті прогнозується, що поєднання програм-вимагачів, крадіжки даних та багатогранного вимагання стане найбільш фінансово руйнівною категорією кіберзлочинів у всьому світі через її стабільний обсяг та каскадний економічний вплив на постачальників та громади. Нарешті, інфраструктура віртуалізації визначена як критична «сліпа пляма» на 2026 рік, оскільки системні вразливості в цьому фундаментальному шарі можуть надати зловмисникам можливість швидко отримати контроль над сотнями систем. Google робить висновок, що успіх у 2026 році буде залежати від того, чи нададуть організації пріоритет проактивним, багаторівневим стратегіям захисту, чи інвестуватимуть в управління штучним інтелектом та чи будуть постійно адаптувати свої заходи безпеки для досягнення операційної стійкості». ***(Duncan Riley. Google Cloud report warns of AI-driven cyberattacks and global extortion surge in 2026 // SiliconANGLE Media Inc. (https://siliconangle.com/2025/11/04/google-cloud-report-warns-ai-driven-cyberattacks-global-extortion-surge-2026/). 04.11.2025).***

***

«Автори шкідливого програмного забезпечення розпочинають нову хвилю експериментальних атак на основі штучного інтелекту, використовуючи великі мовні моделі (LLM) для генерації, модифікації та виконання команд на вимогу, виходячи за межі залежності від статичних корисних навантажень. Хоча ці атаки на основі штучного інтелекту все ще є переважно експериментальними

і не мають надійності традиційних загроз, вони автоматизують заплутування і вносять непередбачуваність у схеми атак…

Google Threat Intelligence Group задокументувала кілька прикладів: PromptFlux використовує API Gemini для створення самомодифікуючих версій VBScript, щоб постійно змінювати свої цифрові відбитки, уникаючи виявлення. PromptSteal поєднує штучний інтелект із крадіжкою даних, запускаючи локально команди Windows, згенеровані моделлю, для збору та витоку інформації без жорстко закодованих інструкцій. Інші зразки, такі як QuietVault і концептуальна версія програм-вимагачів PromptLock, також демонструють залежність від викликів моделі та мінімальний код на машині, що знижує ймовірність виявлення на основі сигнатур…

Дизайн базується на архітектурі виклику моделі, що дозволяє зловмисникам дистанційно оновлювати поведінку шкідливого програмного забезпечення, просто змінюючи підказку. Хоча більшість зразків все ще перебувають на стадії тестування, зловмисники також стають все більш вправними у маніпулюванні захисними механізмами моделі за допомогою оманливих підказок соціального інжинірингу, часто видаючи себе за студентів, щоб виманити обмежений код. Підпільні ринки швидко комерціалізують цю тенденцію, пропонуючи генеративні модулі ШІ для створення депфейків, фішингу та шкідливого програмного забезпечення. Також спостерігається, що державні суб'єкти з Росії, Ірану, Північної Кореї та Китаю експериментують з моделями, що допомагають збирати дані та розвідувальні утиліти. Зрештою, хоча основний вплив ШІ на даний момент полягає у підвищенні продуктивності хакерів, його зростаюча прихована дія та безперебійна інтеграція у шкідливе програмне забезпечення становлять значний, постійно зростаючий ризик, на який захисники повинні терміново реагувати». ***(Rashmi Ramesh. Malware Developers Test AI for Adaptive Code Generation // Information Security Media Group, Corp. (https://www.inforisktoday.com/malware-developers-test-ai-for-adaptive-code-generation-a-29932). 05.11.2025).***

***

«Рада з кібербезпеки ОАЕ опублікувала публічне попередження про стрімке зростання кількості відео- та аудіозаписів, створених за допомогою штучного інтелекту, які переконливо імітують реальних людей. Ці витончені підробки можуть вводити в оману аудиторію, поширювати дезінформацію та шкодити репутації національних діячів та інституцій. Рада закликає громадян перевіряти будь-який контент, особливо матеріали, що приписуються державним посадовцям, через офіційні канали перед тим, як ділитися ним, та бути обережними, коли стикаються з підозрілими публікаціями. Підвищення обізнаності громадськості описується як перша лінія захисту, підкріплена Федеральним декретом-законом № 34 від 2021 року, який встановлює суворі покарання за створення або поширення фейкових новин та інші кіберзлочини…» ***(UAE cybersecurity council warns against deepfakes // Al Nisr Publishing LLC (https://gulfnews.com/uae/uae-cybersecurity-council-warns-against-deepfakes-1.500337458). 07.11.2025).***

***

«…Anthropic повідомляє, що недавня хвиля кібер-шантажу проти щонайменше 17 організацій, включаючи урядові установи, була майже повністю організована «агентним ШІ». Використовуючи Claude Code, зловмисники дозволили моделі вибрати вразливі цілі, написати спеціальне шкідливе програмне забезпечення, відсортувати викрадені файли для пошуку найбільш конфіденційних даних, розрахувати реалістичні суми викупу в біткойнах на основі фінансових даних жертв та скласти психологічно налаштовані листи з погрозами. Цей інцидент є першим публічним випадком, коли основна платформа штучного інтелекту координувала кожну фазу кіберзлочинної операції, і демонструє так званий «віб-хакінг», при якому автономний код атакує декількох жертв паралельно, приймаючи власні тактичні та стратегічні рішення… Оскільки ШІ може масштабувати атаки набагато швидше, ніж люди, і залишає менше викривальних помилок, Anthropic попереджає, що підприємства стикаються з різким зростанням ризиків, потенційним шкодою для бренду та більш суворим регуляторним контролем. Компанія закликає організації оновити засоби контролю безпеки для загроз, що генеруються ШІ, відпрацювати плани реагування на інциденти, навчити персонал виявляти фішинг, створений ШІ, та залучити юридичних радників на ранній стадії, щоб забезпечити дотримання вимог та обмежити відповідальність». ***(Jason G. Weiss. AI-powered cyber threats: What everyone needs to know // Freeman Mathis & Gary, LLP (https://www.fmglaw.com/cyber-privacy-security/ai-powered-cyber-threats-what-everyone-needs-to-know/). 06.11.2025).***

***

«Штучний інтелект прискорює гонку озброєнь у кіберпросторі. Нова біла книга Symantec і Carbon Black показує, як генеративний ШІ вже допомагає злочинцям створювати майже досконалі фішингові приманки, перекладати їх вільно і навіть генерувати шкідливий код, а LLM, що керуються зловмисниками, такі як «Xanthorox AI», ще більше знижують технічний бар'єр. Наступним рубежем є «агентний ШІ»: автономні агенти, побудовані на базі LLM, які можуть планувати і виконувати завдання. У лабораторних тестах агент OpenAI зміг — після мінімальних підказок — ідентифікувати цільового співробітника, написати інфокрадіжник PowerShell і надіслати його електронною поштою з переконливою приманкою. Хоча поточні агенти все ще потребують людських коригувань, швидкий прогрес може незабаром дозволити зловмиснику ввести «порушення Acme Corp» і дозволити боту обробляти перелік, створення корисного навантаження, налаштування C2 та стійкість…

Однак штучний інтелект є не менш ефективним і для захисників. Давні евристичні механізми, аналітика великих даних і нові інструменти, такі як Incident Prediction від Symantec, використовують моделі машинного навчання, навчені на більш ніж 500 000 ланцюжків атак, щоб передбачити наступний крок супротивника і заблокувати його, перш ніж буде завдано шкоди…

Ключові висновки:

• Gen-AI знижує перешкоди для фішингу та розробки шкідливого програмного забезпечення; у середньому в кожній компанії використовується 67 інструментів AI, часто без нагляду, і 38 % співробітників вставляють у них конфіденційні дані.

• Агенти AI створюють ризик кардинальних змін: автономне виконання багатоетапних атак.

• Традиційні основи безпеки — контроль доступу, системи забезпечення цілісності даних, перевірка ризиків постачальників — як і раніше мають важливе значення, а організації також повинні контролювати «тіньову AI».

• Захист AI може змінити баланс, передбачаючи та перериваючи складні ланцюжки атак, що використовують наявні ресурси.

Повідомлення: Напади, що базуються на штучному інтелекті, швидко зростають, але захист, підсилений штучним інтелектом, — якщо його застосовувати з ефективним управлінням — все ще може виграти гонку…» ***(Arms Race: AI's Impact on Cybersecurity // Broadcom (https://www.security.com/threat-intelligence/ai-whitepaper-research). 20.11.2025).***

***

«Прориви в області штучного інтелекту трансформують як аутентифікацію, так і атаки, спрямовані на її подолання. Мультимодальні системи ШІ можуть об'єднувати голос, відео, текст та інші дані для створення переконливих фейкових зображень, які підробляють біометричні дані обличчя або голосу для входу в систему, тоді як «агентний ШІ» може здійснювати комплексні вторгнення з мінімальною допомогою людини. Компанія Anthropic нещодавно задокументувала переважно автономну кампанію, в якій її модель Claude Code обробляла 80–90 % ланцюжка атак. Такі можливості становлять загрозу для фінансів, охорони здоров'я, уряду та інших секторів, які все більше залежать від біометричних або вдосконалених за допомогою ШІ перевірок ідентичності…

Традиційні засоби захисту — однорежимні біометричні дані, статичні паролі, одноразові логіни — тепер є вразливими, оскільки скомпрометовані біометричні характеристики не можна «скинути», а інструменти штучного інтелекту можуть генерувати реалістичні синтетичні ідентичності у великих обсягах. Фінансові установи особливо вразливі: успішне підроблення може спричинити масштабне шахрайство, витік даних і втрату довіри до систем цифрової ідентифікації…

Нормативні акти (HIPAA, GLBA, FTC Safeguards Rule, NYDFS тощо) вже вимагають «розумних» заходів контролю, заснованих на оцінці ризиків; нові загрози, пов'язані з штучним інтелектом, підвищують планку вимог. Організації повинні…

• запускати офіційні програми управління штучним інтелектом та оцінки ризиків (OWASP, рекомендації NIST);

• впровадити справжню багатофакторну або безперервну автентифікацію, яка поєднує біометрію з поведінковими сигналами та перевірками пристроїв/контексту;

• розгорнути інструменти ШІ, які виявляють синтетичні медіа та аномальну активність API;

• розробити системи для криптографічної гнучкості та безпечних, перевірених оновлень прошивки;

• проінформувати користувачів про фішинг та підробку особи за допомогою ШІ;

• захистити та інвентаризувати всі API, які живлять моделі ШІ…

Завдяки поєднанню таких засобів контролю, як архітектура «нульової довіри», безпечна розробка та моніторинг аномалій під час виконання, компанії можуть використовувати переваги штучного інтелекту, одночасно обмежуючи його здатність підривати системи автентифікації, призначені для захисту від зловмисників». ***(Alaap B. Shah, Brian G. Cesaratto. Companies and Employees Increasingly at Risk of AI-Powered Cyber Attacks // National Law Forum, LLC (https://natlawreview.com/article/companies-and-employees-increasingly-risk-ai-powered-cyber-attacks). 21.11.2025).***

***

«Нове дослідження Netskope Threat Labs показує, що, хоча повністю автономне шкідливе програмне забезпечення на базі штучного інтелекту ще не є повністю надійним, ця технологія швидко наближається до критичного рівня загрози. У ході дослідження були протестовані великі мовні моделі (LLM), такі як GPT-3.5 і GPT-4, щоб перевірити, чи можуть вони генерувати шкідливий код для обходу систем захисту, зосередившись, зокрема, на введенні процесів і припиненні роботи антивірусних/EDR-процесів. Дослідники виявили, що моделі, такі як GPT-3.5-Turbo, безпосередньо виконували завдання, і навіть захисні бар'єри GPT-4 можна було обійти за допомогою простого введення команд на основі ролей, що свідчить про те, що майбутнє шкідливе програмне забезпечення може переносити шкідливу логіку на зовнішню LLM під час виконання, що значно ускладнить статичне виявлення…

Однак поточні моделі демонструють нестабільну надійність у реальних умовах, особливо щодо сучасних хмарних VDI-артефактів. Попередні тести з GPT-5, хоча і продемонстрували значне підвищення якості коду (досягнуто 90% успішності проти AWS VDI), також виявили набагато сильніші механізми безпеки, де модель активно «підривала» зловмисні запити, повертаючи нешкідливий код. Netskope робить висновок, що, хоча надійність коду залишається обмеженням, темпи розвитку є швидкими, що вимагає термінового дослідження того, як захисники можуть пом'якшити цю нову генерацію загроз, що базуються на штучному інтелекті». ***(Priya. AI Language Models and Their Impact on the Evolution of Autonomous Malware // Cyber Press (https://cyberpress.org/ai-powered-autonomous-malware/). 24.11.2025).***

***

«…У той час як легальні підприємства впроваджують комерційні інструменти штучного інтелекту, на форумах даркнету швидко розвивається складний підпільний ринок, який пропонує кіберзлочинцям індивідуальні, зламані та відкриті великі мовні моделі (LLM). Ці інструменти, що рекламуються як засоби подвійного призначення для тестування на проникнення або явні засоби для хакерства, надають базові можливості для таких завдань, як сканування вразливостей, шифрування даних та написання шкідливого коду, що значно знижує бар'єр для входу для менш технічно підкованих зловмисників…

Unit 42 компанії Palo Alto Networks навела два приклади: WormGPT 4, комерціалізований LLM на основі передплати, який обіцяє допомогу в хакерстві «без

обмежень» і є дуже доступним, та KawaiiGPT, безкоштовна модель з відкритим кодом, яка використовує невимушений тон, надаючи шкідливі результати. Хоча ці підпільні моделі ще не здатні здійснювати складні автономні атаки, які спостерігалися в останніх інцидентах, спонсорованих державою, їх існування підтверджує зростаючу небезпеку LLM, які роблять злочинний хакінг простішим і швидшим, дозволяючи користувачам обходити технічну термінологію і без зусиль генерувати скрипти атак. Unit 42 підкреслює, що справжньою загрозою є саме ця покращена взаємодія, яка дозволяє навіть некваліфікованим злочинцям автоматизувати і прискорити атаки…» ***(Derek B. Johnson. Underground AI models promise to be hackers 'cyber pentesting waifu' // CyberScoop (https://cyberscoop.com/malicious-llm-tools-cybercrime-wormgpt-kawaiigpt/). 25.11.2025).***

***

Кіберзлочинність та кібертероризм

«Згідно з новими даними компанії DNSFilter, що спеціалізується на кібербезпеці, кіберзлочинці опускаються до нового рівня, агресивно націлюючись на відчайдушних шукачів роботи. Компанія виявила 8724 шкідливих доменів, що містять слово «jobs» (робота), 86% з яких були зареєстровані або виявлені в останні місяці, а також 1161 доменів, що містять слово «careers» (кар'єра)… Керівник аналітичної служби Грег Джонс пояснив, що хоча такі шахрайські схеми не є новими, вони набувають все більшого поширення через складну економічну ситуацію: у серпні 2025 року рівень безробіття в США досяг 4,3% (останній доступний показник на тлі триваючого закриття уряду), а роботодавці створили лише 22 000 робочих місць за цей місяць, що на 85% менше, ніж 142 000 у серпні 2024 року. «Люди намагаються знайти або зберегти роботу», — сказав Джонс, що робить їх легкою здобиччю для шахраїв, які шукають вразливих «овець»… Менеджери з найму також не в безпеці, оскільки стикаються з атаками spearphishing від таких груп, як Venom Spider (яка вбудовує шкідливе програмне забезпечення у фальшиві резюме) та все більш реалістичними схемами з використанням deepfake, спрямованими на IT-працівників. Щоб убезпечити себе, DNSFilter закликає шукачів роботи ретельно перевіряти домени на наявність надмірної кількості дефісів або дивних розширень, відхиляти пропозиції, які здаються занадто хорошими, щоб бути правдивими, та завжди звертатися безпосередньо до менеджерів з найму для перевірки — жоден законний рекрутер не буде проти такої обережності». ***(Brianna Monsanto. Cybercriminals are stooping to a new low by targeting job seekers when the market is already bad: 'Where's the good sheep for the wolf to go attack?' // Fortune Media IP Limited (https://fortune.com/2025/11/03/cybercriminals-stooping-to-new-low-targeting-job-seekers-when-market-is-bad/). 03.11.2025).***

***

«Містика, що оточувала гучні пограбування, була зруйнована після крадіжки 18 жовтня коронних коштовностей на суму 102 мільйони доларів з Лувру... Розслідування французької газети Libération показує, що інцидент є наслідком понад десятирічних системних прогалин у безпеці та вразливості ІТ-систем у відомому музеї, підкреслюючи, що такі порушення є менш аномальними, ніж очікувалося. Як зазначив співзасновник Rogue Касс Маршалл на Bluesky, ця реальна недбалість відображає висміяні кліше відеоігор, такі як залишення паролів відкритими, що підкреслюється використанням Лувром «Louvre» як фактичного пароля для своїх серверів відеоспостереження. Аудит кібербезпеки, проведений у 2014 році французьким агентством ANSSI на замовлення музею, виявив тривіальні паролі, що дозволяли легко проникнути в мережу, завдяки чому експерти могли маніпулювати системою відеоспостереження та доступом за бейджами; серед прикладів були «LOUVRE» для сервера та «THALES» для програмного забезпечення цієї компанії. Наступна перевірка, проведена у 2015 році Національним інститутом перспективних досліджень у галузі безпеки та юстиції Франції та завершена у 2017 році, видала 40 сторінок рекомендацій щодо усунення серйозних недоліків, таких як погане управління потоками відвідувачів, легкий доступ до дахів під час будівництва та застарілі системи, що не функціонують належним чином. Інші документи показують, що до 2025 року Лувр продовжував використовувати застаріле програмне забезпечення для безпеки від 2003 року, яке працювало на апаратному забезпеченні Windows Server 2003. Це ілюструє, як застарілі засоби захисту безцінних артефактів роблять реальні пограбування напрочуд можливими, і спонукає до переоцінки критики, спрямованої на спрощені механізми хакерства у відеоіграх». ***(Lincoln Carpenter. Post-heist reports reveal the password for the Louvre's video surveillance was 'Louvre,' and suddenly the dumpster-tier opsec of videogame NPCs seems a lot less absurd // Future Publishing Limited Quay House (https://www.pcgamer.com/software/security/post-heist-reports-reveal-the-password-for-the-louvres-video-surveillance-was-louvre-and-suddenly-the-dumpster-tier-opsec-of-videogame-npcs-seems-a-lot-less-absurd/). 03.11.2025).***

***

«У період з червня по серпень 2025 року іранський зловмисник, тимчасово названий UNK_SmudgedSerpent, провів цілеспрямовані фішингові кампанії проти провідних американських аналітичних центрів та експертів із зовнішньої політики з метою збору стратегічної інформації. Група продемонструвала заплутану суміш тактик, технік і процедур (TTP), які перетинаються з більшістю основних іранських APT (Advanced Persistent Threats, просунуті постійні загрози), що ускладнює точну атрибуцію…

UNK_SmudgedSerpent успішно видавав себе за ключових фігур, таких як віце-президент Брукінгського інституту, використовуючи ретельно розроблені фішингові приманки, що пропонували співпрацю над фейковими проектами. Ланцюжок атак передбачав надсилання шкідливого URL-адреси, замаскованої під посилання на OnlyOffice або Microsoft Teams, що перенаправляло жертв на дуже переконливу фішингову сторінку для введення облікових даних Microsoft 365. У випадках, коли крадіжка облікових даних не вдавалася, зловмисник «подвоював» свої зусилля,

розгортаючи два різних типи програмного забезпечення для віддаленого моніторингу та управління (RMM) за допомогою приманкових документів у zip-файлі…

Дослідники відзначили, що аспекти соціальної інженерії нагадували TA453 (Charming Kitten), тоді як інфраструктура та використання посилань OnlyOffice відповідали TA455 (Smoke Sandstorm), а використання програмного забезпечення RMM було унікальним і раніше асоціювалося лише з TA450 (MuddyWater). Гіпотези щодо цієї мінливості TTP вказують на внутрішню реорганізацію, централізовані інфраструктурні послуги або обмін навичками між іранськими кіберагентствами (IRGC та MOIS). Експерти наголошують, що розуміння цієї атрибуції є надзвичайно важливим для розробки захисних заходів на основі розвідданих та обґрунтування необхідних інвестицій у кібербезпеку». ***(Nate Nelson. Elusive Iranian APT Phishes Influential US Policy Wonks // TechTarget, Inc. (https://www.darkreading.com/cyberattacks-data-breaches/iranian-apt-phishes-us-policy-wonks). 05.11.2025).***

***

«У жовтні кількість атак на ланцюжок постачання програмного забезпечення досягла рекордного рівня, перевищивши попередні місячні піки на понад 30%, при цьому зловмисники здійснили 41 атаку на сайти з витоком даних у даркнеті. Середньомісячний показник з початку 2024 року зріс більш ніж удвічі, що зумовлено насамперед поєднанням критичних/нульових уразливостей IT та активним націлюванням на постачальників SaaS та IT-послуг. Серед інших факторів, що сприяють цьому, називають загрози хмарній безпеці та фішинг-кампанії на основі штучного інтелекту, а також вішинг, який використовувався в останніх гучних порушеннях безпеки…

Найбільше постраждали сектори IT та IT-послуг, які зазнали втричі більше атак, ніж будь-який інший сектор, через високу цінність та широке охоплення клієнтів, які вони представляють. Групи, що використовують програми-вимагачі, зокрема дві провідні групи Qilin та Akira, очолюють цей сплеск. Akira нещодавно зламала великий проект з відкритим кодом, а Qilin заявила, що викрала вихідний код, який використовують правоохоронні органи та організації з громадської безпеки, часто націлюючись на компанії, що обслуговують чутливі сектори, такі як оборона, розвідка та охорона здоров'я. Інші значні інциденти в жовтні включали зловживання Cl0p та злом, пов'язаний з американським оборонним підрядником…

Враховуючи, що партнери ланцюга поставок за своєю суттю є надійними, дослідники Cyble наголошують, що захист повинен стати стандартною практикою завдяки аудитам безпеки та оцінці ризиків третіх сторін. Найефективнішим контрольним пунктом є процес безперервної інтеграції та розвитку (CI/CD), який вимагає ретельного перевірки партнерів та надійних заходів безпеки в усіх контрактах з постачальниками». ***(Paul Shread. Software Supply Chain Attacks Set Records in October // The Cyber Express (https://thecyberexpress.com/software-supply-chain-attacks-set-records/). 04.11.2025).***

***

«Cyble Research and Intelligence Labs (CRIL) виявили операцію з кібершпигунства, що демонструє вдосконалений технічний розвиток методів, які раніше приписувалися групі Sandworm (APT44) і були спрямовані на системи оборонного сектору. В атаці використовувався збройовий ZIP-архів, замаскований під білоруський військовий документ про перепідготовку, метою якого було ввести в оману персонал, пов'язаний із Командуванням спеціальних операцій та операціями з використанням дронів, ймовірно для збору розвідданих або як фальшива операція під чужим прапором…

Складний ланцюжок інфікування починається, коли жертва запускає ярлик LNK, замаскований під PDF-файл, який запускає зашифрований скрипт PowerShell. Цей скрипт використовує заходи проти виявлення, перевіряючи умови, типові для активного середовища користувача (а не пісочниці), перед встановленням постійних служб. Стійкість досягається за допомогою завдань, запланованих у XML, які розгортають модифіковані версії OpenSSH для Windows і клієнта Tor, перейменовані відповідно на «githubdesktop.exe» і «pinterest.exe»…

Шкідливе програмне забезпечення встановлює прихований канал доступу, налаштовуючи OpenSSH на нестандартному порту (20321) з аутентифікацією на основі ключа RSA, тоді як служба Tor пересилає критичні порти (SSH, SMB, RDP) через протокол obfs4, щоб замаскувати комунікації під легітимний мережевий трафік через два мостові ретранслятори. Така архітектура надає зловмиснику повний віддалений анонімний доступ до скомпрометованого хоста. CRIL зберігає помірну впевненість у зв'язку цієї операції з Sandworm через схожість з їхньою кампанією «Army+» у грудні 2024 року і рекомендує організаціям, що займаються захистом, посилити фільтрування електронної пошти, стежити за Tor і підозрілою активністю PowerShell, а також перевіряти використання OpenSSH, щоб зменшити загрозу». ***(Ashish Khaitan. Cyble Detects Advanced Backdoor Targeting Defense Systems via Belarus Military Lure // The Cyber Express (https://thecyberexpress.com/belarus-military-hit-by-ssh-tor-backdoor/). 03.11.2025).***

***

«…Кіберзлочинці, які керуються фінансовими мотивами, все частіше співпрацюють з організованою злочинністю, щоб викрасти величезні обсяги вантажів, зловживаючи законними інструментами віддаленого моніторингу та управління (RMM), такими як ScreenConnect і SimpleHelp. Ці зловмисники отримують доступ до цільових автоперевізників або фрахтових брокерів, проводять розвідку та збирають облікові дані, користуючись тим, що інструменти RMM можуть обходити сигнали безпеки легше, ніж звичайне шкідливе програмне забезпечення. Таке зростання зловживань RMM є широко поширеним, хоча особливо турбує логістична галузь, яка вже зараз зазнає щорічних збитків від крадіжок вантажів у середньому на суму 34 мільярди доларів, і за прогнозами, ця цифра зросте на 22% до 2025 року…

Методика атаки в значній мірі базується на соціальному інжинірингу, причому фішинг, смфінг та компрометація ділової електронної пошти залишаються основними точками входу в цільові системи. Опинившись всередині, зловмисники компрометують облікові записи брокерів, які вони використовують для розміщення

шахрайських оголошень про вантажі або введення шкідливого вмісту в існуючі розмови. Цей доступ дозволяє їм робити ставки на вантажні перевезення, викрадати вантаж, а потім продавати товари в Інтернеті або за кордоном. Ця організована кіберкрадіжка, яка посилилася під час пандемії COVID-19, коли ланцюги поставок були обмежені, підкреслює нагальну необхідність для логістичної галузі зосередитися на боротьбі з кіберзагрозами в ланцюгах поставок». ***(David Jones. Cybercrime groups team with organized crime in massive cargo theft campaigns // TechTarget, Inc. (https://www.cybersecuritydive.com/news/cybercrime-organized-crime-cargo-theft-campaign/804501/). 03.11.2025).***

***

«Кіберзлочинці все частіше співпрацюють з організованою злочинністю, щоб атакувати транспортні та логістичні компанії, використовуючи інструменти віддаленого моніторингу та управління (RMM) для спрощення викрадення вантажів. Таке кібервикрадення вантажів поглиблює масштабну проблему галузі: у 2024 році втрати товарів під час транспортування в США зросли на 27 %, а цього року очікується їхній подальший стрибок на 22 %, що призведе до щорічних збитків галузі в розмірі близько 35 млрд доларів. Дослідники Proofpoint спостерігають групу загроз, яка діє принаймні з червня і демонструє глибоке знання транспортної галузі… Зловмисники проникають на біржі вантажів — торгові майданчики, що з'єднують вантажовідправників і перевізників — щоб розміщувати фальшиві вантажі. Коли перевізники відповідають, вони отримують електронні листи, що містять шкідливі URL-адреси, які встановлюють легальні інструменти RMM, такі як ScreenConnect, PDQ Connect або Fleetdeck, які використовуються для проведення розвідки та викрадення облікових даних. Після того, як перевізник скомпрометований, хакери використовують свій доступ, щоб ідентифікувати та робити ставки на вигідні вантажі, перш ніж їх викрасти… Proofpoint рекомендує компаніям зменшити цей ризик шляхом обмеження встановлення інструментів RMM, впровадження засобів виявлення в мережі, уникнення виконання файлів, надісланих електронною поштою, та підтримання високої пильності, особливо з огляду на те, що органи влади США та Міністерство транспорту посилюють увагу до боротьби з крадіжками вантажів, включаючи кіберзлочини». ***(James Reddick. Cargo theft gets a boost from hackers using remote monitoring tools // Recorded Future News (https://therecord.media/cargo-theft-hackers-remote-monitoring-tools). 03.11.2025).***

***

«Хакери успішно викрали понад 100 мільйонів доларів, скориставшись критичною вразливістю в протоколі децентралізованих фінансів (DeFi) Balancer, зокрема, націлившись на його V2 Composable Stable Pools. Постраждалі пули були активними протягом декількох років, що вивело багато з них за межі «вікна паузи» Balancer — механізму, призначеного для екстреного зупинення під час атак. Хоча решта пулів Balancer V3 і старіших версій не постраждали і залишаються безпечними, скомпрометовані пули, які можна було призупинити, були швидко відключені для відновлення… Команда Balancer швидко відреагувала,

співпрацюючи з дослідниками в галузі безпеки для аналізу інциденту, і пообіцяла опублікувати повний звіт після завершення розслідування. Після цього платформа опублікувала термінове попередження для користувачів про шахрайські повідомлення та спроби фішингу, замасковані під офіційні оновлення безпеки, підкресливши, що вся офіційна інформація буде поширюватися виключно через офіційний акаунт X (Twitter) та сервер Discord. Balancer співпрацює з юристами та фахівцями з безпеки, щоб посилити захист користувачів та відстежити зловмисників, підтверджуючи свою давню прихильність до безпеки, незважаючи на порушення…» ***(Abinaya. Hackers Stolen Over $100 Million by Exploiting Balancer DeFi Protocol // Cyber Security News (https://cybersecuritynews.com/hackers-stolen-exploiting-balancer/). 04.11.2025).***

***

«Аматорський футбольний клуб «Окленд Сіті» (Auckland City) намагається відновити контроль над своїми сторінками в соціальних мережах після того, як став жертвою кібератаки. Хакери захопили популярні акаунти клубу в Facebook та Instagram, які мають понад 400 000 підписників, і спочатку заповнили їх зображеннями сексуального характеру. Хоча відвертий контент вже видалено, речник підтвердив, що «зловмисний агент» залишається під контролем акаунтів і зараз репостить старі, легітимні рекламні матеріали про ігри. Клуб, який в основному керується волонтерами і привернув міжнародну увагу завдяки недавній нічиїй з «Бока Хуніорс» (Boca Juniors), наразі не має адміністративних прав на сторінки і співпрацює з експертами з кібербезпеки та владою для вирішення проблеми…» ***(Auckland City FC plagued by social media cyber attack // Radio New Zealand (https://www.rnz.co.nz/news/sport/578154/auckland-city-fc-plagued-by-social-media-cyber-attack). 07.11.2025).***

***

«У звіті KasadaIQ про тенденції кіберзагроз у святковий період 2025 року міститься попередження про те, що онлайн-шахрайство стає індустріалізованим бізнесом, що базується на штучному інтелекті, який досягне піку раніше і буде сильнішим, ніж у будь-якому попередньому році. З січня по жовтень кількість зловмисних «конфігурацій» (готових скриптів для крадіжки облікових даних, скрейпінгу та автоматизованої оплати), спрямованих проти роздрібних продавців, зросла на 92%, а кількість тих, що націлені на готелі та ресторани швидкого обслуговування, злетіла на 400% — більшість з них з'явилася за 10–14 днів до «Чорної п'ятниці», щоб злочинці могли доопрацювати атаки та перепродати перевірені набори… Захоплення облікових записів зараз є найшвидше зростаючим каналом шахрайства: понад 311 мільйонів викрадених облікових даних — дві третини з яких пов'язані з роздрібними брендами — вже виставлені на продаж, а Kasada зафіксувала 1100 випадків заповнення облікових даних проти 133 роздрібних продавців за один місяць. Отримавши доступ до облікових записів, зловмисники конвертують цінність, викачуючи кошти з подарункових карток — найпростіший і найприбутковіший спосіб виведення грошей. Майже 17 мільйонів викрадених карток роздрібних мереж і мереж швидкого харчування продаються на

підпільних форумах, а кількість оголошень різко зростає напередодні «Чорної п'ятниці», знову в середині грудня і залишається високою до Нового року. Боти на базі штучного інтелекту генерують більшу частину веб-трафіку під час свят, імітуючи поведінку людей під час перегляду веб-сторінок, реєструючи фальшиві облікові записи лояльності, збираючи дані з API-інтерфейсів запасів і здійснюючи оплату за лічені мілісекунди, що робить захист на основі тарифів застарілим. Весь цикл злочину — порушення, перепродаж, монетизація — скоротився до менше ніж п'яти днів…

Касада рекомендує захисникам перейти в «святковий режим» до 10 листопада, поєднати ботів, шахрайство та телеметрію SOC, посилити кінцеві точки API, розгорнути адаптивну MFA та поведінкове відбиття пальців, а також відстежувати кримінальні ринки для раннього попередження. Тільки організації, які поєднують видимість у реальному часі з гнучкою реакцією між командами, зможуть йти в ногу з супротивниками, чия автоматизація зараз конкурує (і часто імітує) законну діяльність клієнтів…» ***(Holiday Fraud Trends 2025: The Top 5 Cyber Threats to Watch This Season // Techstrong Group Inc. (https://securityboulevard.com/2025/11/holiday-fraud-trends-2025-the-top-5-cyber-threats-to-watch-this-season/). 06.11.2025).***

***

«У сучасному цифровому середовищі кібератаки є неминучими і набувають все більшого розмаху, а глобальні витрати на боротьбу з кіберзлочинністю, за прогнозами, перевищать 10,5 трлн доларів на рік, що робить кібербезпеку основним ризиком для бізнесу, а не лише проблемою ІТ-відділу. Злочинці стають дедалі витонченішими, націлюючись на організації за допомогою спіфішингу (високо персоналізованих атак, що імітують надійні джерела), шкідливого програмного забезпечення (включаючи програми-вимагачі, віруси, черв'яки та шпигунське програмне забезпечення), крадіжки облікових даних через слабкі або повторно використані паролі, внутрішніх загроз (як зловмисних, так і випадкових) та нових ризиків, таких як генеровані штучним інтелектом дипфейки, порушення безпеки ланцюгів постачання, неправильні налаштування хмарних сервісів та зловживання пристроями Інтернету речей…

Реальні інциденти підкреслюють можливі руйнівні наслідки: у 2024 році служба охорони здоров'я NHS Dumfries and Galloway зазнала атаки програм-вимагачів, в результаті якої було викрадено та оприлюднено 3 ТБ даних пацієнтів, коли викуп не був сплачений, що порушило надання медичної допомоги та спричинило розслідування; у 2022 році науковий співробітник Yahoo викрав 570 000 сторінок запатентованих рекламних алгоритмів для конкурента, викривши небезпеку, яку становлять привілейовані інсайдери; а у 2025 році Allianz Life втратила 1,1 мільйона записів про клієнтів через вразливу хмарну CRM-платформу третьої сторони, що підкреслило слабкість ланцюга поставок…

Щоб захистити себе, підприємства повинні застосовувати багаторівневі засоби захисту: регулярне навчання співробітників із використанням симуляцій фішингу, обов'язкову багатофакторну автентифікацію та доступ із мінімальними привілеями, оперативне встановлення виправлень та оновлень, надійні брандмауери та захист кінцевих точок, сегментацію мережі, безпечні резервні копії поза межами

підприємства з регулярним тестуванням та чіткі політики обробки даних. Багато організацій також переходять на архітектуру Zero Trust, стикаючись із зростаючими регуляторними вимогами (GDPR, CCPA, нові закони про штучний інтелект) та атаками на основі штучного інтелекту, які автоматизують та персоналізують загрози…

Страхування кібербезпеки стало важливою запорукою безпеки, що покриває реагування на інциденти, криміналістичну експертизу, відновлення даних, юридичні витрати, штрафи та управління репутацією у разі порушення безпеки. Зрештою, в епоху невпинних і постійно еволюціонуючих загроз, проактивна профілактика, пильність співробітників, ефективне управління та фінансова підготовленість є єдиними надійними способами для підприємств захистити свої дані, діяльність та репутацію». ***(Muthmainur Rahman. Enhancing Business Security: Common Cybersecurity Threats and Effective Protection Strategies // Ankura Consulting Group, LLC (https://angle.ankura.com/post/102lq2l/enhancing-business-security-common-cybersecurity-threats-and-effective-protectio). 06.11.2025).***

***

«…хакери намагаються викрасти паролі на X (раніше Twitter), надсилаючи фальшиві повідомлення про авторські права…

Зазвичай повідомлення надходять електронною поштою та містять твердження про отримання повідомлення DMCA щодо вашого облікового запису. Воно містить велику кнопку «переглянути деталі» та попередження про те, що видимість вашого облікового запису може бути обмежена, якщо ви не відповісте…

Однак, якщо ви натиснете кнопку та введете свої дані для входу, ви фактично надасте зловмисникам доступ до вашого облікового запису. Якщо ваш обліковий запис було скомпрометовано, X попросить вас відвідати сторінку довідки щодо скомпрометованих облікових записів…» ***(Davey Winder. X Users Warned Not To Review These Tweets — It's A Hacker Trap // Forbes Media LLC (https://www.forbes.com/sites/daveywinder/2025/11/15/this-message-from-x-is-actually-an-attack-dont-review-your-details/). 15.11.2025).***

***

«У той час як Лас-Вегас готується до Гран-прі Формули-1, експерти з кібербезпеки попереджають, що справжня гонка також відбуватиметься в Інтернеті, де як туристи, так і місцеві жителі стикаються з підвищеним ризиком цифрових шахрайств та атак. Місто вже є головним об'єктом для кіберзлочинців, про що свідчить нещодавній інцидент з програмним забезпеченням-вимагачем у Неваді та дорогий злом MGM Resorts, в результаті якого були викрадені дані гостей. У вихідні дні, присвячені F1, місто відвідують сотні тисяч туристів, готелі переповнені, а кількість цифрових платежів та активність в Інтернеті різко зростають, що, на думку експертів, створює «ідеальну можливість» для зловмисників…

Люди можуть отримувати дуже переконливі підроблені текстові повідомлення, електронні листи, QR-коди або повідомлення в соціальних мережах, в яких пропонуються оновлення квитків в останню хвилину, знижки на паркування

або пропозиції, пов'язані з F1, які, на перший погляд, надходять від команд, готелів або продавців квитків; натискання на них може призвести до викрадення облікових даних або зараження шкідливим програмним забезпеченням. Фахівці з кібербезпеки наголошують, що слабкі, повторно використовувані паролі, застарілі програми та програмне забезпечення без оновлень роблять людей особливо вразливими, коли місто перебуває під таким тиском, і закликають усіх використовувати надійні, унікальні паролі та ставитися до небажаних пропозицій, особливо тих, що здаються занадто хорошими, щоб бути правдою, з особливою обережністю». ***(Abel Garcia. Cybersecurity experts warn of increased scam risks during Formula 1 Las Vegas Grand Prix // Scripps Media, Inc (https://www.ktnv.com/news/cybersecurity-experts-warn-of-increased-scam-risks-during-formula-1-las-vegas-grand-prix). 21.11.2025).***

***

«Система публічного оповіщення CodeRED, яка використовується службою з надзвичайних ситуацій округу Атчісон, наразі не працює через нещодавній інцидент з кібербезпекою...

Під час цього відключення округ використовуватиме Інтегровану систему оповіщення та попередження населення (IPAWS) лише для надзвичайних ситуацій та повідомлень, що стосуються безпеки життя, якщо це буде необхідно.

IPAWS не може використовуватися для повідомлень, що не стосуються надзвичайних ситуацій або є суто інформаційними. Система регулюється на федеральному рівні FEMA і призначена виключно для надсилання термінових повідомлень, що стосуються громадської безпеки.

Мешканцям рекомендується стежити за місцевими новинами, офіційними веб-сайтами округу/міста та офіційними сторінками в соціальних мережах, щоб отримувати оновлення та інформацію, яка зазвичай поширюється через CodeRED». ***(Cameron Montemayor. Cybersecurity incident damages notification system for Atchison County Emergency Management // NEWS-PRESS & GAZETTE CO. (https://www.newspressnow.com/public-safety/2025/11/19/cybersecurity-incident-damages-notification-system-for-atchison-county-emergency-management/). 19.11.2025).***

***

«…17 листопада 2025 року кібератака на короткий час вивела з ладу десятки веб-сайтів уряду Кенії, відобразивши повідомлення про пошкодження, такі як «Доступ заборонено PCP» та «14:88 Хайль Гітлер». Головний секретар міністерства внутрішніх справ Реймонд Омолло підтвердив цей інцидент, заявивши, що попереднє розслідування вказує на групу, яка називає себе «PCP@Kenya». Команди екстреного реагування активували процедури відновлення після інциденту, співпрацювали із зовнішніми зацікавленими сторонами та відновили роботу уражених порталів міністерств внутрішніх справ, охорони здоров'я, освіти, енергетики, праці, водних ресурсів, імміграції, DCI, Державного будинку та інших. Системи знову працюють і перебувають під постійним моніторингом, а захисні заходи посилюються для виявлення та нейтралізації майбутніх загроз…

Омолло, який очолює Національний координаційний комітет з питань комп'ютерних та кіберзлочинів, назвав цей злом порушенням кенійського законодавства і пообіцяв, що винні будуть притягнуті до відповідальності відповідно до Закону про неправомірне використання комп'ютерних систем та кіберзлочини, Закону про інформацію та комунікації Кенії та Закону про захист даних. Громадськість закликали повідомляти про будь-які підозрілі дії через офіційні канали, такі як Національний KE-CIRT/CC». ***(State websites restored after cyber breach, incident contained // The Star (https://www.the-star.co.ke/news/2025-11-17-state-websites-restored-after-cyber-breach). 17.11.2025).***

***

«Групи, що використовують просунуті постійні загрози, все частіше націлюються на слабкі місця в процесах управління, ризиків та дотримання вимог (GRC) організацій, а не покладаються виключно на технічні експлойти, попереджає Мохаммед Альмунаджам із саудівської академії Туваїк. Під час нещодавніх криміналістичних розслідувань він побачив, як зловмисники маніпулювали робочими процесами затвердження, графіками дотримання вимог, часовими мітками журналів подій та іншими «логічними» прогалинами, щоб непомітно обійти засоби контролю, перетворюючи GRC на об'єкт атаки…

Щоб протидіяти цій тенденції, Алмунаджам сформулював «6 законів Black Hat» — поведінкову модель, яка відображає, як сучасні APT-групи використовують часові вікна, точки прийняття рішень та лазівки в політиках для досягнення стійкості. На конференції Black Hat Middle East & Africa 2025 він продемонструє випадки, в яких зловмисники затримували виявлення витоку даних шляхом зміни часових міток або використовували передбачувані процедури дотримання вимог, щоб обійти засоби безпеки…

Замість того, щоб купувати нові точкові продукти, він радить компаніям привести внутрішню політику у відповідність до реальних загроз: зіставити наміри зловмисників з заходами управління, ретельно перевіряти винятки щодо привілейованого доступу та вводити дані GRC в аналітику SOC, щоб зловживання виявлялися до того, як вони стануть причиною компрометації. Зрілі команди з безпеки можуть швидко впровадити ці заходи, каже він, закривши «тихі шляхи», які технологія сама по собі не може побачити». ***(Arielle Waldman. Hack the Hackers: 6 Laws for Staying Ahead of the Attackers // TechTarget, Inc. (https://www.darkreading.com/cyber-risk/hack-hackers-6-laws-staying-ahead-cyberattackers). 21.11.2025).***

***

«…Компанії, що розробляють відеоігри, стали головними цілями кібератак: інструменти для обману загрожують цілісності ігор, злочинці-хакери шукають цінні ігрові предмети та особисті дані, а державні структури розглядають ігрову інфраструктуру як важливу цифрову власність. Як наслідок, регуляторні органи ЄС поширюють на цей сектор основні правила щодо критичної інфраструктури та додають нові зобов'язання, що стосуються конкретних продуктів…

Основні кіберризики

• Маніпулювання ігровим процесом та економікою: експлойти та боти спотворюють конкуренцію та копіюють віртуальні товари.

• Витік даних: студії зберігають величезні масиви платіжних даних, аналітики поведінки та комерційних таємниць (наприклад, витік інформації про GTA VI від Rockstar у 2022 році).

• Оперативний саботаж: атаки на ігрові або дистрибуційні сервери можуть нагадувати атаки на інші критично важливі системи…

Альтернативні механізми вирішення спорів та співпраця (наприклад, розподіл доходів між лейблами та платформами UGC або ліцензійні угоди між видавцями новин та моделями штучного інтелекту) все частіше замінюють марні судові процеси в швидкозмінному цифровому середовищі. Суди також почали застосовувати «динамічні судові заборони», які дозволяють правовласникам блокувати нові піратські сайти без повторних судових процесів…

Нові вимоги ЄС щодо відповідності

• Директива NIS2 (введена в дію з жовтня 2024 року) поширюється на всі середні та великі підприємства, які використовують або залежать від послуг цифрової інфраструктури, таких як хмарні сервіси, CDN або центри обробки даних, що опосередковано стосується багатьох видавців ігор. Зобов'язання включають кіберуправління на рівні правління, детальний технічний контроль, повідомлення про інциденти протягом 24/72 годин та добровільний обмін інформацією про загрози під загрозою відповідальності керівництва.

• Закон про кіберстійкість (CRA) (набуває чинності в грудні 2024 року; повне виконання до 2027 року) вимагає забезпечення безпеки за замовчуванням, управління вразливостями та звітування ENISA щодо всіх «продуктів з цифровими елементами». Більшість програмних ігор підпадають під режим самооцінки, тоді як підключене обладнання (консолі, смарт-аксесуари) підпадає під більш суворі правила класу I/II або «критичних продуктів», а також під великі штрафи за недотримання вимог.

Кроки, які слід вжити компаніям, що розробляють ігри

Картографічні сервіси: визначте хмарні/CDN та інші залежності від цифрової інфраструктури, що активують NIS2.

Впровадьте на рівні правління нагляд, аналіз ризиків, безпеку ланцюга постачання, MFA та плани безперервності бізнесу відповідно до NIS2.

Для будь-якого підключеного обладнання або важливого програмного забезпечення розпочніть аналіз прогалин CRA; впровадьте безпеку за замовчуванням, заплануйте тести на проникнення, заплануйте швидкі канали виправлення та документацію для самодекларацій або зовнішніх аудитів.

Впроваджуйте динамічні заходи захисту даних (наприклад, диференційоване резервне копіювання, обмеження терміну зберігання даних) для зменшення витрат на енергію для зберігання та підвищення стійкості.

Використовуйте інструменти моніторингу на основі штучного інтелекту для виявлення підробок та автоматичного видалення; розгляньте можливість медіації/ліцензування замість судових розглядів у спорах, пов'язаних із контентом, створеним користувачами, або навчанням штучного інтелекту.

Проводьте регулярні перевірки свободи діяльності, щоб уникнути патентних та інтелектуальних прав у швидко розвиваючихся технологіях ігор та активах метавсесвіту…

Інтегруючи проактивну кібергігієну в нові режими ЄС, ігрові компанії можуть мінімізувати збитки від порушень, зберегти довіру гравців і відповідати зростаючим вимогам до безпеки цифрових продуктів, одночасно підтримуючи більш екологічний IT-слід». ***(Jasper Geerdes, Jurriaan Jansen. Video gaming and cybersecurity: Navigating legal and technological challenges // Norton Rose Fulbright(https://www.nortonrosefulbright.com/en/knowledge/publications/77cbcb67/video-gaming-and-cybersecurity). 11.2025).***

***

«Супутникові мережі, які раніше вважалися занадто нішевими та ізольованими, щоб привабити хакерів, тепер є головним полем кібербоїв. Нещодавні дослідження виявили 16 серйозних вразливостей у широко використовуваних комерційних супутникових модемах, включаючи незашифровані оновлення прошивки та відкриті веб-інтерфейси, що доводить, що багато космічних систем все ще покладаються на десятиліття старі припущення про «безпеку через невідомість». Державні суб'єкти та кіберзлочинці звернули на це увагу: звіт Microsoft про цифрову оборону та інші дослідження показують, що супротивники використовують ланцюги постачання, застарілі протоколи та застаріле обладнання для порушення роботи військових і комерційних супутникових зв'язків, які підтримують глобальне командування та контроль, морське та авіаційне сполучення, нафтогазові операції та реагування на надзвичайні ситуації…

Ставки високі. Для Міністерства оборони США SATCOM є життєво важливим засобом ведення війни; для підприємств він є основою критично важливих послуг та національної економіки. Однак багато супутників були спроектовані з урахуванням екстремальних рівнів радіації та температури, а не з урахуванням програм-вимагачів або експлойтів нульового дня. Модернізація системи безпеки є складною, але необхідною. Comtech та інші компанії стверджують, що сучасна архітектура супутників повинна включати принципи «безпеки за замовчуванням» та дотримуватися багаторівневого підходу «нульової довіри»:

- Аутентифікація з нульовим рівнем довіри на кожному етапі — відсутність неявної довіри між супутниками, наземними станціями або хмарними контролерами.
- Криптографічно підписані ланцюжки безпечного завантаження та аутентифіковані бездротові оновлення прошивки.
- Криптографічна гнучкість для ротації ключів та переходу на постквантові алгоритми протягом 15–30 років терміну експлуатації.
- Мови з безпечною пам'яттю, такі як Rust, пісочниця та ретельне фуз-тестування для усунення класичних недоліків переповнення буфера, поширених у C/C++.
- Постійний моніторинг часу виконання та виявлення аномалій для виявлення ненормальних потоків пакетів або зловмисних змін конфігурації.
- Глибока оборона в гібридних архітектурах, де супутникові системи взаємодіють з наземними та хмарними мережами…

Співпраця в масштабах всієї галузі має вирішальне значення. Comtech закликає операторів вимагати сертифікати FIPS/Common-Criteria, наполягати на прозорих практиках постачання програмного забезпечення, проводити незалежне тестування «червоної команди», створювати посібники з реагування на кіберінциденти для космічних систем та обмінюватися інформацією про загрози через такі групи, як Space ISAC та NIST. Компанія модернізує власний портфель Digital Common Ground за допомогою безпечного вбудованого програмного забезпечення, перевірок цілісності ланцюга постачання та моніторингу часу виконання…

Ера «відкритих вхідних дверей» закінчилася. У наступному десятилітті переможці SATCOM будуть ставитися до супутників як до критично важливих кіберресурсів, розроблених з нуля для забезпечення стійкості до наземних і орбітальних атак. Стійкість більше не є опцією; вона є основою майбутньої космічної та комунікаційної інфраструктури». ***(Cybersecurity in the Space Domain: Why It's Time to Stop Leaving the Front Door Unlocked // Comtech Telecommunications Corp.(https://comtech.com/it/general/2025/11/21/cybersecurity-in-the-space-domain-why-its-time-to-stop-leaving-the-front-door-unlocked/). 21.11.2025).***

***

«Основна картина кіберзагроз змінилася набагато менше, ніж це можна судити з заголовків новин, вважає Кіаран Мартін, колишній глава Національного центру кібербезпеки Великобританії. Західні економіки як і раніше стикаються з тими ж чотирма акторами і мотивами, які домінували в минулому десятилітті: китайським шпигунством, російськими деструктивними діями, іранським хактивізмом і північнокорейським політичним втручанням — тепер у поєднанні з високоприбутковою кіберзлочинністю. Змінилася лише ефективність: зловмисники завдають більших операційних збитків і фінансових втрат. Наприклад, Північна Корея лише у 2025 році викрала близько 3 мільярдів доларів США, переважно з «мостів» криптовалюти. Злочинні угруповання також навчилися зупиняти виробничі лінії, як показав випадок, коли злом Jaguar Land Rover зупинив виробництво автомобілів у Великій Британії і завдав економіці збитків на суму близько 1,9 мільярда фунтів стерлінгів…

Інструменти штучного інтелекту не змінили ландшафт загроз, але вони роблять атаки дешевшими та ефективнішими, вдосконалюючи бізнес-модель злочинців. Для фінансових установ ставки вищі, оскільки (1) новіші активи, такі як криптовалюта, є більш вразливими, (2) конфіденційні дані сектору легко монетизуються, і (3) перебої в наданні послуг мають системний вплив. Тому компанії повинні розрізняти, які порушення дійсно мають значення, а не ставитися однаково до кожного витоку малоцінних персональних даних…

Хоча масштабні кіберінциденти рідко коштують людських життів, альянс «П'ять очей» попереджає, що проникнення Китаю в критичну інфраструктуру може змінити ситуацію в майбутній кризі. Мартін стверджує, що квантові обчислення навряд чи «зруйнують Інтернет»; квантостійка криптографія вже розробляється і з'явиться разом із квантовими можливостями. Стратегічна гонка полягає в тому, яка країна першою застосує квантові переваги, а не в кінці сучасного шифрування». ***(Darcy Song. Same attacks, more pain: Cyber security face up to exponential threats //***

Conexus Financial (https://www.top1000funds.com/2025/11/same-attacks-more-pain-cyber-security-face-up-to-exponential-threats/). 21.11.2025).

***

«13 листопада 2025 року компанія Eurofiber France виявила, що хакери скористалися вразливістю в її внутрішній системі управління квитками та клієнтському порталі ATE — платформах, які використовують її французькі бренди Eurafibre, FullSave, Netiwan, Avelia та Eurofiber Cloud Infra France. Зловмисники викрали дані клієнтів, але критична інфраструктура, банківська інформація та послуги не постраждали, а діяльність Eurofiber у Бельгії, Німеччині та Нідерландах не була порушена…

Eurofiber виправила недолік, посилила моніторинг, залучила зовнішніх фахівців і повідомила про порушення французькому органу з захисту даних (CNIL) та агентству з кібербезпеки (ANSSI) відповідно до правил GDPR. Компанія також подала кримінальну скаргу за вимагання, вказавши, що зловмисники, ймовірно, вимагали викуп. Клієнти були повідомлені про це та отримали відповідні вказівки…

Цей інцидент, який було швидко локалізовано без перебоїв у роботі, підкреслює постійний ризик вразливості програмного забезпечення на бізнес-платформах та важливість проактивного виправлення, сегментації систем та перевірки безпеки сторонніми організаціями у всьому секторі цифрової інфраструктури Європи». ***(Hackers Steal Sensitive User Data After Exploiting Eurofiber Security Vulnerability // Cyber Press (https://cyberpress.org/eurofiber-security-vulnerability/). 18.11.2025).***

***

«Кілька лондонських рад, включаючи Королівський район Кенсінгтон і Челсі (RBKC) та Вестмінстерську міську раду (WCC), зазнали серйозної кібератаки, яка могла поставити під загрозу дані мешканців. Цей інцидент, який також вплинув на раду Хаммерсміта і Фулема через спільні IT-системи, змусив як RBKC, так і WCC повідомити про це Управління комісара з питань інформації та співпрацюють із спеціалізованими командами реагування на інциденти та Національним центром кібербезпеки (NCSC) з метою забезпечення безпеки систем, розслідування можливого витоку даних та відновлення послуг. Електронна пошта та телефонні ресурси були перенаправлені для надання допомоги населенню, оскільки «деякі системи» залишаються відключеними…

Експерти з безпеки, серед яких Грем Стюарт з Check Point, стверджують, що така схема — виведення з ладу декількох районів, внутрішні попередження про необхідність уникати міжрайонівного обміну електронною поштою — свідчить про те, що зловмисники отримали доступ до облікових даних і перемістилися по спільній інфраструктурі, що підвищує ризик викрадення даних або використання програм-вимагачів. Районні ради зберігають конфіденційну інформацію, таку як файли соціального забезпечення та житлові записи, що робить їх привабливою мішенню…

NCSC і, за повідомленнями, столична поліція оцінюють інцидент, який підкреслює вразливість місцевих органів влади, які намагаються впоратися з великим обсягом цифрової роботи при обмеженому бюджеті та неоднаковій

кіберзрілості…» ***(Tim Baker. London councils hit by 'cyber attack' with data potentially compromised // Sky UK (https://news.sky.com/story/london-councils-hit-by-cyber-attack-with-data-potentially-compromised-13475400). 26.11.2025).***

***

«У святковий сезон різко зростає кіберризик для роздрібної торгівлі. Під час ажіотажу Чорної п'ятниці/Кіберпонеділка 2025 року зловмисники використовують перевантажені ІТ-команди, різке зростання трафіку електронної комерції та розгалужені мережі постачальників для розгортання програм-вимагачів, фішингу та автоматизованих ботів для введення облікових даних…

Ключові моменти

• Середня сума викупу в роздрібній торгівлі подвоїлася і становить близько 2 мільйонів доларів.

• Майже 50 % інцидентів пов'язані з «невідомими прогалинами в безпеці»: неправильною конфігурацією, незахищеним програмним забезпеченням і мережами з «сліпими зонами».

• У листопаді минулого року кількість фішингових кампаній зросла на 692 %; святкові пропозиції приваблюють співробітників і клієнтів, встановлюючи шкідливе програмне забезпечення для поширення.

• Удари по ланцюжку поставок мають каскадний ефект: програмне забезпечення для вимагання викупу на японському Askul зупинило онлайн-продажі Muji; порушення безпеки британського постачальника програмного забезпечення Blue Yonder порушило роботу Starbucks і Morrisons…

Рекомендовані заходи захисту

• Перехід від реактивної до превентивної, багаторівневої безпеки.

• Використання технології Moving Target Defense (наприклад, Morphisec AMTD) для рандомізації пам'яті та блокування нульових днів, безфайлових експлойтів на POS і серверах.

• Впровадження технології обману — цифрових приманок, які сповіщають тільки про реальну зловмисну діяльність — без перешкоджання напруженій роботі роздрібної торгівлі…

У пікові періоди продажів очікуються логістичні проблеми, але кризи в області кібербезпеки не повинні бути неминучими. Проактивний захист кінцевих точок, моніторинг ланцюгів поставок і постійна обізнаність про фішинг є необхідними умовами для збереження доходів і якості обслуговування клієнтів в умовах зростання вимог про викуп і складності атак». ***(Ransomware Groups Target Retailers Ahead of the Holiday Season With Malicious Payload Campaigns // Cyber Press (https://cyberpress.org/retail-ransomware-threats/). 21.11.2025).***

***

«Аналітики з безпеки компанії Oligo викрили «ShadowRay 2.0» — глобальну кампанію, яка використовує відкриту платформу Ray AI-orchestration для майнінгу криптовалюти. Зловмисники, які використовують псевдонім IronErn440, експлуатують вразливість Ray CVE-2023-48022, яка залишає

API Jobs і панель управління без аутентифікації. До листопада 2025 року понад 230 000 екземплярів Ray, включаючи ті, що використовуються в стартапах і дослідницьких лабораторіях, були доступними і потенційно піддавалися ризику…

Потік атаки

Розвідка за допомогою зондів interact.sh для виявлення незахищених панелей Ray без шумного сканування.

Віддалене виконання коду: неавтентифіковані POST-запити надсилають шкідливі завдання Ray, які виконуються з привілеями на рівні кластера.

Бічне поширення: корисні навантаження Python використовують NodeAffinitySchedulingStrategy Ray для переліку вузлів, копіювання скриптів інфікування та виділення ~60 % ресурсів CPU/GPU — достатньо для отримання прибутку, але недостатньо для того, щоб привернути увагу…

Стійкість: завдання cron, перехоплення systemd та скидання ключів root-SSH. Процеси маскуються під робочі процеси ядра (наприклад, [kworker/0:0]).

Монетизація та боротьба за територію: вбудовані майнери підключаються до пулів, специфічних для регіону; скрипти вбивають майнерів-конкурентів та блокують конкуруючі пули за допомогою iptables та редагування файлів hosts…

Гнучкість інфраструктури

• Початкові корисні навантаження розміщувалися на репозиторії GitLab; після видалення 5 листопада 2025 року зловмисники перенесли код на GitHub до 10 листопада, продемонструвавши «інфраструктуру як код» у стилі DevOps.

• Корисні навантаження адаптуються шляхом запиту до ip-api.com для надання проксі-серверів і бінарних файлів, адаптованих для китайських або міжнародних жертв.

• Інструменти штучного інтелекту, ймовірно, допомогли створити відмовостійкі скрипти, що самостійно оновлюються…

Стрибок з «тисяч» до понад 230 тисяч відкритих серверів Ray збільшує площу атаки для хмарних і AI-кластерів по всьому світу, що робить ShadowRay 2.0 значним посиленням порівняно з версією березня 2024 року. Організації, що використовують Ray, повинні негайно встановити виправлення CVE-2023-48022, заблокувати API-інтерфейси завдань, забезпечити аутентифікацію та стежити за незрозумілими процесами, що запускаються Ray, підробками [kworker/*] або завантаженнями GitHub/GitLab у завданнях cron та systemd». ***(Tushar Subhra Dutta. New ShadowRay Attack Exploit Ray AI-Framework Vulnerability to Attack AI Systems // Cyber Security News (https://cybersecuritynews.com/new-shadowray-attack-exploit-ray-ai-framework/). 19.11.2025).***

***

«Агентство з кібербезпеки та безпеки інфраструктури США (CISA) опублікувало попередження про те, що хакери, які фінансуються державою, та оператори комерційного шпигунського програмного забезпечення активно атакують Signal, WhatsApp та інші мобільні месенджери. Використовуючи фішинг, підроблені QR-коди, шкідливі програми-двійники та навіть експлойти без кліків, зловмисники спочатку встановлюють шпигунське програмне забезпечення, а

потім запускають додаткові програми, щоб отримати повний доступ до телефонів жертв…

Цілями є високопоставлені урядовці, військові та політичні діячі, а також групи громадянського суспільства в США, Європі та на Близькому Сході. Останні випадки:

• Групи, пов'язані з Росією, зловживали функцією «пов'язані пристрої» Signal, обманюючи користувачів, щоб вони сканували підроблені QR-коди, і непомітно додавали пристрій, контрольований зловмисниками, щоб усі майбутні повідомлення копіювалися в режимі реального часу.

• Кампанія під назвою LANDFALL використовувала як вразливість Samsung, так і експлойт зображень WhatsApp без кліків, щоб встановити шпигунське програмне забезпечення на пристрої Galaxy без взаємодії з користувачем.

• Інші групи поширювали шкідливе програмне забезпечення для Android (ProSpy, ToSpy, ClayRat) через підроблені додатки Signal, Telegram, TikTok і YouTube, збираючи чати, записи та файли…

Бюлетень CISA з'явився в той час, коли американські регулятори вживають жорстких заходів щодо постачальників комерційного шпигунського програмного забезпечення (наприклад, NSO Group) і навіть забороняють використання певних месенджерів на пристроях членів Конгресу, підкреслюючи, що зловмисники обходять шифрування, атакуючи кінцеві точки та функції облікових записів, що знаходяться під ним». ***(Carly Page. CISA warns spyware crews are breaking into Signal and WhatsApp accounts // The Register (https://www.theregister.com/2025/11/25/cisa_spyware_gangs/). 25.11.2025).***

***

Діяльність хакерів та хакерські угруповування

«…YouTube Ghost Network, стійка кіберзлочинна організація, що діє з 2021 року і активність якої в 2025 році зросла втричі, використовує поєднання соціальних маніпуляцій і технічних засобів приховування, щоб націлюватися на користувачів, які шукають «хаки/чіти для ігор» та «краки/піратське програмне забезпечення». Мережа створює помилкове відчуття безпеки, використовуючи зламані або фальшиві акаунти для публікації скоординованих позитивних коментарів, лайків та дописів у спільнотах, завдяки чому контент виглядає легітимним і стійким до індивідуальних спроб його видалення…

Коли користувачі натискають на надані посилання, вони перенаправляються на сервіси обміну файлами або фішингові сайти, які містять архіви, захищені паролем, що ускладнює їх сканування антивірусними програмами, і отримують вказівку вимкнути Windows Defender перед інсталяцією, тим самим знешкоджуючи власний захист. Ці атаки в першу чергу поширюють потужне шкідливе програмне забезпечення для викрадення інформації, таке як Lumma Stealer і Rhadamanthys, яке збирає паролі, дані браузера та конфіденційну інформацію. Стійкість мережі пояснюється її рольовою структурою, в якій заблоковані акаунти швидко

замінюються іншими, що спеціалізуються на завантаженні, розміщенні посилань або підвищенні авторитетності.

Основні кампанії, зафіксовані Check Point Research, включали використання інфокрадера Rhadamanthys через скомпрометований канал та інший, що використовував великий канал (@Afonesio1) для розповсюдження зламаних версій професійного програмного забезпечення через фішингові сторінки, які прямо вимагали від користувачів вимкнути програмне забезпечення для захисту. Навіть відвідування цих сайтів, на які ведуть посилання, становить ризик крадіжки облікових даних.

Для забезпечення безпеки користувачам рекомендується уникати завантаження зламаного програмного забезпечення, ніколи не вимикати антивірус або Windows Defender, коли з'являється відповідне повідомлення, використовувати надійне антивірусне рішення, яке працює постійно, бути обережними з посиланнями на YouTube та отримувати програмне забезпечення тільки з офіційних джерел. Для додаткового захисту необхідна багаторівнева безпека: увімкнення двофакторної автентифікації (2FA), використання менеджера паролів для безпечного зберігання облікових даних, оновлення всього програмного забезпечення та розгляд можливості використання надійної служби видалення даних, щоб обмежити обіг особистої інформації в Інтернеті, якою можуть скористатися кіберзлочинці…» ***(Kurt Knutsson. 3,000+ YouTube videos deliver malware disguised as free software // FOX News Network, LLC. (https://www.foxnews.com/tech/3000-youtube-videos-deliver-malware-disguised-free-software). 03.11.2025).***

***

«Китайська урядова хакерська група, ідентифікована Google як UNC6384 і дуже схожа на відомого зловмисника «Mustang Panda», нещодавно, у вересні та жовтні, здійснила атаку на європейських дипломатів з Угорщини, Бельгії, Сербії, Італії та Нідерландів, використовуючи фішингові електронні листи. Ця кампанія кібершпигунства використовує давню, не виправлену вразливість у файлах ярликів Windows (.LNK), яка дозволяє приховувати команди командного рядка в пробілах файлу — техніку, популярну серед різних урядових груп з 2017 року…

У цій кампанії шкідливі файли .LNK розгортають троян PlugX для віддаленого доступу після того, як заманюють жертв, показуючи їм підроблений PDF-файл із справжнім порядком денним засідання Європейської комісії. Хоча про цю конкретну вразливість (CVE-2025-9491 або ZDI-CAN-25373) компанія Trend Micro повідомила Microsoft у 2024 році, а раніше — у 2017 році, Microsoft відмовилася випустити патч безпеки, стверджуючи, що ця проблема не є вразливістю. Microsoft стверджує, що для успішного використання уразливості необхідна значна взаємодія з користувачем, оскільки система вже видає попередження про безпеку, коли користувачі намагаються відкрити ненадійні файли .LNK, особливо ті, що завантажені з Інтернету…

Компанія Arctic Wolf, яка виявила цю кампанію, зазначає, що швидке використання UNC6384 цієї вразливості свідчить про доступ до передових ресурсів і вказує на масштабну операцію зі збору розвідувальної інформації в декількох європейських країнах. Оскільки патч недоступний, Arctic Wolf радить організаціям

зменшити ризик, заблокувавши виконання файлів .LNK у всіх системах Windows, надавши пріоритет кінцевим точкам, які використовуються персоналом, що обробляє конфіденційну дипломатичну інформацію, та здійснюючи моніторинг пов'язаних елементів ланцюжка експлуатації, таких як утиліта Canon printer assistant cnmpaui.exe. Повторне використання вразливостей ярликів Windows підкреслює складність виправлення цього типу вразливостей без порушення роботи законних застарілих додатків». ***(John E. Dunn. Chinese hackers target Western diplomats using hard-to-patch Windows shortcut flaw // FoundryCo, Inc. (https://www.csoonline.com/article/4082701/chinese-hackers-target-western-diplomats-using-hard-to-patch-windows-shortcut-flaw.html). 06.11.2025).***

***

«…Група хакерів Rhysida (раніше Vice Society), що спеціалізується на розробці програм-вимагачів, розпочала нову кампанію з використанням шкідливої реклами, яка націлена на користувачів екосистеми Microsoft і використовує власну інфраструктуру Microsoft для підписання коду, щоб виглядати надійною. Зловмисники купують рекламу в пошуковій системі Bing для популярних інструментів, таких як Microsoft Teams, Zoom і PuTTY; коли співробітник натискає на рекламу, він перенаправляється на схожу сторінку завантаження, на якій помітна кнопка «Завантажити» запускає зашифрований завантажувач «OysterLoader». Це шкідливе програмне забезпечення уникає раннього виявлення, встановлює стійкість, а потім завантажує додаткові корисні дані (включаючи завантажувач Latrodectus) для більш глибокого вторгнення в мережу та крадіжки даних…

Щоб придушити попередження про безпеку, Rhysida підписує свої бінарні файли сертифікатами, що виглядають законними, багато з яких отримано шляхом зловживання службою Trusted Signing від Microsoft. Хоча ці сертифікати зазвичай втрачають чинність через 72 години, угруповання настільки ефективно автоматизувало процес підписання, що може поширювати свіже, належним чином підписане шкідливе програмне забезпечення до того, як кожен сертифікат втратить чинність. Дослідники каталогізували понад 40 різних сертифікатів, пов'язаних з Rhysida, з червня 2025 року, що на 7 більше, ніж у тому ж періоді минулого року. Microsoft вже анулювала понад 200 підозрілих сертифікатів, проте Expel та інші аналітики стверджують, що схема зловмисної реклами залишається активною, підкреслюючи здатність групи «прослизати крізь щілини» існуючих засобів контролю безпеки». ***(Izabelė Pukėnaitė. Rhysida exploits Microsoft certificates to infect Teams, Zoom, PuTTY // Cybernews (https://cybernews.com/security/rhysida-malvertising-teams-zoom-putty/). 04.11.2025).***

***

«Північнокорейські зловмисники, зокрема група Kimsuky, вдосконалюють свої стратегії атак, використовуючи інструменти, орієнтовані на розробників, як вектори зараження для шпигунських операцій. Нещодавня кампанія починається з простого файлу JavaScript «Themes.js», який зв'язується з сервером управління та контролю (C2), розміщеним на легальній інфраструктурній

службі домену, яку часто не помічають системи безпеки. Цей початковий дропер ініціює багатоетапну атаку, спочатку надсилаючи ім'я хоста скомпрометованої машини для розвідки з метою виявлення цілей високої цінності…

Якщо ціль обрана, надсилається другий JavaScript-код для збору детальної інформації про систему, включаючи апаратне забезпечення, мережеві конфігурації, запущені процеси та файли користувача, які потім викачуються на сервер C2. Щоб забезпечити довгостроковий доступ, шкідливе програмне забезпечення встановлює стійкість, створюючи заплановане завдання, яке щохвилини повторно запускає дроппер за допомогою легальної утиліти Windows, що ускладнює його виявлення. Хоча на останньому етапі використовується документ Word, який виявився порожнім, це вказує на потенційне місце для майбутньої соціальної інженерії, завершуючи складний ланцюжок інфікування, призначений для прихованого та стійкого контролю…» ***(Tushar Subhra Dutta. Threat Actors May Abuse VS Code Extensions to Deploy Ransomware and Use GitHub as C2 Server // Cyber Security News (https://cybersecuritynews.com/threat-actors-may-abuse-vs-code-extensions/). 06.11.2025).***

***

«…Компанія Trend Micro повідомляє, що північнокорейські групи Kimsuky та Lazarus APT розпочали скоординовані кампанії «шпигунства та крадіжок», поєднуючи збір розвідувальної інформації методом фішингу, який використовує Kimsuky, із використанням уразливостей нульового дня та крадіжкою криптовалюти, які застосовує Lazarus…

В одній з операцій 2024 року Kimsuky заманював жертв підробленим електронним листом «Blockchain Security Symposium», встановлюючи бекдор FPSpy і кейлогер KLogEXE для відображення мереж і викрадення облікових даних. Потім Lazarus використав уразливість Windows zero-day CVE-2024-38193 через підроблені проекти Node.js, розгорнув бекдор InvisibleFerret і викрав понад 30 мільйонів доларів у криптовалюті, використовуючи Fudmodule, щоб уникнути виявлення…

Спільна інфраструктура C2 пов'язує ці групи, які перебувають під контролем Головного розвідувального управління Північної Кореї, а нещодавні фішинг-атаки на європейські енергетичні компанії свідчать про розширення кола цілей, до якого тепер входить і критична інфраструктура. Захисникам рекомендується негайно встановлювати виправлення, застосовувати перевірку електронної пошти та стежити за такими показниками, як winlogon.exe, що породжується з файлів HWP, раптовий доступ до каталогу гаманця та сліди підвищення привілеїв». ***(North Korean Hacking Groups Target Critical Sectors Worldwide with Zero-Day Exploits // Cyber Press (https://cyberpress.org/north-korean-hacking-groups/). 21.11.2025).***

***

«Індійська APT-група «Dropping Elephant» атакує оборонний сектор Пакистану за допомогою багатоетапної фішингової кампанії, яка приховує Python RAT всередині дроппера MSBuild. Фальшивий електронний лист, пов'язаний з обороною, доставляє ZIP-файл, що містить проект MSBuild і PDF-файл-приманку. Під час запуску проект розміщує компоненти в папці

\Windows\Tasks, створює заплановані завдання з назвами «KeyboardDrivers» і «MsEdgeDrivers» та завантажує повну версію Python runtime в папку \AppData. Там підроблена DLL (python2_pycache_.dll) містить маршальований байт-код Python, який виконується без головного процесу через pythonw.exe…

Модулі бекдору (клієнт, команди, remote_module, base.py) надають зловмисникам повний контроль, спілкуючись з доменами C2 nexnxky.info, upxvion.info та soptr.info. Код зашифрований за допомогою зворотного кодування рядків UTF, команд base64 та динамічного вирішення API, щоб уникнути антивірусних інструментів. Дослідник Ідан Тараб зазначає, що ця операція демонструє «значну технічну зрілість», використовуючи вбудовані утиліти Windows для приховування.

Цілі включають науково-дослідні та закупівельні об'єкти, пов'язані з Національною радіо- і телекомунікаційною корпорацією Пакистану. Захисникам рекомендується стежити за активністю MSBuild, незвичайними середовищами виконання Python у шляхах користувачів і підозрілими назвами запланованих завдань, а також посилити антифішинговий контроль…» ***(Tushar Subhra Dutta. Dropping Elephant Hacker Group Attacks Defense Sector Using Python Backdoor via MSBuild Dropper // Cyber Security News (https://cybersecuritynews.com/dropping-elephant-hacker-group-attacks-defense-sector/#google_vignette). 24.11.2025).***

***

«Дослідники з GenDigital виявили докази того, що дві відомі APT-групи, які підтримуються державою, — пов'язана з Росією Gamaredon і північнокорейська Lazarus — використовують один і той самий сервер управління (IP 144.172.112.106). Сервер, який спочатку відстежувався як частина інфраструктури Gamaredon на базі Telegram/Telegraph, через чотири дні був виявлений як хост зашифрованого корисного навантаження Lazarus «InvisibleFerret», доставленого через URL-адресу, ідентичну попереднім кампаніям Lazarus, таким як «ContagiousInterview». Хеш зразка шкідливого програмного забезпечення збігається з інструментами Lazarus…

Gamaredon зосереджується на шпигунстві проти українських організацій і пов'язаний з російською ФСБ; Lazarus викрав понад 1,7 мільярда доларів у криптовалюті і займається як шпигунством, так і фінансовими пограбуваннями. Сервер, який спочатку був помічений під час відстеження шпигунської інфраструктури Gamaredon, згодом виявився хостом шкідливого програмного забезпечення Lazarus InvisibleFerret, яке поширювалося через структуру, що відповідала попереднім кампаніям Lazarus з фінансового крадіжок. Якщо це підтвердиться, це буде перший задокументований випадок російсько-північнокорейської кіберспівпраці в реальному житті, що поєднує фокус Gamaredon на шпигунстві проти українських цілей із спеціалізацією Lazarus на експлуатації нульового дня та масштабних фінансових крадіжках. Командам безпеки настійно рекомендується посилити аналіз кореляції інфраструктури для захисту від цих скоординованих міжгалузевих загроз...» ***(Tushar Subhra Dutta. Russian and North Korean Hackers Form Alliances to Attack Organizations Worldwide // Cyber Security***

News (https://cybersecuritynews.com/russian-and-north-korean-hackers-form-alliances/#google_vignette). 25.11.2025).

***

Вірусне та інше шкідливе програмне забезпечення

«Російська кібершпигунська група Curly COMrades, яка діє з середини 2024 року і відповідає геополітичним інтересам Росії, використовувала Microsoft Hyper-V в Windows для уникнення виявлення та реагування на кінцевих точках (EDR) шляхом розгортання прихованої віртуальної машини (VM) на базі Alpine Linux для розміщення та виконання шкідливого програмного забезпечення, як виявила компанія Bitdefender у співпраці з грузинською CERT після атак на урядові та судові органи в Грузії та енергетичні компанії в Молдові… На початку липня, отримавши віддалений доступ до комп'ютерів жертв, хакери увімкнули Hyper-V, вимкнули його інтерфейс управління та створили легку віртуальну машину під назвою «WSL», яка потребувала лише 120 МБ дискового простору та 256 МБ пам'яті, щоб маскуватися під підсистему Windows для Linux. Вони налаштували її так, щоб трафік маршрутизувався через мережевий адаптер Default Switch хоста, завдяки чому зловмисні повідомлення здавалися такими, що надходять із законної IP-адреси хоста, тим самим обходячи системи EDR, які не мають функції перевірки мережі віртуальних машин. У цьому прихованому середовищі група розгорнула два спеціальні бінарні файли ELF на основі libcurl: CurlyShell, зворотний шел, який виконує команди, зберігається за допомогою завдання cron, працює без інтерфейсу і підключається до серверів управління та контролю (C2) через HTTPS; та CurlCat, супутній зворотний проксі, що викликається для тунелювання, який обгортає трафік SSH у запити HTTPS, щоб забезпечити мережеве півотування, поєднуючись із звичайним трафіком… Крім того, Curly COMrades використовували два скрипти PowerShell для забезпечення стійкості та поперечного переміщення — один для введення квитків Kerberos в LSASS для віддаленої автентифікації та виконання команд, а інший — для створення локальних облікових записів на машинах домену через групову політику, демонструючи складні тактики, такі як шифрування корисних даних та мінімальні сліди для збереження прихованості. Bitdefender рекомендує організаціям стежити за незвичайними активаціями Hyper-V, доступами до LSASS та скриптами PowerShell, розгорнутими через групову політику, які скидають паролі або створюють нові локальні облікові записи, щоб виявляти такі загрози». ***(Bill Toulas. Russian hackers abuse Hyper-V to hide malware in Linux VMs // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/russian-hackers-abuse-hyper-v-to-hide-malware-in-linux-vms/). 04.11.2025).***

***

«Компанія Microsoft викрила таємну операцію кібершпигунства, в рамках якої зловмисники перетворили API Assistants від OpenAI на

зашифрований канал команд для прихованого бекдору під назвою «SesameOp». Після проникнення в ціль і встановлення декількох веб-оболонок зловмисники використовували ін'єкцію .NET AppDomainManager, щоб захопити утиліти Visual Studio, змусивши їх завантажити шкідливу бібліотеку (Netapi64.dll). Ця DLL, у свою чергу, розмістила бекдор (OpenAIAgent.Netapi64) у папці Temp системи і зберігала його там протягом декількох місяців…

Замість того, щоб безпосередньо зв'язуватися зі звичайним сервером C&C, SesameOp отримував інструкції та надсилав результати виконання на контрольований зловмисником обліковий запис OpenAI Assistants. Під час кожної перевірки бекдор запитував векторні сховища та список помічників облікового запису: якщо векторне сховище, що відповідало зараженому хосту, не існувало, воно створювалося; після чого зловмисник просто редагував поля «опису» асистента, щоб вбудувати ключові слова завдань, такі як «Сон» або «Корисне навантаження», тоді як значення «інструкції» містило код для виконання. Після завершення корисного навантаження SesameOp відправляв результат назад на той самий канал під тегом «Результат», ефективно приховуючи живий трафік C&C всередині легітимних викликів API.

Microsoft відстежила активність, ідентифікувала несанкціонований ключ API OpenAI та спільно з OpenAI заблокувала ключ і закрила пов'язаний з ним обліковий запис. Хоча API Assistants буде виведений з експлуатації в серпні 2026 року, цей інцидент підкреслює, як сервіси генеративної штучної інтелекту можуть бути залучені до малопомітних інфраструктур C&C, і чому захисники повинні ретельно перевіряти на предмет зловживань навіть на перший погляд нешкідливий трафік хмарної штучної інтелекту…» ***(Ionut Arghire. SesameOp Malware Abuses OpenAI API // Wired Business Media (https://www.securityweek.com/sesameop-malware-abuses-openai-api/). 04.11.2025).***

***

«У листопаді 1988 року аспірант Корнельського університету Роберт Таппан Морріс випустив черв'яка Морріса (Morris), який за 24 години ненавмисно заразив приблизно 10% всього Інтернету, що на той час складався з близько 60 000 систем, спричинивши значні перебої в роботі та збитки, оцінювані від 100 000 до мільйонів доларів. Хоча ретроспективний аналіз ФБР свідчить, що це перше шкідливе програмне забезпечення було створено без злого умислу, а лише з метою оцінити розмір новоствореної мережі, його непередбачені наслідки призвели до значного уповільнення роботи систем, збою та тривалих перебоїв у роботі мережі в таких установах, як Гарвард, Принстон і NASA…

Самореплікуючийся черв'як, написаний на мові C і націлений на системи BSD UNIX, використовував вразливості в системі електронної пошти Інтернету та програмі «finger». Морріс, який анонімно випустив черв'яка через комп'ютер MIT, був пізніше ідентифікований завдяки випадковій помилці друга і підтверджений аналізом ФБР. Згодом він був звинувачений за щойно прийнятим Законом про комп'ютерне шахрайство та зловживання 1986 року. Після судового розгляду у 1989 році Морріс уникнув тюремного ув'язнення, отримавши штраф, умовний термін та 400 годин громадських робіт. На момент інциденту основою Інтернету була мережа

NSFNET, наступниця ARPANET, яка в основному з'єднувала академічні установи і передувала створенню Всесвітньої павутини та комерційного Інтернету, що з'явилися в 1990-х роках…» ***(Mark Tyson. 37 years ago this week, the Morris worm infected 10% of the Internet within 24 hours — worm slithered out and sparked a new era in cybersecurity // Future US, Inc. (https://www.tomshardware.com/tech-industry/cyber-security/on-this-day-in-1988-the-morris-worm-slithered-out-and-sparked-a-new-era-in-cybersecurity-10-percent-of-the-internet-was-infected-within-24-hours). 04.11.2025).***

***

«Після семимісячної перерви зловмисне програмне забезпечення Gootloader повернулося, використовуючи отруєння пошукової оптимізації (SEO) для просування підроблених веб-сайтів, які поширюють шкідливе програмне забезпечення, замасковане під юридичні документи та угоди. Цей завантажувач на основі JavaScript обманює користувачів, змушуючи їх завантажувати шкідливі файли, які потім надають зловмисникам початковий доступ до корпоративних мереж, що часто призводить до атак програм-вимагачів…

Нова кампанія використовує кілька складних технік, щоб уникнути виявлення. Вона використовує спеціальний веб-шрифт, який замінює літери схожими символами, приховуючи шкідливі ключові слова в вихідному коді веб-сайту від автоматизованих інструментів аналізу. Крім того, шкідливе програмне забезпечення поширюється в пошкоджених ZIP-архівах, призначених для вилучення шкідливого файлу JavaScript тільки при відкритті за допомогою Windows Explorer, при цьому виглядаючи нешкідливим для платформ аналізу безпеки…

Після зараження системи Gootloader встановлює бекдор «Supper SOCKS5», що дозволяє зловмиснику, відомому як Vanilla Tempest, отримати віддалений доступ. Було помічено, що ця група діє дуже швидко, компрометуючи критично важливі системи, такі як контролер домену, за лічені години. Оскільки Gootloader знову активний, користувачам рекомендується бути надзвичайно обережними та уникати завантаження шаблонів з невідомих веб-сайтів…» ***(Lawrence Abrams. Gootloader malware is back with new tricks after 7-month break // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/gootloader-malware-is-back-with-new-tricks-after-7-month-break/). 05.11.2025).***

***

«Дослідники в галузі безпеки виявили складну багатоетапну кампанію з розповсюдження шкідливого програмного забезпечення під назвою «ClickFix», яка повністю базується на соціальному інжинірингу з метою спонукати користувачів Windows вручну виконувати шкідливі команди. Атака починається з оманливих веб-сайтів, які часто імітують підроблені екрани Windows Update або Human Verification і пропонують жертві скопіювати та вставити команду в діалогове вікно Windows Run. Ця дія запускає ланцюжок сильно заплутаних скриптів, які в кінцевому підсумку призводять до розгортання шкідливого програмного забезпечення для викрадення інформації, такого як LummaC2 або Rhadamanthys…

Ключовою особливістю кампанії є використання стеганографії, коли кінцевий шкідливий шел-код прихований у піксельних даних, на перший погляд, нешкідливих PNG-зображень, що вимагає спеціальної процедури для розшифрування. Щоб зменшити цю загрозу, яка обходить традиційні механізми безпеки, важливе значення має обізнаність користувачів, оскільки законні оновлення системи ніколи не вимагають ручного виконання команд. Організаціям також рекомендується впровадити технічні засоби захисту, такі як відключення вікна «Виконати» в Windows і моніторинг незвичайних ланцюжків процесів, таких як mshta.exe, що запускає powershell.exe…» ***(ClickFix Attack Hides Malware in Fake Windows Security Update via Steganography // Cyber Press (https://cyberpress.org/clickfix-steganography-attack/). 25.11.2025).***

***

«Нова масова хвиля шкідливого програмного забезпечення «Shai-Hulud» заразила близько 700 пакетів npm і понад 19 000 репозиторіїв GitHub, що значно перевищує спалах вересня 2025 року, який вразив 180 репозиторіїв…

Як працює атака

• Хакери заволодівають обліковими даними адміністратора npm і публікують троянські оновлення, які виглядають як легітимні.

• Коли розробники встановлюють пакет, черв'як викрадає секретні дані CI/CD, записує їх у власні репозиторії жертви та вводить свій корисний вантаж у всі інші пакети npm, які контролює адміністратор, швидко поширюючись (≈1000 нових репозиторіїв кожні 30 хвилин, згідно з Wiz Threat Research).

• Нові функції: виконання через скрипти npm install-lifecycle та нові файли корисного навантаження (setup_bun.js, bun_environment.js). Якщо збереження не вдається, шкідливе програмне забезпечення видаляє весь домашній каталог користувача…

Серед відомих жертв — пакети, пов'язані з Zapier, Ethereum Name Service, PostHog і Postman. GitHub і npm видаляють шкідливі репозиторії, але зловмисники продовжують створювати нові. Величезний, заплутаний корисний вантаж настільки великий, що сканери коду на основі штучного інтелекту часто помилково класифікують його як нешкідливий.

Заходи з мінімізації ризиків для розробників/підприємств

• Порівняйте встановлені пакети з опублікованими списками скомпрометованих пакетів і видаліть уражені версії.

• Змініть усі облікові дані (GitHub, npm, CI/CD, хмара) на машинах, де були встановлені інфіковані пакети.

• Вимкніть скрипти npm після встановлення в конвеєрах CI, застосуйте MFA на облікових записах GitHub/npm, призупиніть автоматичні оновлення до перевірки пакетів.

• Знайдіть несанкціоновані репозиторії GitHub з назвою «Shai Hulud: The Second Coming»…

Сплеск активності відбувається безпосередньо перед 9 грудня, коли npm має скасувати «класичні» токени доступу, що свідчить про те, що зловмисники використовують уразливість адміністраторів, які не перейшли на більш безпечні та

надійні методи публікації». ***(Emma Woollacott. Shai-Hulud malware is back with a vengeance and has hit more than 19,000 GitHub repositories so far — here's what developers need to know // Future US, Inc. (https://www.itpro.com/security/cyber-attacks/shai-hulud-malware-is-back-with-a-vengeance-and-hit-more-than-19-000-github-repositories-so-far-heres-what-developers-need-to-know). 25.11.2025).***

***

Програми-вимагачі

«Атаки програм-вимагачів в Японії набувають все більшого розмаху, а ноу-хау комерціалізується як «програма-вимагач як послуга» (RaaS), що дозволило таким групам, як російська Qilin, значно збільшити частоту і серйозність вторгнень. Qilin, яка тільки в 2025 році здійснила понад 700 атак з використанням програм-вимагачів, нещодавно взяла на себе відповідальність за атаку на Asahi Group Holdings Ltd., опублікувавши в даркнеті заяви про викрадення 27 ГБ внутрішніх документів і даних співробітників, ймовірно, як тактику тиску після невдалої спроби отримати викуп. Ця атака, а також нещодавнє порушення роботи системи онлайн-ритейлера Askul Corp., підкреслюють вразливість компаній, що не належать до визначених секторів критичної інфраструктури…

Бізнес-модель RaaS, в якій розробка програм-вимагачів відокремлена від здійснення атаки, дозволяє особам без глибоких знань здійснювати складні атаки, що значно підвищує прибутковість і кількість жертв у всьому світі. Хакери все частіше застосовують подвійні, потрійні та чотирикратні тактики вимагання, включаючи погрози витоку даних, DDoS-атаки та націлювання на бізнес-партнерів, щоб змусити жертв платити, хоча експерти застерігають від оплати, оскільки це сприяє подальшому розвитку кіберзлочинності…

Японський уряд намагається посилити захист за допомогою частково прийнятого закону про активну кіберзахист (ACD), який зобов'язує операторів критичної інфраструктури повідомляти про інциденти та дозволяє нейтралізувати сервери, що здійснюють атаки. Однак урядові контрзаходи наразі є недостатніми, оскільки такі великі компанії, як Asahi та Askul, не були визначені як критична інфраструктура. Хоча новий прем'єр-міністр Санае Такаїчі висловила тверду прихильність до посилення кібербезпеки та кризового управління, необхідне більш широке охоплення, а також заходи для захисту конституційних прав та запобігання зловживанню даними, зібраними в рамках ACD». ***(Firms at risk as Japan struggles to keep up with cybercrime amid rise of ransomware // THE MAINICHI NEWSPAPERS (https://mainichi.jp/english/articles/20251031/p2a/00m/0bu/020000c). 03.11.2025).***

***

«Атаки програм-вимагачів перетворюються на складні психологічні операції, в яких зловмисники активно шукають і використовують поліси кіберстрахування компаній, щоб максимізувати свої незаконні прибутки. Отримавши деталі полісу, хакери отримують важливу стратегічну інформацію про фінансову підготовленість організації, межі покриття та бажаних постачальників

послуг з реагування на інциденти (юридичні консультанти, експерти-криміналісти), перетворюючи свої припущення на прораховані стратегії вимагання. Ці внутрішні знання дозволяють зловмисникам адаптувати вимоги щодо викупу, часто відображаючи межі покриття, та застосовувати психологічний тиск, посилаючись на потенційні штрафи за порушення конфіденційності або погрожуючи безпосередньо зв'язатися з клієнтами чи співробітниками жертви…

Щоб захистити цей цінний актив, організації повинні ставитися до своєї політики кіберстрахування з такою ж суворістю, як і до інших конфіденційних фінансових документів. Найкращі практики вимагають безпечного зберігання полісів у системах із суворим доступом на основі дозволів (наприклад, у цифрових сейфах), уникаючи спільних хмарних дисків або поштових скриньок. Доступ повинен бути суворо обмежений невеликою групою ключових зацікавлених сторін (юридичний, фінансовий, безпековий, вище керівництво). Крім того, зберігання чистої офлайн-копії (часто у зовнішнього консультанта або спеціалізованого постачальника послуг) забезпечує доступ під час збою шифрування. Нарешті, надзвичайно важливо проінформувати всі відповідні команди про захист полісів та включити роботу з полісами до навчання з питань безпеки, щоб поліси залишалися інструментом відновлення та стійкості, а не засобом для вимагання». ***(Jason Vitale. How Ransomware Attacks Leverage Cyber Insurance Policies // Techstrong Group Inc. (https://securityboulevard.com/2025/11/how-ransomware-attacks-leverage-cyber-insurance-policies/). 03.11.2025).***

***

«Останнє опитування Sophos, в якому взяли участь 361 керівник IT-безпеки роздрібних компаній з 16 країн, показує неоднозначну картину щодо програм-вимагачів: хоча роздрібні компанії все краще справляються з атаками до того, як файли будуть зашифровані — лише 48 % інцидентів зараз закінчуються шифруванням, що є найнижчим показником за останні п'ять років — ті, хто все ж втрачає дані, платять рекордні суми і за вищими цінами. Серед жертв, дані яких були зашифровані, 58 % заплатили викуп (другий за величиною показник в історії дослідження), хоча лише 29 % задовольнили всі вимоги зловмисників; 59 % домовилися про меншу суму, а 11 % в кінцевому підсумку заплатили більше. Середня сума вимог подвоїлася в порівнянні з минулим роком і становить 2 мільйони доларів США, а середні виплати зросли на 5 % до 1 мільйона доларів США…

Первинний доступ залишається слабким місцем: 46 % зломів здійснювалися з використанням невідомих прогалин у безпеці, а 30 % — з використанням відомих, не виправлених вразливостей, особливо в системах віддаленого доступу та інших пристроях, підключених до Інтернету. За останній рік Sophos відстежила близько 90 окремих груп, що займаються викраденням даних та вимаганням викупу, які націлені на роздрібну торгівлю, серед яких найактивнішими були Akira, Cl0p, Qilin, PLAY та Lynx. Ці висновки підкреслюють більш складну ситуацію з загрозами, в якій швидке виявлення та комплексна стратегія безпеки, а не виплата викупу, є ключовими факторами для уникнення тривалих перебоїв у роботі та шкоди репутації». ***(Ian Barker. More than half of retailers pay up when hit by ransomware //***

BetaNews, Inc. (https://betanews.com/2025/11/04/more-than-half-of-retailers-pay-up-when-hit-by-ransomware/). 04.11.2025).

***

«…Згідно з вичерпним звітом чиновників штату Невада, складна кібератака, яка в серпні паралізувала державні системи, була результатом тривалого вторгнення, від якого штат успішно відновився всього за 28 днів, не сплачуючи викуп. Атака, яка почалася з того, що в травні державний службовець несвідомо завантажив шкідливе програмне забезпечення, призвела до того, що зловмисник отримав віддалений контроль над державними комп'ютерами, отримав доступ до сервера сховища паролів і скомпрометував понад 26 000 файлів…

Коли 24 серпня було запущено програмне забезпечення для вимагання викупу, воно вивело з ладу важливі служби, зокрема систему запису на прийом до Департаменту транспортних засобів, систему перевірки анкетних даних штату та онлайн-додатки соціальних служб. Зловмисник вимагав викуп, але штат відмовився, впевнений у своїй здатності відновити роботу. Хоча слідчі виявили, що дані були упаковані для транспортування, не було жодних доказів того, що будь-яка конфіденційна інформація була успішно викрадена або опублікована в Інтернеті…

Швидке відновлення було забезпечено завдяки дисциплінованому плануванню, багаторічним стратегічним інвестиціям у кібербезпеку та цілодобовому реагуванню. Державні службовці працювали понад 4200 годин понаднормово, а штат витратив понад 1,3 мільйона доларів на зовнішніх постачальників, таких як компанія з кібербезпеки Mandiant. Пріоритетами під час відновлення були своєчасна обробка заробітної плати та відновлення систем, що безпосередньо впливали на суспільне благо. Після цього штат впровадив численні заходи з підвищення безпеки, хоча в звіті визнається, що кібербезпека є безперервним процесом, який вимагає постійної пильності». ***(Eric Neugeboren. Report: Nevada didn't pay ransom in statewide cyberattack, spent $1.5M on response // THE NEVADA INDEPENDENT (https://thenevadaindependent.com/article/report-nevada-didnt-pay-ransom-in-statewide-cyberattack-spent-1-5m-on-response). 05.11.2025).***

***

«Глобальне опитування 1773 керівників служб безпеки виявило значну розбіжність між впевненістю та реальністю у підготовці до атак програм-вимагачів. Хоча переважна більшість (95%) керівників впевнені у своїй здатності відновити роботу після атаки, дані показують набагато сумнішу картину: із 40% організацій, які зазнали атак протягом останнього року, лише 15% повністю відновили свої дані, а 45% заплатили викуп…

Опитування, проведене OpenText, також підкреслює зростаючу загрозу штучного інтелекту, який полегшує здійснення фішингових атак і атак з використанням програм-вимагачів. Більше половини респондентів вже помітили збільшення кількості атак завдяки ШІ, а 44% стикалися з підробками глибокої підробки. Цей ризик посилюється тим фактом, що, хоча 88% організацій дозволяють використання генеративних інструментів ШІ, менше половини з них мають офіційну політику використання.

Позитивним моментом є те, що побоювання щодо програм-вимагачів стимулюють інвестиції, причому хмарна безпека, технології резервного копіювання та навчання користувачів є головними пріоритетами на 2026 рік. Однак у звіті зазначається, що організації все ще стоять перед складним вибором: інвестувати значні кошти в забезпечення відмовостійкості або ризикувати виплатою викупу, щоб уникнути дорогого простою, без гарантії, що виплата запобіжить майбутнім атакам. Зрештою, кожна організація повинна зважити витрати на безпеку та потенційний вплив недоступності даних…» ***(Michael Vizard. Survey: Organizations Are Too Confident in Their Cyber Resiliency // Techstrong Group Inc. (https://securityboulevard.com/2025/11/survey-organizations-are-too-confident-in-their-cyber-resiliency/). 05.11.2025).***

***

«Згідно з доповіддю Veeam «Тенденції у сфері програм-вимагачів у 2024 році» (2024 Ransomware Trends Report), атаки програм-вимагачів стають все частішими, витонченішими та дорожчими. У 2024 році кількість інцидентів у світі зросла на 11 % до 5414, причому лише в останньому кварталі спостерігалося різке зростання на 32 %. Ця тенденція прискорилася в 2025 році, коли кількість інцидентів у США зросла на 149% у порівнянні з аналогічним періодом минулого року за перші п'ять тижнів. Фінансові ризики також зросли: середня сума викупу збільшилася з 400 000 доларів у 2023 році до 2 мільйонів доларів у 2024 році…

Зловмисники пішли далі простого шифрування і тепер застосовують подвійні та потрійні тактики вимагання, що включають крадіжку даних та погрози публічного викриття. Екосистема програм-вимагачів також стала більш динамічною: на початку 2025 року було виявлено 88 активних груп, у тому числі 35 нових, що ускладнює захисникам відстеження їх діяльності. Жоден сектор не є захищеним, але у 2024 році найбільшою мішенню стали медичні послуги, де кількість атак зросла на 50% порівняно з попереднім роком.

Справжня вартість атаки набагато перевищує суму викупу. В середньому втрачається 18% даних організації, а час відновлення становить 24,6 дня, що є надзвичайно тривалим. Основне фінансове навантаження пов'язане з перериванням діяльності, шкодою репутації та втратою продуктивності, а не з самим викупом…

Для боротьби з цим Veeam пропонує триетапний підхід, орієнтований на відмовостійкість. До атаки організації повинні використовувати інтелектуальне виявлення загроз і безпечні, незмінні резервні копії (відповідно до правила 3-2-1-1-0) як останній захист. Під час і після атаки важливе значення має швидке і чисте відновлення за допомогою перевірених резервних копій і скоординованого відновлення в карантинній «пісочниці» для запобігання повторному зараженню. Програма «Cyber Secure» від Veeam пропонує комплексне рішення, інтегруючись з іншими інструментами безпеки та забезпечуючи реагування на інциденти, гарантії відновлення та навчання, щоб організації були готові до атаки, коли вона відбудеться, а не якщо вона відбудеться…» ***(Ransomware Attacks Reach Record Levels: How Veeam Addresses the Most Persistent Threat to Business Continuity // metro***

Atlanta (https://roughdraftatlanta.com/2025/11/06/veeam-ransomware-trends-report/). 06.11.2025).

***

«…На офіційному ринку VS Code компанії Microsoft було виявлено шкідливе розширення під назвою susvsex, яке, судячи з усього, було створено за допомогою штучного інтелекту. Розширення, яке мало базові функції програм-вимагачів, відкрито рекламувалося як шкідливе в його описі, проте Microsoft спочатку не видалила його після того, як про це повідомили дослідники в галузі безпеки…

Після активації susvsex викрадає файли, стискаючи їх і виводячи на віддалений сервер, а потім шифрує оригінали за допомогою AES-256-CBC. Аналіз коду виявив коментарі, які вказують на те, що він був створений за допомогою штучного інтелекту, що спонукало одного з дослідників назвати його «AI slop» (штучний інтелект-неудачник). Розширення також опитує приватне сховище GitHub на наявність команд, що допомогло відстежити ймовірного автора в Азербайджані. Хоча воно і не є складним, його присутність на офіційному ринку вказує на потенційний новий вектор загрози…» ***(Bill Toulas. AI-Slop ransomware test sneaks on to VS Code marketplace // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/ai-slop-ransomware-test-sneaks-on-to-vs-code-marketplace/). 06.11.2025).***

***

«Газета Washington Post підтвердила, що стала жертвою недавньої хвилі атак програм-вимагачів Cl0p, які використовували уразливість нульового дня в Oracle E-Business Suite (EBS). Російськомовна банда розмістила назву газети, виділену яскраво-жовтим кольором, у верхній частині свого сайту в даркнеті, що є тактикою тиску, яка попереджає, що викрадені дані будуть оприлюднені, якщо не буде сплачено викуп… Широко використовувана платформа EBS від Oracle, яка управляє всім, від логістики до записів про клієнтів, була масово зламана влітку; дослідники Google відстежують початковий злом до липня, тоді як Oracle випустила неповну аварійну латку на початку жовтня і друге критичне виправлення 11 жовтня. Десятки організацій виявили злом лише в серпні, часто після того, як Cl0p надіслав електронною поштою записки з вимогою викупу. Серед відомих жертв, інформація про яких вже опублікована на сайті з витоками, є Гарвардський університет, Envoy Air, DXC Technology та Чиказькі державні школи. The Post не розкриває, які саме дані були викрадені та в якій кількості. Cl0p, відповідальний за MOVEit, GoAnywhere та інші масові хакерські атаки, які принесли сотні мільйонів доларів, продовжує використовувати публічне ганьблення та інсценовані витоки даних, щоб вимагати виплати від своїх відомих жертв». ***(Stefanie Schappert. Washington Post is latest victim of Oracle-hacking Cl0p gang // Cybernews (https://cybernews.com/security/washington-post-clop-oracle-ebs-victim-zero-day-hack/). 06.11.2025).***

***

«…У червні 2025 року дослідники з AhnLab виявили нову фінансово мотивовану операцію з використанням програм-вимагачів під назвою «Cephalus». Злочинне угруповання проникає в систему за допомогою викрадених облікових даних протоколу віддаленого робочого столу (Remote Desktop Protocol, RDP) — майже завжди там, де відсутня багатофакторна автентифікація — а потім діє за фіксованим сценарієм: закріплюється в системі, викачує конфіденційні файли і, нарешті, шифрує середовище жертви. Написаний на Go, Cephalus вимикає Windows Defender, видаляє тіньові копії та зупиняє такі служби, як Veeam і Microsoft SQL Server, перш ніж запустити дворівневу процедуру шифрування (AES-CTR для даних, RSA для ключів). Щоб заплутати аналітиків, він створює фальшивий ключ AES і маскує справжній за допомогою XOR…

Тактика тиску є настільки ж витонченою: записки з вимогою викупу містять посилання на репозиторії GoFile, де зберігаються зразки викрадених даних, що підкреслює ризик публічного розголошення інформації у разі відмови від оплати. Cephalus створює кожний бінарний файл індивідуально для своєї цілі, що свідчить про наявність внутрішньої команди або тісної співпраці з RaaS. Захисникам рекомендується ввімкнути MFA на кожному кінцевому пристрої RDP, посилити гігієну облікових даних, зберігати ізольовані резервні копії та стежити за характерними ознаками діяльності групи в рамках надійної програми виявлення кінцевих пристроїв…» ***(Abinaya. Threat Actors Leveraging RDP Credentials to Deploy Cephalus Ransomware // Cyber Security News (https://cybersecuritynews.com/cephalus-ransomware-rdp-credentials/). 08.11.2025).***

***

«З моменту атаки програм-вимагачів на лікарню Хілель Яффе в 2021 році сектор охорони здоров'я Ізраїлю залишається вкрай вразливим, а війна жовтня 2023 року перетворила кіберпростір на ще один фронт: до грудня влада зафіксувала 3380 атак — на 150% більше, ніж у попередні роки, — з яких 800 мали «значний потенціал шкоди». У звіті Microsoft про цифрову оборону за 2025 рік Ізраїль посідає третє місце у світі за кількістю атак (після США та Великої Британії) і перше місце в регіоні Близького Сходу та Африки, приймаючи на себе більше п'ятої частини регіональних атак…

Приблизно 64 відсотки хакерських атак з боку Ірану зараз спрямовані на Ізраїль з метою отримання розвідувальної інформації, дезорганізації та пропагандистських вигод. Зловмисники використовують звичні, але ефективні тактики — незахищене програмне забезпечення, слабкі або повторно використані паролі, викрадені облікові дані та базовий фішинг — для проникнення в мережі лікарень. Хоча державні актори відіграють значну роль, все ж переважною є жага до прибутку: 80 відсотків інцидентів пов'язані з крадіжкою даних, а більше половини — з використанням програм-вимагачів.

Технічний директор Claroty Амір Премінгер каже, що за останні три роки його компанія зафіксувала 136 заявлених випадків порушення безпеки критичної інфраструктури Ізраїлю, у тому числі 34 випадки проти основних служб і вісім проти лікарень. Він виділяє два типи дій, що фінансуються державою: удари з великим ефектом, покликані шокувати і потенційно поставити під загрозу пацієнтів, та

повільні кампанії з викраденням конфіденційних медичних даних. Швидке впровадження інструментів штучного інтелекту збільшує ризик, дозволяючи навіть недосвідченим зловмисникам автоматизувати складні вторгнення, тоді як медичні установи впроваджують ШІ швидше, ніж можуть його захистити…

Національне кібердиректорат Ізраїлю має сучасні можливості, але обмежені повноваження щодо впровадження стандартів у приватних лікарнях та у постачальників. Премінгер закликає до введення обов'язкових базових вимог безпеки, державної фінансової підтримки та посилення навчання та інформування, перш ніж наступне велике порушення безпеки паралізує систему охорони здоров'я країни». ***(Cyber threats spike 150% since Oct. 2023, Israeli healthcare most vulnerable // i24news (https://www.i24news.tv/en/news/israel/technology-science/artc-cyber-threats-spike-150-since-oct-2023-israeli-healthcare-most-vulnerable). 23.11.2025).***

***

«…У вересні 2025 року атака програм-вимагачів на систему обробки пасажирів MUSE компанії Collins Aerospace паралізувала роботу аеропортів Хітроу, Брюсселя та Берліна, що призвело до скасування понад 200 рейсів і збитків на мільйони доларів. Цей інцидент показує, як одна вразливість у стороннього постачальника операційних технологій може паралізувати критичну інфраструктуру в різних країнах, і підкреслює разючі відмінності в кіберрегулюванні США та Європи:

• Реакція Європи

– Згідно з Директивою ЄС NIS2 та GDPR, аеропорти та компанія Collins є «важливими організаціями», які повинні повідомляти про серйозні інциденти протягом 24/72 годин.

– Національні CSIRT у Бельгії та Німеччині проводять розслідування; ENISA збирає анонімні дані, але не оприлюднює результати.

– Широка сфера застосування NIS2 означає, що американський постачальник підпадає під регулювання, якщо його програмне забезпечення є основою критично важливих послуг ЄС…

• Реакція Великої Британії

– Після виходу з ЄС Велика Британія планує прийняти закон про кібербезпеку та стійкість, який дозволить регуляторним органам класифікувати постачальників з високим рівнем впливу як «визначених критичних», накладаючи на них прямі обов'язки, подібні до NIS2.

• Реакція США

– Нагляд є фрагментарним. RTX (материнська компанія Collins) повинна була лише подати форму 8-K до Комісії з цінних паперів і бірж (SEC), в якій зазначалося, що це не має істотного впливу на США.

– Закон CISA про обов'язкове повідомлення (CIRCIA) все ще перебуває на стадії розробки, тому повідомлення залишаються переважно добровільними, якщо не постраждали активи США.

– Правила сектору (TSA для авіації, SEC для інвесторів) створюють мозаїку замість єдиної федеральної системи…

Ключові висновки

• Атаки на ланцюги постачання в операційних технологіях завдають операційних збитків у режимі реального часу; ручні резервні варіанти «ручка і папір» виявляють серйозні прогалини в стійкості.

• ЄС і Великобританія рухаються в напрямку прямого регулювання критично важливих постачальників; США все ще покладаються на розкриття інформації та галузеві правила.

• Розбіжні режими ускладнюють транскордонне вирішення інцидентів і підкреслюють необхідність гармонізованих стандартів, оскільки зловмисники використовують найслабші ланки в глобальній інфраструктурі». ***(Rodrigo Pérez-Alonso. Lessons From the European Airports Ransomware Attack // The Lawfare Institute (https://www.lawfaremedia.org/article/lessons-from-the-european-airports-ransomware-attack). 21.11.2025).***

***

Віруси-трояни

«Дослідники виявили прихований троян для віддаленого доступу під назвою «SleepyDuck», який видавав себе за плагін Solidity на ринку розширень Open VSX. Опубліковане 31 жовтня 2025 року як juan-bianco.solidity-vlang (v0.0.7), розширення виглядало нешкідливим до оновлення 1 листопада (v0.0.8), до того часу воно вже було завантажене близько 14 000 разів розробниками, які використовують Cursor, Windsurf та інші редактори, сумісні з VS Code. Після встановлення SleepyDuck активується щоразу, коли відкривається нове вікно редактора або завантажується файл .sol, збирає основні ідентифікатори машини та встановлює 30-секундний цикл опитування зі своїм доменом C2 sleepyduck[.]xyz…

Визначною особливістю цього шкідливого програмного забезпечення є рівень стійкості, побудований на блокчейні Ethereum. Якщо основний C2 виходить з ладу, SleepyDuck запитує контракт 0xDAfb81732db454DA238e9cFC9A9Fe5fb8e34c465, щоб отримати нові адреси серверів, інтервали опитування та резервні команди, надаючи зловмисникам динамічний канал управління, захищений від виведення з ладу. Код досягає стійкості за допомогою перевірки файлу блокування та оманливої процедури webpack.init(), яка запускає пісочницю JavaScript (vm.createContext) для виконання команд.

Оскільки розширення маскується під допомогу в розробці Solidity, кампанія ставить під загрозу саме інженерів, що працюють з блокчейном і смарт-контрактами, надаючи операторам повний і постійний віддалений контроль над зараженими комп'ютерами з Windows, при цьому залишаючись важким для знищення завдяки децентралізованій інфраструктурі на базі Ethereum…» ***(Tushar Subhra Dutta. New 'SleepyDuck' Malware in Open VSX Marketplace Allow Attackers to Control Windows Systems Remotely // Cyber Security News (https://cybersecuritynews.com/new-sleepyduck-malware-in-open-vsx-marketplace/). 04.11.2025).***

***

«…Шпигунське програмне забезпечення — це шкідливе програмне забезпечення, яке ховається на смартфоні, часто маскуючись під легальний додаток або надходить через фішингове посилання, і непомітно викачує дані, відстежує місцезнаходження, записує дзвінки, захоплює камери, робить знімки екрана тощо. Воно охоплює широкий спектр: (1) небажане програмне забезпечення, яке просто бомбардує користувачів спливаючими вікнами та збирає дані про звички перегляду веб-сторінок для рекламних мереж; (2) загальне мобільне шпигунське програмне забезпечення, яке поширюється в рамках широких фішингових кампаній з метою викрадення даних ОС, облікових даних або криптовалютних гаманців; (3) просунуте шпигунське програмне забезпечення або stalkerware, яке зазвичай пов'язане з домашнім насильством і відстежує дзвінки, повідомлення, GPS, активність у соціальних мережах і навіть навколишні звуки; та (4) пакети національного рівня, такі як Pegasus, що продаються урядам для цільового спостереження…

Ранні ознаки спроби зараження включають дивні електронні листи, SMS-повідомлення або повідомлення в соціальних мережах, які закликають вас натиснути на посилання або завантажити вкладення. Після встановлення шпигунське програмне забезпечення може видати себе через швидке розряджання батареї, незрозуміле використання даних, перегрів, випадкові перезавантаження, загадкові фонові шуми під час дзвінків, платні SMS-повідомлення або нові програми та налаштування, які ви не впізнаєте. На Android наявність опції «інсталювати з невідомих джерел» або незнайомих додатків з підвищеними правами доступу може бути підказкою; iPhone важче зламати, але застарілі версії iOS або експлойти нульового дня все ще становлять ризик, а складні імпланти можуть не залишати видимих слідів…

Видалення починається з надійного мобільного антивірусного сканування, видалення підозрілих додатків, скасування прав адміністратора та застосування оновлень ОС; у складних випадках може знадобитися видалення в безпечному режимі або повне відновлення заводських налаштувань, а в екстремальних ситуаціях (наприклад, якщо стеження пов'язане з особистою безпекою) необхідно звернутися до поліції. Після очищення змініть усі паролі, увімкніть біометричні дані та багатофакторну автентифікацію (MFA) і розгляньте можливість створення нового облікового запису електронної пошти. Профілактичні заходи включають фізичну безпеку пристроїв, своєчасну інсталяцію оновлень, відмову від сторонніх додатків, перегляд дозволів, запуск антивірусних сканувань, уникнення джейлбрейку, стеження за фішинговими посиланнями та щоденне перезавантаження для знешкодження нестійкого високотехнологічного шпигунського програмного забезпечення. Хоча жоден мобільний телефон не є повністю захищеним, пильність, своєчасні оновлення та сувора гігієна додатків значно зменшують ймовірність стати жертвою шпигунського програмного забезпечення…» ***(Charlie Osborne. Is spyware hiding on your phone? How to find and remove it – fast // A Ziff Davis company***

(https://www.zdnet.com/article/is-spyware-hiding-on-your-phone-how-to-find-and-remove-it-fast/). 04.11.2025).

***

Фішингові атаки

«У липні 2025 року група хакерів під назвою «Cavalry Werewolf» провела високотехнологічну фішингову атаку на російські урядові установи, отримавши доступ до ключових мереж і використовуючи для цього кілька спеціальних та відкритих інструментів… Операція розпочалася з електронних листів, що містили захищені паролем архіви, які видавалися за офіційні документи; після відкриття вони запускали BackDoor.ShellNET.1, зворотний шел, створений на основі відкритого коду Reverse-Shell-CS. Використовуючи утиліту Windows Bitsadmin (тактика «життя за рахунок місцевих ресурсів»), зловмисники потім завантажували додаткові корисні навантаження, включаючи Trojan.FileSpyNET.5 для крадіжки файлів Word, Excel, PDF та зображень, а також BackDoor.Tunnel.41 (похідний від ReverseSocks5) для створення прихованих тунелів SOCKS5.

Цей багатоступеневий ланцюжок — зворотні оболонки, трояни для крадіжки даних, техніки введення процесів та зашифрована інфраструктура C2 з декількома серверами — надав зловмисникам стійкий, малопомітний контроль та свободу додавати нове шкідливе програмне забезпечення відповідно до результатів розвідки. За даними аналітиків Dr.Web, ця кампанія відрізняється значним підвищенням рівня складності: Cavalry Werewolf поєднує легальні системні утиліти з модифікованим відкритим кодом, завдяки чому їхня діяльність виглядає рутинною в журналах, а також забезпечує кілька запасних точок доступу на випадок виявлення одного з бекдорів…» ***(Tushar Subhra Dutta. Cavalry Werewolf Attacking Government Organizations to Deploy Backdoor for Network Access // Cyber Security News (https://cybersecuritynews.com/cavalry-werewolf-attacking-government-organizations/). 07.11.2025).***

***

«Нова фішинг-кампанія використовує типографічні помилки, замінюючи букву «m» в microsoft.com на «r n» і створюючи домен rnicrosoft.com, який на перший погляд виглядає легітимним, оскільки сучасні шрифти роблять «rn» майже не відрізними від «m». Зловмисники копіюють логотип, макет і стиль Microsoft, спонукаючи користувачів натискати на посилання або завантажувати шкідливі файли, щоб зібрати облікові дані, здійснити шахрайство з рахунками-фактурами або провести афери в стилі HR. Ризик є більшим на мобільних пристроях, де маленькі екрани та скорочені URL-адреси приховують заміну, а також на екранах настільних комп'ютерів, де мозок читачів автоматично виправляє візуальну аномалію. Схожі трюки включають заміну літери «o» на нуль або вставку дефісів…

Захист залежить більше від пильності користувачів, ніж від автоматичних фільтрів: завжди розгортайте повну адресу відправника, наведіть курсор (або натисніть і утримуйте на мобільному пристрої) на посилання, щоб побачити

справжнє місце призначення, перевіряйте заголовки «Відповісти», ігноруйте вбудовані посилання в несподіваних повідомленнях про зміну пароля — замість цього перейдіть на офіційний веб-сайт, ввівши його URL-адресу вручну в новій вкладці. Організації повинні навчати співробітників виявляти такі схожі домени та не натискати мимоволі на знайомі повідомлення». ***(Guru Baran. Hackers Replace 'm' with 'rn' in Microsoft(.)com to Steal Users' Login Credentials // Cyber Security News (https://cybersecuritynews.com/microsoft-phishing-replace-m-with-rn/). 24.11.2025).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Федеральні прокурори звинуватили трьох американських фахівців з кібербезпеки — Райана Кліффорда Голдберга, Кевіна Тайлера Мартіна та неназваного співучасника — у зраді своїх обов'язків щодо допомоги компаніям у боротьбі з програмним забезпеченням-вимагачем, замість чого вони з травня 2023 року розпочали власні атаки з використанням програмного забезпечення-вимагача ALPHV/BlackCat проти п'яти американських підприємств, причому, згідно з обвинувальним актом, поданим до окружного суду США Південного округу Флориди та вперше опублікованим газетою Chicago Sun-Times, змова тривала до квітня 2025 року… На той час Голдберг працював менеджером з реагування на інциденти в компанії Sygnia, а Мартін і неназваний спільник працювали перемовниками з питань викупу в компанії DigitalMint, де останній, як повідомляється, відкрив партнерський рахунок в ALPHV, відомій групі, що надає послуги з вимагання викупу, яка з'явилася наприкінці 2021 року і націлилася на критичну інфраструктуру, включаючи масштабну атаку 2023 року на дочірню компанію UnitedHealth Group Change Healthcare, в результаті якої були скомпрометовані дані 190 мільйонів людей і отримано викуп у розмірі 22 мільйони доларів. Тріо нібито діяло протягом шести місяців у 2023 році, завдавши шкоди медичній компанії з Флориди, яка заплатила їм майже 1,3 мільйона доларів, а також фармацевтичній фірмі з Меріленду, лікарській практиці з Каліфорнії, інженерній компанії з Каліфорнії та виробнику дронів з Вірджинії, хоча подальших викупів не було отримано. Sygnia підтвердила негайне звільнення Голдберга після виявлення його причетності, а DigitalMint заявила, що дії відбувалися поза її системами без порушення безпеки даних клієнтів, зазначивши, що жодна з причетних осіб не працювала там більше чотирьох місяців, і відмовившись надати детальну інформацію про те, коли і як вона дізналася про цю схему. 2 жовтня Мартін був звинувачений у змові з метою втручання в комерційну діяльність шляхом вимагання, втручанні в комерційну діяльність шляхом вимагання та навмисному пошкодженні захищеного комп'ютера — кожне з яких карається максимальним тюремним ув'язненням на 50 років. 14 жовтня Мартін був заарештований, звільнений під заставу в розмірі 400 000 доларів після того, як не визнав себе винним, і позбавлений права працювати в сфері кібербезпеки до закінчення судового розгляду. Голдберг, заарештований 22 вересня і утримуваний під вартою через ризик втечі після того, як

у червні втік до Європи одностороннім рейсом, а пізніше намагався дістатися до Мексики, нібито зізнався агентам ФБР 17 червня, що його завербував неназваний співучасник змови, щоб «спробувати вимагати викуп у деяких компаній» для уникнення боргів, визнавши, що отримав 200 000 доларів від платежу медичної компанії, а влада вилучила його пристрої під час допиту…» ***(Matt Kapko. Prosecutors allege incident response pros used ALPHV/BlackCat to commit string of ransomware attacks // Scoop News Group (https://cyberscoop.com/incident-response-ransomware-professionals-charged-attacks/). 03.11.2025).***

***

«Управління з контролю за іноземними активами (OFAC) Міністерства фінансів США наклало санкції на вісім осіб та дві організації за їхню вирішальну роль у відмиванні коштів, які фінансують програми озброєння Корейської Народно-Демократичної Республіки (КНДР) і були отримані переважно за допомогою складних кіберзлочинів та шахрайських схем, пов'язаних з працівниками IT-галузі. Заступник міністра фінансів Джон К. Херлі заявив, що ці дії безпосередньо загрожують безпеці США та світовій безпеці, оскільки забезпечують незаконні доходи для програм Пхеньяна з розробки зброї масового знищення (WMD)…

Хакерські угруповання, що фінансуються державою КНДР, відповідальні за крадіжку понад 3 мільярдів доларів за останні три роки, переважно у вигляді криптовалюти, використовуючи сучасне шкідливе програмне забезпечення та соціальну інженерію. Одночасно, сотні мільйонів доларів щорічно заробляють IT-працівники КНДР, які працюють по всьому світу, приховуючи свою особу за допомогою підроблених або викрадених документів, щоб отримати роботу та контракти на фріланс. Вони часто залучають до співпраці програмістів-фрілансерів, які не є громадянами КНДР, розділяючи між собою доходи від замовлених проектів…

Серед нових санкцій – банкіри Чан Кук Чол і Хо Чон Сон, які управляли понад 5,3 мільйонами доларів у криптовалюті для визначеного OFAC банку First Credit Bank, частина з яких пов'язана з північнокорейським хакером-вимагачем. OFAC також внесло до списку північнокорейську IT-компанію Korea Mangyongdae Computer Technology Company (KMCTC) та її президента У Йон Су за організацію делегацій IT-працівників та використання громадян Китаю як банківських посередників для приховування походження коштів…

Крім того, дві фінансові установи, що базуються в Північній Кореї, – Ryujong Credit Bank та її міжнародні представники, що діють у Китаї та Росії (включно з Хо Йон Чолем, Хан Хон Гілем, Чон Сон Хьоком, Чо Чун Помом та Рі Чін Хьоком), – були піддані санкціям за сприяння відмиванню грошей, переказуванню іноземної валюти та ухиленню від санкцій з метою підтримки програм КНДР у сфері зброї масового знищення». ***(US Sanctions North Korea Bankers And Institutions Involved In Laundering Cybercrime Proceeds And IT Worker Funds // Eurasia Review (https://www.eurasiareview.com/05112025-us-sanctions-north-korea-bankers-and-institutions-involved-in-laundering-cybercrime-proceeds-and-it-worker-funds/). 05.11.2025).***

***

«Пітер Вільямс, колишній генеральний директор Trenchant (підрозділу оборонного підрядника L3Harris, що спеціалізується на засобах спостереження та хакерських інструментах), визнав себе винним у крадіжці надзвичайно цінних запатентованих експлойтів та їх продажу російському брокеру за 1,3 мільйона доларів у криптовалюті в період з 2022 по липень 2025 року. Вільямс, який мав доступ «суперкористувача» завдяки своїй керівній посаді та тривалому стажу роботи, викрав вісім експлойтів — деякі з них оцінювалися в 35 мільйонів доларів — із захищених мереж Trenchant із багатофакторною автентифікацією в Сіднеї та Вашингтоні, використовуючи портативний зовнішній жорсткий диск, а потім передав їх через зашифровані канали брокеру (ймовірно, Operation Zero)…

Вільямс, відомий всередині компанії як «Doogie» і раніше працював в Австралійському управлінні зв'язку, скористався своїм необмеженим доступом, який практично не контролювався. Крадіжка була виявлена наприкінці 2024 року, коли компанія Trenchant отримала повідомлення про витік інформації про один зі своїх продуктів. За іронією долі, Вільямс був призначений відповідальним за внутрішнє розслідування, яке він використав, щоб виключити можливість злом мережі. Він також нібито намагався підставити колишнього розробника, звинувативши його в крадіжці нульових днів, до яких він не мав доступу, незадовго до того, як особистий iPhone цього розробника став мішенню для найманого шпигунського програмного забезпечення. Вільямс зізнався ФБР у серпні після того, як йому були пред'явлені докази. Ця справа викликала шок у спільноті кібербезпеки, яка розглядає дії Вільямса як глибоку зраду західного апарату національної безпеки, що безпосередньо ставить під загрозу можливості головного супротивника, Росії…» ***(Lorenzo Franceschi-Bicchierai. How an ex-L3Harris Trenchant boss stole and sold cyber exploits to Russia // TechCrunch Media LLC (https://techcrunch.com/2025/11/03/how-an-ex-l3-harris-trenchant-boss-stole-and-sold-cyber-exploits-to-russia/). 03.11.2025).***

***

«Австралія ввела нові фінансові та туристичні санкції проти чотирьох організацій та однієї особи, пов'язаних з кіберзлочинним апаратом Північної Кореї, з метою перекрити джерела доходів, які фінансують програми Пхеньяна з розробки балістичних ракет та зброї масового знищення. Міністр закордонних справ Пенні Вонг заявила, що ці заходи є відповіддю на «глибоко тривожні» дії — крадіжки криптовалюти, шахрайство в сфері IT та кібершпигунство — які, як показала моніторингова група ООН, здійснюються північнокорейськими організаціями, що перебувають під санкціями ООН… Тільки в 2024 році хакери з КНДР викрали криптовалюту на суму близько 1,9 млрд доларів США, відмиваючи доходи через мережу північнокорейських громадян та іноземних посередників і навіть обмінюючи цифрові монети на сировину, таку як мідь. Дії Канберри, скоординовані зі Сполученими Штатами, посилюють глобальний тиск на Пхеньян, блокуючи його доступ до фінансів і технологій, а також попереджаючи австралійських громадян і підприємства, що будь-які операції з організаціями,

включеними до чорного списку, можуть спричинити суворі юридичні санкції. Цей крок відповідає більш широким міжнародним зусиллям, очолюваним Міністерством фінансів США та іншими організаціями, спрямованим на ліквідацію кібермереж фінансування Північної Кореї та змушення режиму дотримуватися резолюцій Ради Безпеки ООН і ліквідувати свої незаконні програми озброєння…» ***(Ishika Kumari. Australia strikes at North Korea's cyber crime empire with new sanctions // AMBCrypto (https://ambcrypto.com/explaining-the-zk-price-trend-this-week-and-what-traders-can-expect-next/). 07.11.2025).***

***

«Двоє британських підлітків не визнали себе винними у звинуваченнях, пов'язаних із «складним» кібератакою на Transport for London (TfL) у серпні 2024 року — вторгненням, яке слідчі пов'язують із злочинним угрупованням «Scattered Spider». 19-річний Талха Джубайр зі східного Лондона та 18-річний Оуен Флауерс з Уолсолла були заарештовані у вересні 2024 року після спільної операції Національного агентства з боротьби зі злочинністю та поліції Лондона…

Прокурори стверджують, що в період з 29 серпня по 6 вересня ця пара змовилася з метою здійснення несанкціонованих дій проти комп'ютерних систем TfL, отримавши доступ до імен та контактних даних клієнтів і завдавши — або ризикнувши завдати — серйозної шкоди благополуччю людей; це порушення коштувало TfL мільйони і змусило вимкнути камери спостереження за дорожнім рухом, систему бронювання Dial-a-Ride та деякі системи обробки платежів, хоча це не зупинило роботу транспортних служб. Флауерс також звинувачується у вторгненні в системи американських медичних установ SSM Health і Sutter Health, а Джубайр звинувачується у відмові передати паролі до пристроїв, вилучених у березні 2025 року. Попереднє слухання призначено на 13 лютого 2026 року, а попередня дата судового розгляду — 8 червня 2026 року в Королівському суді Саутварка…» ***(Adele Robinson. Teenagers plead not guilty to London transport cyber attack // Sky UK (https://news.sky.com/story/teenagers-plead-not-guilty-to-london-transport-cyber-attack-13473518). 21.11.2025).***

***

Технічні аспекти кібербезпеки

Виявлені вразливості технічних засобів та програмного забезпечення

«…Уряд США видав попередження про те, що вразливість ядра Linux високого рівня небезпеки, відома як CVE-2024-1086, наразі активно використовується в атаках програм-вимагачів, незважаючи на те, що вона була виправлена понад рік тому. Вразливість, введена в ядро Linux у лютому 2014 року, є «слабкістю використання після звільнення» в компоненті netfilter: nf_tables, має рівень серйозності 7,8/10 і дозволяє зловмисникам досягти локального підвищення

привілеїв. Дослідники в галузі безпеки продемонстрували експлойт «доказ концепції» на початку цього року, підтвердивши, що він впливає на основні дистрибутиви Linux, включаючи Debian, Ubuntu та Red Hat. Агентство з кібербезпеки та безпеки інфраструктури США (CISA) додало цю помилку до свого каталогу відомих вразливостей (KEV) у травні 2024 року і нещодавно оновило запис, щоб підтвердити її активне використання в кампаніях з використанням програм-вимагачів. CISA закликає організації негайно виправити свої дистрибутиви Linux або, якщо виправлення неможливе, застосувати заходи для зменшення ризику, такі як блокування nf_tables або обмеження доступу до просторів імен користувачів, оскільки ці вразливості становлять значну загрозу для підприємств…» ***(Sead Fadilpašić. US government warns Linux flaw is now being exploited for ransomware attacks // Future US, Inc. (https://www.techradar.com/pro/security/us-government-warns-linux-flaw-is-now-being-exploited-for-ransomware-attacks). 03.11.2025).***

***

«Провідна австралійська агенція з кібербезпеки, підрозділ Центру кібербезпеки Австралійського управління зв'язку (ASD), випустила попередження про те, що понад 150 австралійських маршрутизаторів і комутаторів Cisco залишаються зараженими критичним веб-шелом BADCANDY, незважаючи на те, що патчі для усунення вразливості (CVE-2023-20198) доступні вже понад два роки. Імплант BADCANDY, вперше виявлений Cisco Talos у жовтні 2023 року, використовує вразливість максимального рівня (10,0/10) у пристроях Cisco IOS XE, що дозволяє неавторизованим зловмисникам створювати облікові записи адміністраторів, віддалено виконувати команди та повністю компрометувати пристрої…

Агентство зазначило, що вразливість BADCANDY активно експлуатується і відбувається повторне зараження, що свідчить про те, що зловмисники можуть виявити, коли імплант видалено. Ця веб-оболонка на базі Lua з низькою капіталізацією виявилася привабливою як для злочинних угруповань, так і для державних суб'єктів, включаючи китайську організацію Salt Typhoon, яка використовує її для глобального шпигунства, перехоплюючи мережевий трафік і досягаючи стійкості. ASD настійно рекомендує організаціям негайно застосувати виправлення, обмежити доступ до веб-інтерфейсу користувача та перевірити конфігурації, що працюють, на наявність підозрілих облікових записів з привілеями 15, щоб запобігти початковому компрометації та повторному використанню…» ***(Juha Saarinen. Scores of Australian Cisco devices remain BADCANDY infected // nextmedia Pty Ltd. (https://www.itnews.com.au/news/scores-of-australian-cisco-devices-remain-badcandy-infected-621482). 04.11.2025).***

***

«Дослідники в галузі кібербезпеки та служби моніторингу брандмауерів виявили різке і тривожне зростання активності розвідки, спрямованої на інфраструктуру Windows Server Update Services (WSUS) через TCP-порти 8530 і 8531. Ця скануюча активність безпосередньо пов'язана з CVE-2025-59287,

критичною вразливістю серверів WSUS, яка дозволяє віддалено виконувати код без вимог аутентифікації…

Сплеск, виявлений за допомогою мережевих датчиків таких організацій, як Shadowserver, свідчить про активні спроби експлуатації, що використовують той факт, що достатньо технічних деталей було оприлюднено, що знижує бар'єр для вторгнення зловмисників. Зловмисники зазвичай використовують двоступеневу схему атаки: спочатку проводиться розвідка за допомогою сканування портів, а потім здійснюється експлуатація, під час якої розгортаються шкідливі скрипти для отримання широкого контролю над скомпрометованими серверами.

Вразливість має максимальний рівень серйозності 9,8, що спонукає експертів рекомендувати вважати будь-який публічно доступний сервер WSUS, що відповідає профілю вразливості, скомпрометованим. Організації повинні негайно провести аудит периметра своєї мережі, а в разі виявлення вразливих екземплярів — вжити заходів з їхньої екстреної ізоляції та провести криміналістичне розслідування. Якщо негайне виправлення недоступне, необхідно впровадити сегментацію мережі, щоб обмежити доступ сервера WSUS лише до авторизованих внутрішніх мереж, а системи розширеного виявлення загроз повинні контролювати підозрілі вихідні з'єднання, що походять від процесів WSUS…» ***(Hackers Actively Scanning for TCP Port 8530/8531 Linked to WSUS Vulnerability CVE-2025-59287 // Cyber Security News (https://cybersecuritynews.com/hackers-tcp-port-wsus-vulnerability/). 04.11.2025).***

***

«Компанія NVIDIA випустила патч для усунення вразливості високого рівня небезпеки, відстежуваної як CVE-2025-23358, у своєму додатку для Windows, яка могла б дозволити місцевим зловмисникам виконувати довільний код і отримати підвищені системні привілеї. Ця вразливість, яка має оцінку CVSS 8,2, знаходиться в компоненті інсталятора програми і викликана неконтрольованим елементом шляху пошуку… Зловмисник з низьким рівнем локального доступу може скористатися цим, маніпулюючи шляхом пошуку для введення шкідливого коду, який потім буде виконаний з підвищеними правами під час процесу інсталяції. Хоча для активації уразливості необхідна взаємодія користувача, її низька складність робить її значним ризиком, особливо в багатокористувацьких корпоративних середовищах. NVIDIA закликає всіх користувачів, які використовують версії до 11.0.5.260, негайно оновити програмне забезпечення до останньої версії, щоб зменшити загрозу…» ***(Abinaya. NVIDIA NVApp for Windows Vulnerability Let Attackers Execute Malicious Code // Cyber Security News (https://cybersecuritynews.com/nvidia-nvapp-windows-vulnerability/). 07.11.2025).***

***

«Дослідники Unit 42 виявили «Landfall» — цілеспрямовану шпигунську кампанію, яка використовувала вразливість нульового дня (CVE-2025-21042) у бібліотеці обробки зображень Samsung для Android. Landfall діяла з липня 2024 року до квітня 2025 року, коли Samsung випустила патч. Вона поширювалася у вигляді підроблених файлів зображень DNG, які часто надсилалися через

месенджери, такі як WhatsApp. Оскільки експлойт спрацьовував одразу після того, як система відображала зображення, взаємодія з користувачем не була потрібна (атака «zero-click»)…

Після обробки прихований ZIP-архів зображення викладав бібліотеки спільних об'єктів, які змінювали політики SELinux, надаючи шкідливому програмному забезпеченню глибокі системні привілеї. Потім Landfall зв'язувався з сервером управління та контролю і дозволяв операторам збирати контакти, файли, історію переглядів, ідентифікатори пристроїв та активувати мікрофон/камеру. Шпигунське програмне забезпечення посилалося на моделі Galaxy S22, S23, S24, Z Flip 4 та Z Fold 4 і спостерігалося переважно в Іраку, Ірані, Туреччині та Марокко, що свідчить про мотив спостереження.

Хоча стиль кодування нагадує комерційне програмне забезпечення для стеження від таких компаній, як NSO Group і Variston, його походження залишається невідомим. Тепер, коли технічні деталі стали публічними, незахищені пристрої Samsung з ОС Android 13–15 можуть бути схильні до ризику атак з використанням копій цього шкідливого програмного забезпечення. Користувачам слід переконатися, що вони встановили оновлення безпеки від квітня 2025 року або пізнішу версію, а тим, хто вже заразився, може знадобитися професійна допомога через глибоке вкорінення шкідливого програмного забезпечення в системі…» ***(Ryan Whitwam. Commercial spyware "Landfall" ran rampant on Samsung phones for almost a year // Condé Nast (https://arstechnica.com/gadgets/2025/11/commercial-spyware-landfall-ran-rampant-on-samsung-phones-for-almost-a-year/). 07.11.2025).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«VIGILTECH (Чехія) запустила платформу безпеки нового покоління, розроблену для того, щоб зробити кібербезпеку корпоративного рівня доступною та недорогою для малих і середніх підприємств, підприємців та споживачів. Платформа пропонує уніфіковане рішення для захисту осіб, їхніх пристроїв та даних як вдома, так і в дорозі. Її основні функції включають вдосконалену систему розширеного виявлення та реагування (XDR), яка використовує поведінковий аналіз та машинне навчання для виявлення та блокування як відомих, так і нових загроз у режимі реального часу. Платформа також забезпечує захист від сучасних загроз, таких як програми-вимагачі та атаки «нульового дня», за допомогою хмарного пісочниці, а також повного шифрування диска для Windows і macOS, що допомагає відповідати стандартам відповідності, таким як GDPR і NIS2…

Усі функції безпеки управляються через єдину централізовану консоль для максимальної простоти та контролю, доступну в хмарних або локальних розгортаннях. Ключовою відмінністю є опціональний цілодобовий моніторинг Центру безпеки (SOC), що надає користувачам експертний аналіз загроз та реагування без необхідності створення внутрішньої команди. Також доступна

опціональна послуга безпечного хмарного зберігання даних. Загальна мета полягає в забезпеченні проактивної, професійної безпеки, яка є одночасно потужною та простою в управлінні». ***(VIGIL TECH Launches Intelligent Cyber Defense Designed for a Rapidly Evolving Threat Landscape // MarketersMEDIA Newswire (https://news.marketersmedia.com/vigil-tech-launches-intelligent-cyber-defense-designed-for-a-rapidly-evolving-threat-landscape/89176681). 22.11.2025).***

***

«Німеччина створить частково автоматизовану систему «Cyber Dome» для більш швидкого виявлення, аналізу та протидії кібератакам, оголосив у Берліні міністр внутрішніх справ Олександр Добріндт. Описуючи цифрову безпеку як життєво важливу для національного суверенітету, він зазначив, що система об'єднає державні органи, підприємства та суспільство в спільних захисних зусиллях. Берлін також планує підписати угоду про співпрацю в галузі кібербезпеки з Ізраїлем та розширити юридичні повноваження німецьких органів влади, щоб вони могли «знищувати, атакувати, порушувати роботу та руйнувати» ворожу цифрову інфраструктуру, навіть якщо вона знаходиться за кордоном — така можливість відсутня в чинному законодавстві…

Клаудія Платтнер, глава федерального агентства з кібербезпеки BSI, попередила, що програми-вимагачі залишаються найбільш шкідливою кіберзагрозою для Німеччини, а шпигунство, що фінансується державою, та політично мотивовані атаки, особливо з боку Росії, Китаю, Ірану та Північної Кореї, набувають все більшого поширення. Незважаючи на нещодавні покращення, мережі німецького уряду, підприємства та критична інфраструктура продовжують залишатися одними з головних цілей у світі». ***(Germany plans 'Cyber Dome' to counter digital threats, interior minister says // Anadolu Ajansı (https://www.aa.com.tr/en/europe/germany-plans-cyber-dome-to-counter-digital-threats-interior-minister-says/3740830). 11.11.2025).***

***

Основи кібергігієни

«…Коаліція з 86 лідерів у галузі кібербезпеки, серед яких колишній директор CISA Джен Істерлі, колишній директор з інформаційної безпеки Yahoo Боб Лорд та керівники з безпеки Microsoft, Google та Uber, запустила сайт Hacklore.org, щоб розвінчати застарілі «хакерські міфи»: народні поради з безпеки, які лякають користувачів, але мало допомагають запобігти реальним порушенням…

Міфи, які вони хочуть розвіяти:

• Уникайте публічних мереж Wi-Fi.

• Ніколи не скануйте QR-коди.

• Відмовляйтеся від публічних USB-зарядних пристроїв (атаки типу «juice-jacking» залишаються суто теоретичними).

• Вимикайте Bluetooth/NFC (бездротові атаки на звичайних користувачів трапляються вкрай рідко).

• Видаляйте файли cookie для безпеки.

• Регулярно змінюйте паролі…

Такі поради, на їхню думку, відволікають увагу від перевірених засобів захисту:

• Своєчасно встановлюйте оновлення та підтримуйте програмне забезпечення в актуальному стані.

• Використовуйте надійні, унікальні паролі або, ще краще, ключі доступу.

• Увімкніть багатофакторну автентифікацію, стійку до фішингу.

• Розробляйте системи, які залишаються безпечними, навіть коли люди припускаються помилок, і дозволяють легко повідомляти про підозрілу діяльність, не звинувачуючи співробітників…

Вони також закликають постачальників програмного забезпечення застосовувати практики «безпечного проектування», публікувати дорожні карти безпеки, використовувати сучасне шифрування, запускати програми винагороди за виявлення помилок та розкривати вразливості за допомогою точних CVE.

Запущений напередодні святкового сезону, коли зазвичай знову з'являються сумнівні поради, Hacklore має на меті скерувати споживачів та організації до заходів, які дійсно зменшують кіберризики». ***(Jessica Lyons. Ex-CISA officials, CISOs dispel 'hacklore,' spread cybersecurity truths // The Register (https://www.theregister.com/2025/11/24/hacklore_launch/). 24.11.2025).***

***

«…Сім ознак того, що ваша система кібербезпеки потребує реорганізації…

1. Відсутність динамічного моніторингу

• Якщо план не переглядався або не оновлювався протягом двох і більше місяців, або не враховувалися фактори штучного інтелекту, ви рухаєтеся наосліп.

• Сучасна структура потребує сенсорних технологій та людей, які можуть виявляти зміни та вносити виправлення в режимі реального часу…

2. Порушення — будь-якого масштабу

• Навіть невеликий інцидент виявляє застарілі протоколи або прогалини в навчанні.

• Використовуйте огляди після інцидентів, щоб переглянути заходи контролю та привести їх у відповідність до поточних загроз і бізнес-цілей.

3. Відсутність постійного нагляду

• Якщо ви не можете побачити ризики в цілому або пов'язати засоби контролю зі стандартами, такими як NIST, та нормами вашої галузі, почніть спочатку.

• Поєднайте основні принципи NIST із галузевими правилами, щоб забезпечити повне охоплення…

4. Багаторічні цикли перегляду

• Трирічне очікування на перегляд структури ігнорує сучасні швидкі зміни в загрозах та регуляторних вимогах (AI, NIS2, DORA тощо).

• Запровадьте піврічні глибокі перегляди та проміжні «швидкі перевірки», щоб забезпечити постійне вдосконалення.

5. Постійне гасіння пожеж

• Якщо команда більшу частину часу витрачає на реагування на сповіщення, а не на прогнозний аналіз та перспективне планування, система є реактивною, а не проактивною.

• Перебудуйте систему з урахуванням схильності бізнесу до ризику, багаторівневої безпеки кінцевих точок та пошуку загроз на основі штучного інтелекту…

6. KRI та KPI мають негативну динаміку

• Негативні показники свідчать про те, що заходи контролю не відповідають реальним бізнес-ризикам.

• Уникайте «франкенштейнських структур», побудованих на основі декількох моделей; адаптуйте заходи контролю до власних цілей.

7. Вони створені лише для того, щоб «пройти аудит»

• Підхід, що ставить на перше місце відповідність вимогам, а на друге — бізнес, часто не враховує ключових зацікавлених сторін, не пов'язаних з IT, і залишає реальні прогалини.

• Відновлюйте систему після значних змін — нових бізнес-моделей, регуляторних вимог або розширення спектру загроз — і постійно надавайте пріоритет областям з найвищим ризиком…

Ефективні рамки — це живі системи, які часто оновлюються, ґрунтуються на поточних загрозах, бізнес-стратегії та вимірюваних показниках ефективності, а не статичні документи, спрямовані виключно на виконання вимог відповідності. ***(John Edwards. 7 signs your cybersecurity framework needs rebuilding // FoundryCo, Inc. (https://www.csoonline.com/article/4094743/7-signs-your-cybersecurity-framework-needs-rebuilding.html). 25.11.2025).***

***