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

КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

№ 9 (вересень)

Київ – 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. №9 (вересень). 176 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

«Українська військова розвідка (HUR) заявила, що її кіберспеціалісти порушили роботу систем оплати паливними картками та закрили десятки російських онлайн-сторінок під час скоординованої кібератаки, приуроченої до недільного Дня військової розвідки.

Кібератака також сталася на тлі посилення фізичних ударів по російських нафтопереробних заводах, трубопроводах та складах протягом останніх тижнів.

За даними розвідувальних джерел Kyiv Post, операція розпочалася в неділю, 7 вересня, з масштабної розподіленої атаки типу «відмова в обслуговуванні» (DDoS) , спрямованої на мережеву інфраструктуру, яка дозволяє здійснювати оплату паливом у Росії, включаючи платформи, що обробляють паливні картки.

DDoS-атака — це форма кібератаки, метою якої є паралізувати систему шляхом затоплення її автоматизованими запитами, що робить сервіс недоступним.

Серед постраждалих систем була платформа «Advanced Payment Systems», що використовується для паливних карток RosPetrol, а також сервери, що належать цифровій компанії «Ростелеком» та енергетичній корпорації «Лукойл».

Джерела оцінюють збитки Росії від збоїв у розмірі від 1 до 3 мільйонів доларів.

Пізніше того ж дня українські кіберпідрозділи завдали удару по інформаційно-комунікаційній інфраструктурі телекомунікаційного оператора K-Corp, який надає послуги російській оборонній компанії «Концерн «Калашников». За словами джерела, було виведено з ладу понад 700 комутаторів та 13 серверів у двох центрах обробки даних, що повністю зупинило роботу K-Corp.

Також було пошкоджено десятки російських вебсайтів, на яких публікувалися повідомлення, присвячені Дню військової розвідки України.

Джерела у військовій розвідці заявили, що операції проти російських компаній, які підтримують війну, триватимуть «до повної деокупації українських територій та справедливого покарання агресора»…» ***(Kateryna Zakharchenko. Kyiv Cyber Unit Hits Russian Fuel and Telecoms, Sparks Millions in Losses // BISNESGROUPP LLC (https://www.kyivpost.com/post/59696). 08.09.2025).***

***

«Компанія ESET, що спеціалізується на питаннях безпеки, знайшла переконливі докази того, що дві російські хакерські групи, пов'язані з державою, які довгий час вважалися окремими — Gamaredon (гучні, масові фішингові вторгнення) і Turla (приховані, високотехнологічні шпигунські операції) — тепер співпрацюють всередині українських мереж. У лютому, квітні та червні 2024 року ESET спостерігала, як чотири комп'ютери, спочатку заражені звичайним шкідливим програмним забезпеченням сімейства Ptero від Gamaredon, згодом отримали власний бекдор Kazuar від Turla; на одному хості

Turla навіть використовувала імплант PteroGraphin від Gamaredon, щоб перезапустити невдале завантаження Kazuar. Подальші зараження Gamaredon супроводжувалися встановленням нових дроперів Kazuar v2, що свідчить про навмисну передачу, а не про захоплення інфраструктури…

Це поєднання є примітним, оскільки ці групи традиційно діяли дуже по-різному: Gamaredon, пов'язана з Центром 18 ФСБ, розповсюджує фішингові листи та файли-ярлики серед сотень українських урядових та інфраструктурних цілей, швидко, але гучно збираючи дані; Turla, пов'язана з Центром 16 ФСБ, віддає перевагу хірургічним вторгненням, які залишаються невиявленими роками, і раніше атакувала Пентагон, європейські міністерства закордонних справ та супутниковий трафік. Аналітики дійшли висновку, що широкі позиції Gamaredon тепер слугують воронками, дозволяючи Turla вибирати стратегічні машини, що містять конфіденційну інформацію, залишаючи при цьому більш широку колекцію Gamaredon недоторканою…

Ця конвергенція відображає попередню координацію ФСБ — Гамаредон колись надав доступ до групи InvisiMole — і відповідає військовому сценарію, за якого кіберпідрозділи Москви поєднують масовий доступ із точним шпигунством для підтримки операцій проти України…» ***(Skye Jacobs. Russian hacking groups long seen as rivals now appear to be teaming up in Ukraine // TechSpot, Inc. (https://www.techspot.com/news/109572-russian-hacking-groups-long-seen-rivals-now-appear.html). 23.09.2025).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Міністри закордонних справ Японії, США та Південної Кореї зустрілися в Нью-Йорку 22 вересня. Вони обговорили співпрацю в галузі кібербезпеки, економічної безпеки та штучного інтелекту…

Міністри закордонних справ наголосили на необхідності протидії дедалі складнішим кібератакам Північної Кореї, які фінансують її програми озброєння. Офіційні особи наголосили, що хакерська група Lazarus викрала мільярди доларів лише у 2025 році. Група була спрямована на децентралізовані фінансові платформи та використовувала вразливості смарт-контрактів. У поєднанні з фішинговими шахрайствами та порушеннями ланцюгів поставок ці атаки забезпечують критично важливе фінансування ядерних та ракетних програм Північної Кореї.

Тристороння зустріч також нагадала про спільну заяву Японії, США та Південної Кореї від січня 2025 року. У ній йшлося про крадіжки криптовалюти та співпрацю між державним і приватним секторами. Зараз загроза з боку Північної Кореї виходить за межі традиційних військових сфер і поширюється на кіберпростір. Регулярні тристоронні зустрічі, які з 2010 року проводяться майже щомісяця по телефону або особисто, забезпечують платформу для координації дій…» ***(Shigeki Mori, Harsh Notariya. Japan, US, and South Korea Unite to***

Strengthen Cybersecurity and AI // BeInNews Academy (https://beincrypto.com/japan-us-and-south-korea-unite-to-strengthen-cybersecurity-and-ai/). 24.09.2025).

***

Світові тенденції в галузі кібербезпеки

«У світі існує надзвичайна нестача фахівців з кібербезпеки. Національний інститут стандартів і технологій (NIST) повідомляє про існуючий дефіцит робочої сили в 3,4 мільйона осіб у світі. У той час, коли цифрова безпека важливіша, ніж будь-коли, цей зростаючий дефіцит талантів становить надзвичайну загрозу для державних і приватних організацій. Фактично, згідно з тими ж даними NIST, очікується, що понад половина значних інцидентів у сфері кібербезпеки цього року будуть спричинені браком талантів або людським фактором.

Отже, як нам вирішити цю проблему? Підтримуючи програми, які готують наступне покоління талановитих фахівців галузі.

Поточна нестача талановитих фахівців у галузі – це саме та ситуація, коли студенти можуть скористатися послугами центрів операцій безпеки (SOC). Ці унікальні, нові для ринку програми пропонують академічним установам можливість покрити витрати, часто пов'язані з роботою SOC, зміцнюючи свої системи кібербезпеки, водночас надаючи студентам практичний досвід, який перетворюється на навички, затребувані на ринку, після закінчення навчання.

У Луїзіані перший у своєму роді студентський SOC очолює цю ініціативу у 34 кампусах Університету штату Луїзіана (LSU), використовуючи загальнодержавний підхід до кібербезпеки. Запущена у 2023 році програма LSU залучає студентів з усіх спеціальностей, не лише з кібербезпеки та IT, для роботи над SOC за постійної підтримки та навчання від TekStream через його сервіс MDR, який використовує програмне забезпечення SIEM/SOAR від Splunk, розгорнуте на AWS. SOC забезпечує цілодобове охоронне покриття у 34 закладах, надаючи студентам до 1000 годин досвіду безпеки на передовій щороку. З початку 2024 року студенти працювали приблизно над 33% усіх інцидентів кібербезпеки SOC.

В рамках цієї інноваційної моделі студенти навчаються у ветеранів галузі, як керувати мережевим центром LSU за допомогою технології Splunk. Студенти проходять навчання на тому ж рівні, що й співробітники TekStream, з питань кібератак, аналізу, захисту мережі, політики та ескалації, а також тактики реагування на реальні інциденти в режимі реального часу. Це означає, що вони отримують цінний досвід у професійних ролях, які користуються великим попитом, під час завершення навчання…

Окрім того, що студентські SOC слугують чудовим ресурсом для навчання та підвищення кваліфікації галузевих талантів, вони також надають додаткові переваги. По-перше, студентські SOC також пропонують доступне та масштабоване джерело талантів на місці для академічних установ, які прагнуть розширити або посилити свої програми кібербезпеки, особливо якщо вони хочуть застосувати загальнодержавний підхід.

Крім того, вона пропонує унікальну та конкурентоспроможну освітню пропозицію для студентів, які прагнуть успішної кар'єри в галузі кібербезпеки після закінчення навчання. Ті, хто бере участь у програмі, отримують виписку з оцінками після завершення, яка допомагає їм безпосередньо перейти на ринок праці. Це додаткова перевага для студентів, які бажають вийти в цю галузь, оскільки це дає їм перевагу під час співбесіди та процесу переговорів щодо пропозиції роботи порівняно зі студентами з інших університетів.

Зрештою, студентський SOC в LSU діє як масштабована модель, яку можуть використовувати інші організації, як приватні, так і державні, по всьому світу для покращення нашої загальної інфраструктури кібербезпеки. Інші академічні установи, такі як Технологічний інститут Нью-Джерсі (NJIT), вже впроваджують аналогічні програми у своїх кампусах…

Переваги студентського SOC не обмежуються підвищенням кваліфікації робочої сили. Завдяки державно-приватним партнерствам, таким як між LSU, TekStream, Splunk та AWS, LSU перейшов від реактивної до проактивної моделі безпеки. Це пояснюється тим, що завдяки цій структурі LSU отримує доступ до кращої автоматизації, розширеного розподілу загроз та їх усунення, використовуючи загальнодержавний підхід та узгодженість зі своєю архітектурою. Водночас їхні витрати нижчі, ніж при автономному підході, і вони можуть використовувати штучний інтелект у своїй програмі кібербезпеки, допомагаючи подолати бар'єр входу, який штучний інтелект створив для багатьох випускників…» ***(Bruce Johnson. Embracing the Next Generation of Cybersecurity Talent // TechTarget, Inc. (https://www.darkreading.com/cybersecurity-operations/embracing-next-generation-cybersecurity-talent). 05.09.2025).***

***

«…У сфері кібербезпеки склалася парадоксальна ситуація: в той час як кібератаки поширюються з тривожною швидкістю, бюджети на безпеку зростають найповільніше за останні роки. За даними галузевих аналітиків, зростання бюджету впало з 17% у 2022 році до лише 4% у 2025 році, що змушує організації робити більше з меншими витратами. Ці фінансові обмеження супроводжуються гострою нестачею талантів: майже 90% лідерів у сфері безпеки повідомляють, що їхні команди недоукомплектовані. Поєднання скорочення ресурсів та ескалації загроз створило ідеальний шторм, що змушує компанії все більше покладатися на рішення на основі штучного інтелекту, щоб заповнити цю прогалину.

ШІ виявляється особливо цінним в автоматизації рутинних завдань, таких як виявлення загроз і сортування тривог, що дозволяє перевантаженим командам безпеки зосередитися на більш складних завданнях. Ці інструменти на основі штучного інтелекту не лише підвищують ефективність, але й допомагають фахівцям вдосконалювати свої навички. Однак людський фактор залишається вирішальним, оскільки експертів з кібербезпеки стає дедалі менше, а їхній найм стає дедалі дорожчим.

Тим часом освітній сектор став головною мішенню кіберзлочинців, кількість атак на нього зросла на 41% порівняно з попереднім роком. Школи та університети

по всьому світу наразі зазнають в середньому 4 356 атак на тиждень, причому на заклади в Азійсько-Тихоокеанському регіоні припадає майже 8 000 щотижневих атак. Особливо вразливим виявився сезон повернення до навчання, коли хакери використовують фішингові атаки, замасковані під сторінки входу в систему університету, та шахрайство з оновленням платежів. Розподілена IT-інфраструктура сектору, обмежені бюджети на безпеку та величезні сховища конфіденційних даних студентів і дослідників роблять його привабливим для атак…

Щодо інших подій у сфері кібербезпеки, то великі інциденти продовжують потрапляти в заголовки новин. Гігант роздрібної торгівлі Marks & Spencer нещодавно відновив свою послугу "натисни і забери" після 15-тижневої перерви, спричиненої атакою вірусу-вимагача, яка, за прогнозами, коштувала компанії 400 мільйонів доларів упущеної вигоди. Дослідники також б'ють на сполох щодо нової вразливості ШІ, яка отримала назву "біт-фліп", коли незначні помилки в міркуваннях ШІ можуть мати катастрофічні наслідки для критично важливих систем, таких як автономні транспортні засоби та медична діагностика…

Мабуть, найбільше занепокоєння викликає використання генеративного ШІ зловмисниками на озброєнні. Anthropic, компанія, яка створила чат-бота Claude, попередила, що хакери використовують її технологію для створення складного коду атаки, вибору цінних цілей і навіть розрахунку оптимальних вимог викупу - в одному з відомих випадків вони зламали щонайменше 17 організацій…

Уряди також вживають заходів проти нових цифрових загроз. Данія посилила свої закони про авторське право для боротьби зі зловживанням глибокими фейками, що дозволяє жертвам вимагати видалення контенту та компенсації за несанкціоноване використання їхньої зовнішності. Оскільки кіберзагрози зростають як у масштабах, так і в складності, спільнота кібербезпеки стикається з нагальною потребою в інноваційних рішеннях, міжнародному співробітництві та стратегічних інвестиціях для захисту нашого світу, що стає все більш цифровим…» ***(Akshay Joshi. AI fills the gap as cybersecurity budgets shrink, and other cybersecurity news // World Economic Forum (https://www.weforum.org/stories/2025/09/ai-chatbots-education-and-other-cybersecurity-news/). 05.09.2025).***

***

«…Сфера кібербезпеки значною мірою покладається на такі метафори, як "кібервійна", "цифрові фортеці" та "кібергігієна", щоб спростити складні поняття. Однак ці метафори можуть суттєво впливати на стратегію і процес прийняття рішень - іноді призводячи до контрпродуктивних результатів. Дослідження демонструють силу метафоричного фреймінгу: Стенфордське дослідження 2011 року показало, що опис злочинності як "вірусу", а не "звіра", збільшує підтримку системних рішень на 70%, тоді як дослідження 2015 року виявило, що сприйняття раку як "дисбалансу", а не "ворога", збільшує ймовірність того, що люди будуть вживати профілактичних заходів…

Поширені метафори кібербезпеки містять як сильні, так і слабкі сторони:

Кібервійна ефективно відображає адаптивну природу загроз, але заохочує надмірне інвестування в інструменти реагування, а не в фундаментальні практики

безпеки. Кращою аналогією може бути "оборонна кіберкампанія", що нагадує стійку стратегічну позицію часів холодної війни.

Система "Замок і рів" спрощує захист периметра, але вона застаріла в епоху внутрішніх загроз і атак на ланцюги поставок. Еволюція до "міста нульової довіри" з внутрішніми контрольно-пропускними пунктами і постійною перевіркою була б більш ефективною.

Кібергігієна справедливо наголошує на рутинних практиках, але часто звинувачує користувачів замість того, щоб усунути системні недоліки. Перехід до "організаційної гігієни" або "здоров'я системи" краще розподілить відповідальність.

Цифрова імунна система ідеалізує адаптивний, самовідновлювальний захист, але може сприяти самозаспокоєнню. Її слід розглядати як бажану мету, а не як поточну реальність…

Зрештою, метафори неминучі в комунікації з питань кібербезпеки, але їх потрібно обирати свідомо. Правильна метафора може зорієнтувати організацію на стратегію і бачення, тоді як неправильна може неправильно спрямувати ресурси і створити хибне уявлення про безпеку. Ключовим моментом є вихід за межі спрощених аналогій і прийняття нюансованих рамок, які відображають складну, еволюціонуючу природу кіберзагроз…» ***(Phil Venables. Metaphors Matter: Cyber War vs. Cyber Hygiene // Philip Venables (https://www.philvenables.com/post/metaphors-matter-cyber-war-vs-cyber-hygiene). 06.09.2025).***

***

«У секторі кібербезпеки спостерігається тенденція, коли стартапи віддають перевагу поглинанню над IPO, і навіть такі високозростаючі компанії, як Wiz, відмовляються від планів публічного розміщення акцій на користь поглинання (у випадку Wiz — компанією Google). За останні роки лише кілька компаній з кібербезпеки, таких як SentinelOne (2021) і Rubrik (2024), вийшли на біржу. Наступного тижня до них приєднається Netskope, 13-річна хмарна платформа кібербезпеки, яка проведе рідкісне IPO в секторі кібербезпеки…

Netskope має спільного ключового інвестора з Rubrik: Lightspeed Venture Partners, який володіє 19,3% акцій компанії. Lightspeed, яка вперше підтримала Netskope в 2013 році, може отримати приблизно 1,1 млрд доларів від своєї частки, якщо ціна IPO буде на верхній межі діапазону 15–17 доларів за акцію. Іншими великими інвесторами є ICONIQ Growth (19,2%) та Accel (9%).

Netskope, постачальник послуг Secure Access Service Edge (SASE), конкурує з Zscaler і Palo Alto Networks, пропонуючи хмарні рішення з безпеки, такі як безпечні веб-шлюзи та брандмауер як послуга. Незважаючи на залучення 300 мільйонів доларів у 2021 році (оцінка компанії — 7,5 мільярда доларів) і конвертовану облігацію на суму 401 мільйон доларів у 2023 році, компанія залишається збитковою. Її дохід зріс до 328,5 мільйонів доларів у першій половині 2024 року (з 251,3 мільйонів доларів роком раніше), а чисті збитки скоротилися до 169,5 мільйонів доларів з 206,7 мільйонів доларів…

Якщо Netskope дебютує з цільовою оцінкою в 6,5 млрд доларів, вона приєднається до зростаючого списку компаній, що підтримуються венчурним капіталом, таких як

Chime і Hinge Health, які вийшли на біржу з оцінкою нижче їх останньої приватної оцінки. Однак не всі недавні IPO зазнали труднощів; Figma і Circle продемонстрували сильний стрибок у перший день, що свідчить про те, що інтерес інвесторів залишається вибірковим. Результати Netskope стануть ключовим тестом для життєздатності IPO в галузі кібербезпеки на ринку, де домінуючим шляхом виходу були придбання». ***(Marina Temkin. Netskope follows Rubrik as a rare cybersecurity IPO, both backed by Lightspeed // TechCrunch Media LLC. (https://techcrunch.com/2025/09/08/netskope-follows-rubrik-as-a-rare-cybersecurity-ipo-both-backed-lightspeed/). 08.09.2025).***

***

«Незважаючи на свою репутацію цифрових аборигенів, покоління Z досить погано володіє методами кібербезпеки .

Аналіз, проведений платформою споживчої аналітики GWI, показав, що хоча багато хто з цієї демографічної групи виріс в Інтернеті, лише троє з десяти мають звичку регулярно змінювати свої паролі порівняно з 42% представників покоління бебі-бумерів.

Вони також є поколінням, яке найменше схильне оновлювати програмне забезпечення та пристрої, лише 43% з них цим переймаються. кібергігієни . У дослідженні зазначається, що покоління Z не дотримується інших базових практик

Наприклад, лише 36% повідомили про використання будь-якого антивірусного програмного забезпечення , але понад половина (58%) принаймні використовують двофакторну автентифікацію (2FA).

Покоління Z також більше ризикує. Лише 35% уникають використання незахищеного громадського Wi-Fi, на відміну від 48% бебі-бумерів. Вони також рідше перевіряють свої облікові записи на наявність підозрілої активності, лише 40% роблять це, порівняно з 54% бебі-бумерів.

На запитання, наскільки вони стурбовані загрозами кібератак, лише 44% представників покоління Z сказали, що вони «дуже» або «надзвичайно» стурбовані, порівняно з 49% представників покоління бумерів…

Одним із позитивних висновків дослідження є те, що значна більшість респондентів прагнуть покращити свої навички кібербезпеки . Наприклад, 91% сказали, що навчання персоналу з питань безпеки даних має бути ключовим пріоритетом на робочому місці.

Дослідники припустили, що причиною розриву зв'язків є надмірна залежність покоління Z від смартфонів, де такі функції, як Face ID, автоматичний вхід та менеджери паролів, є нормою…

Звіт узгоджується з аналогічним дослідженням щодо звичок безпеки покоління Z, проведеним Bitwarden раніше цього року. Компанія виявила, що це покоління найгірше використовує паролі повторно: 72% визнали, що повторно використовують облікові дані, порівняно з лише 42% представників покоління бебі-бумерів…» ***(Emma Woollacott. Gen Z has a cyber hygiene problem // Future US, Inc. (https://www.itpro.com/security/gen-z-has-a-cyber-hygiene-problem). 06.09.2025).***

***

«…Cisco Talos проаналізувала інциденти з викраденням даних за останні два роки і виявила, що швидкість і підготовленість є вирішальними факторами у запобіганні атакам. Приблизно в третині випадків, які вивчала Talos, захисники, які відреагували на сповіщення про виявлення загрози на кінцевому пристрої або в системі управління протягом двох годин, вигнали зловмисників, перш ніж ті встигли викрасти дані або запустити шифрування. Ще одна третина успішних випадків порятунку сталася, коли жертва помітила підозрілу активність і залучила сторонню команду реагування на інциденти протягом 48 годин — чим швидше, тим краще. Ранні попередження від зовнішніх джерел заблокували ще 14% атак; у США багато з цих попереджень надходили через програму попередження про викрадення даних CISA, яка повідомляє організації про те, що злочинне угруповання вже отримало доступ до системи, але ще не здійснило атаки. Агресивно налаштовані засоби контролю безпеки дозволили запобігти 13% спроб, а жорсткі обмеження прав доступу, такі як обмеження доступу до компрометованих облікових записів служб, дозволили запобігти 9% атак…

Talos підкреслює, що більшість цих контрзаходів повинні бути вжиті до того, як виникнуть проблеми: добре налаштовані засоби захисту, детальне ведення журналів або покриття SIEM для швидкого відтворення подій, а також заздалегідь укладені договори з постачальниками послуг реагування на інциденти. Посередники, що забезпечують початковий доступ, залишаються поширеним попередником, продаючи доступ до мережі, що часто закінчується викраденням даних з метою вимагання викупу, тому швидке виявлення на цьому етапі має вирішальне значення. Зловмисники розраховують на шок і поспіх, щоб змусити платити викуп; організації, які готуються, стежать і швидко реагують, можуть розірвати цей цикл і уникнути гри за правилами злочинців…» ***(Mathew J. Schwartz. Here's What Blocks In-Progress Ransomware Attacks the Best // Information Security Media Group, Corp. (https://www.govinfosecurity.com/heres-what-blocks-in-progress-ransomware-attacks-best-a-29393). 09.09.2025).***

***

«…Зрілість кібербезпеки — це безперервний, ніколи не закінчуючийся процес, в якому розширення видимості виявляє більше площі атаки і, разом з тим, більше вразливостей, тоді як більш потужні можливості створюють більше можливостей випередити супротивників. Зазвичай організації проходять шлях від реактивного «гасіння пожеж» з низькою видимістю, розрізненими інструментами, перевантаженими командами, неповними інвентаризаціями активів і виправленнями лише CVE до тактичної фази, яка зменшує роз'єднаність між безпекою та IT і покращує обізнаність про поверхню атаки, але все ще покладається на ручні процеси, запізнілі виправлення та непослідовну, не засновану на ризиках пріоритезацію… Наступним важливим етапом є безпека, орієнтована на ризики: впровадження систем, заснованих на ризиках, автоматизація оцінки та кількісного визначення ризиків для об'єктивного визначення пріоритетів, а також впровадження автоматизованих заходів з усунення недоліків та забезпечення відповідності вимогам, все це за підтримки інформації

про поверхню атаки, що надходить майже в режимі реального часу. На найбільш зрілому, проактивному етапі ці досягнення об'єднуються в систему постійного зниження ризиків — передбачення та зменшення вразливості шляхом зміни умов поверхні атаки, використання автоматизації на основі штучного інтелекту/машинного навчання, узгодження безпеки з бізнес-цілями та включення кібербезпеки в систему управління ризиками на рівні правління. Хоча етапи можуть перетинатися, розгляд їх як орієнтирів допомагає командам перейти від реагування до стратегії; із зростанням зрілості управління ризиками стає більш безперервним (відображаючи підходи на зразок CTEM). Незалежно від вихідної точки, завдання залишається тим самим: побудувати шлях, який виведе вас із режиму реагування до проактивної, автоматизованої оборони, орієнтованої на ризики…» ***(What's Your Cybersecurity Maturity? // Trend Micro Incorporated. (https://www.trendmicro.com/en_us/research/25/i/cybersecurity-maturity.html). 10.09.2025).***

***

«…Дрони еволюціонували від гаджетів для хобі до важливих інструментів для ведення війни, інспекції інфраструктури, логістики та сільського господарства, але їх зростаюча корисність несе з собою гострі кіберризики. Зіткнення 8 травня над Джамму, де Індія обстріляла рої дронів, що перетинали кордон з Пакистаном, стало сигналом до початку нової гонки озброєнь, керованої машинами, і спонукало Індію до планів інвестувати до 470 мільйонів доларів у технології безпілотних літальних апаратів протягом наступних 12–24 місяців, оскільки дрони можуть наносити удари без ризику для персоналу. Більшість безпілотних літальних апаратів (UAV) здійснюють зв'язок через відкриті бездротові діапазони (часто 2,4 ГГц), що робить їх вразливими до DDoS-атак, перехоплення, маніпуляцій або тихого викрадення даних, тоді як традиційне шифрування, пов'язане з маршрутизаторами, хмарною автентифікацією та централізованим управлінням ключами, не працює в мобільних середовищах з низькою швидкістю з'єднання та в ситуаціях ad hoc Новим рішенням є вбудоване, інтегроване в апаратне забезпечення, легке шифрування «від кінця до кінця», яке знаходиться всередині дрона та його приймального сервера, що забезпечує «приватну мову», яка приймає тільки автентифіковані, зашифровані команди і розглядає неавторизовані сигнали як шум… Оскільки Китай і Пакистан також посилюють можливості безпілотних літальних апаратів, Індія повинна розглядати кібербезпеку дронів як основоположну в оборонних і цивільних цілях, забезпечуючи, щоб пристрої мали власні криптографічні «замки» і точно перевіряли, хто володіє ключами, щоб операції залишалися надійними навіть там, де мережі є нестабільними, а інфраструктура ненадійною…» ***(Srinivas Shekar. Securing the skies: how cybersecurity will define the future of drones // YourStory (https://yourstory.com/2025/09/securing-skies-cybersecurity-future-of-drones). 11.09.2025).***

***

«Підводні кабелі, які передають понад 99% транскордонних даних у світі, зараз стикаються з трьома загрозами, які виходять далеко за межі звичайної безпеки мережі. Фізично вони можуть бути зачеплені, саботовані або прослуховувані, особливо в мілководних районах і на станціях виходу, де оптичні траси відкриті. Логічно, що застарілі засоби віддаленого доступу, слабка або відсутня багатофакторна автентифікація (MFA) та погана сегментація VLAN дозволяють зловмисникам переміщатися вбік після того, як вони зламають платформу постачальника або використають непідписане оновлення прошивки. З геополітичної точки зору кабелі, прокладені через стратегічні вузькі місця, вразливі до втручання держави, законних вимог про перехоплення та маніпулювання трафіком…

Оскільки ці системи охоплюють кілька юрисдикцій, оператори повинні орієнтуватися в безлічі різних нормативних актів: Федеральна комісія зв'язку США (FCC) пропонує обов'язкові плани управління ризиками та щорічну сертифікацію, Європа вже застосовує аналогічні суворі правила, тоді як багато інших регіонів відстають у цьому питанні. Найкращий захист — це вбудувати безпеку в кожен рівень — наскрізне шифрування, контроль доступу на основі ролей, перевірені API постачальників — задовго до того, як регуляторні органи змусять це зробити.

Навіть при наявності надійних засобів контролю порушення є неминучими, тому найважливішим є стійкість. Ефективні оператори ведуть детальні плани реагування на інциденти, проводять навчальні тренування, визначають, хто спілкується з клієнтами та ЗМІ, а також мають перевірені резервні копії, готові до швидкого відновлення роботи. Швидке виявлення, ізоляція та прозора комунікація можуть перетворити потенційну катастрофу на локалізовану подію…

У майбутньому штучний інтелект посилить гонку озброєнь: супротивники використовують його для створення більш інтелектуальних фішингових атак та адаптивного шкідливого програмного забезпечення, а захисники застосовують його для аналізу величезних обсягів телеметричних даних з метою виявлення аномалій. Квантові обчислення становлять ще більшу загрозу — атаки типу «зібрати зараз, розшифрувати пізніше» вже зараз крадуть зашифрований трафік з надією на його розшифрування в майбутньому, тому організації повинні вже сьогодні розпочати оцінку квантових ризиків та планування міграції.

Зрештою, кібербезпека повинна бути спільною відповідальністю на рівні правління; для кабельних операторів, які продають безпечний транспорт, довіра є продуктом, і ставлення до безпеки як до фактора, що сприяє розвитку бізнесу, є ключовим для довгострокової стійкості…» ***(Greg Bryan. Cybersecurity Challenges in Submarine Cable Systems // TeleGeography (https://blog.telegeography.com/cybersecurity-submarine-cable-systems). 11.09.2025).***

***

«…Кіберзахист все ще є переважно реактивним — виправлення після розкриття інформації, розслідування після отримання сповіщень — оскільки команди з безпеки не мають надійного способу побачити завтрашні загрози вже сьогодні. Цифрові двійники змінюють цю ситуацію. Ці постійно оновлювані, високоточні копії всього IT-майна організації відображають кожен запис у журналі,

робоче навантаження, пристрій і дії користувача в режимі реального часу, що дозволяє захисникам відпрацьовувати атаки в «кіберпісочниці», яка не відрізняється від виробничої середовища. Усередині двійника команди можуть запускати симульовані програми-вимагачі, фішинг з використанням помилок в адресах, зловживання з боку інсайдерів або експлойти нульового дня, спостерігати за тим, як розгортається латеральний рух, і тестувати тактики локалізації ще до того, як супротивники виявлять слабкі місця… Siemens, Microsoft і ціла низка стартапів вже використовують середовища на основі двійників — деякі з них у поєднанні з генераторами атак на основі штучного інтелекту, які створюють карти ймовірності майбутніх компрометацій — для зміцнення промислових систем управління, хмарних послуг і складних ланцюгів постачання. Виклики залишаються: обробка терабайтів телеметричних даних гібридної хмари без відхилень, захист самого двійника (план, який сподобається хакерам), фінансування обчислювальних витрат і переконання правління діяти на основі прогнозних, а не криміналістичних доказів. Проте траєкторія розвитку є чіткою: із зниженням витрат і зростанням автоматизації атак цифрові двійники обіцяють перевести кібербезпеку з режиму реагування на кризові ситуації в режим прогнозування, перетворивши реагування на інциденти з кризового управління на відпрацьовану процедуру і перетворивши безпеку на проактивну функцію, що сприяє розвитку бізнесу…» ***(*Isla Sibanda.** ***Digital twins give cyber defenders a predictive edge // SiliconANGLE Media Inc. (https://siliconangle.com/2025/09/13/digital-twins-give-cyber-defenders-predictive-edge/). 13.09.2025).***

***

«…Блакитна економіка, що охоплює рибальство, аквакультуру, судноплавство, офшорну енергетику та портову логістику, швидко перетворюється під впливом цифровізації та біологічних інновацій, виявляючи критичну межу на перетині кіберпростору та наук про життя, відому як кібербіобезпека. Активність загроз прискорюється: опитування DNV 2024 року виявило, що 31% морських фахівців зазнали кібератаки протягом року (що більш ніж удвічі перевищує показник за попередні п'ять років), а 71% вважають свої промислові активи більш вразливими, ніж будь-коли, і вважають кібербезпеку головним ризиком для бізнесу. Кількість зареєстрованих інцидентів у судноплавстві зросла з трьох десять років тому до 64 у 2023 році (Університет NHL Stenden), багато з яких пов'язані з державними структурами Росії, Китаю, Північної Кореї та Ірану. Наслідки є відчутними і мають ланцюговий ефект: у березні 2025 року Lab Dookhtegan, як повідомляється, вивів з ладу супутниковий зв'язок 116 іранських суден, а Норвезький центр морської кіберстійкості зафіксував 239 руйнівних кібератак у морській галузі у 2024 році, багато з яких пов'язують із проросійською організацією NoName057(16)…

Біологічні операції також піддаються ризику. Сучасна аквакультура залежить від автоматизованого годування, генетичного аналізу та моніторингу якості води, що робить її вразливою до атак, які можуть спотворити графіки, підробити геномні записи або маніпулювати екологічним контролем — загрози, що мають як

економічні, так і екологічні наслідки. ISAC з питань продовольства та сільського господарства повідомила, що 5,5 % кіберінцидентів у першому кварталі 2025 року були пов'язані з програмним забезпеченням-вимагачем, що майже вдвічі більше, ніж у попередньому році, що свідчить про зростаючу увагу злочинців до систем водопостачання. Тим часом порти впроваджують цифровий біологічний моніторинг баластної води для виявлення інвазивних видів, однак надійність цих заходів залежить від цілісності даних, а їх фальсифікація може приховати екологічні загрози. З огляду на те, що понад 90% світової торгівлі здійснюється морським транспортом, а до 2030 року «блакитна економіка» має додати трильйони до світового ВВП, ставки є надзвичайно високими: один випадок зараження шкідливим програмним забезпеченням вже коштував провідній судноплавній компанії майже 300 мільйонів доларів…

Для зменшення ризиків необхідне управління, яке йде в ногу з технологіями: вбудовування кібербезпеки в морську біоавтоматизацію на етапі проектування; усунення прогалин у кваліфікації (три чверті морських фахівців вважають, що нинішнє навчання є недостатнім); запровадження обов'язкового навчання, звітування про інциденти та офіційних кіберпланів (як того вимагає Берегова охорона США для суден і портів до 2027 року); а також підвищення прозорості та транскордонного обміну інформацією про інциденти та найкращі практики. Ініціативи з прикладних досліджень, такі як Cyber-SHIP Lab Університету Плімута, що моделює реалістичні мережі суден і портів, ілюструють, як тестувати та зміцнювати системи на практиці. У більш широкому сенсі, безпека океанів тепер охоплює коди, генетичні дані, автоматизацію та програмне забезпечення для біологічного спостереження; кібербіобезпека лежить в основі продовольчої безпеки, раціонального використання навколишнього середовища та стійкості морської торгівлі. Геополітичний вимір набуває все більшого значення — від центрів в Індійському океані, таких як Гвадар і Чабахар, де серйозне порушення може спровокувати дипломатичні конфлікти, до малих острівних держав, економіка яких залежить від рибальства та аквакультури, до великих держав, що інвестують у цифрову морську інфраструктуру. Як і в випадку з історичним морським правом, для управління гібридними цифрово-біологічними океанами 21 століття необхідний новий режим кібербіобезпеки, що поєднує морські патрулі з захищеними мережами, зашифрованими біобазами даних та стійкими спільними системами захисту…» ***(Amina Munir. Cyberbiosecurity in the Blue Economy // moderndiplomacy.eu (https://moderndiplomacy.eu/2025/09/14/cyberbiosecurity-in-the-blue-economy/). 14.09.2025).***

***

«…У подкасті Data Xposure Джастін Толман і Джон Вілсон, директор з інформаційної безпеки HaystackID, стверджують, що найбільшим чинником впливу на порушення безпеки є не розумні хакери, а «data ROT» — надлишкові, застарілі та тривіальні дані, які накопичують організації. Вілсон називає ROT мультиплікатором порушень: одне скомпрометоване пристрій або облікові дані стають катастрофічними, коли вони розблоковують розгалужені, некласифіковані архіви, як показано на прикладі інциденту з AT&T, в результаті

якого було викрадено понад 100 мільйонів записів, де незначні витрати на зберігання контрастують із середньою вартістю порушення в США, яка, за даними IBM, у 2024 році становитиме майже 10 мільйонів доларів. Добре фінансувані, навіть підтримані венчурними капіталами синдикати, зараз досліджують системи глибше, ніж це можуть зробити багато захисників, тоді як IoT і хмарні технології розкидають конфіденційні дані по кінцевих точках і забутих серверах, розширюючи кожну поверхню атаки. Вимоги до дотримання нормативних вимог також зростають: безцільне зберігання даних збільшує збитки та послаблює захист під час аудитів і судових розглядів, а більшість компаній недооцінюють, де дублюються та залишаються незахищеними конфіденційні ідентифікатори. Вирішення проблеми очевидне — знищіть data ROT: проаналізуйте свої дані, щоб знайти PII, PHI та фінансові записи; видаліть те, що не має комерційної або нормативної цінності; анонімізуйте або псевдонімізуйте те, що залишилося. Брандмауери та нульова довіра мають значення, але найшвидшим і найдешевшим способом зменшення ризиків є очищення даних. У 2025 році питання не в тому, чи буде порушено вашу безпеку, а в тому, скільки непотрібних збитків завдасть розростання ваших даних…» ***(The $10 Million Problem You've Already Created: How Data ROT Is Fueling the Next Cyber Crisis // Exterro (https://www.exterro.com/resources/blog/the-10-million-problem-youve-already-created-how-data-rot-is-fueling-the-next-cyber-crisis). 03.09.2025).***

***

«Кібербезпека підприємств перейшла з виключно компетенції CIO/CISO до спільної юридичної відповідальності, і тепер від генеральних юрисконсультів (GC) очікується розуміння істотних кіберризиків та спільне керівництво заходами щодо їх мінімізації в умовах посилення регуляторного клімату та жорстких штрафних санкцій. Барометр генеральних юрисконсультів CSC 2025 року оцінює мінливий регуляторний ландшафт як головний ризик для юридичної діяльності, за яким слідують штучний інтелект, GDPR, конфіденційність даних та кіберзагрози; лише GDPR може накласти штрафи в розмірі 20 мільйонів євро або 4% від глобального обороту, що спонукає GC більш активно залучатися до захисту даних та підготовки до порушень. GC все частіше спільно з CIO/CISO відповідають за політику, контролюють планування на випадок кризових ситуацій та управління радою директорів, а також протистоять атакам на домени (викрадення DNS, кіберсквотинг), які переростають у вимагання викупу, що зараз посилюється фішингом та розвідкою на основі штучного інтелекту. Окрім технічних засобів контролю, успіх залежить від управління, освіти та узгодження, щоб політика йшла в ногу з часом. Основні режими включають GDPR; NIS2 (штрафи до 10 млн євро або 2% від глобального обороту); DORA для фінансових установ (з січня 2025 року, до 10 млн євро або 2%); та Закон США про корпоративну прозорість (до 10 000 доларів за кожне порушення), а правила транскордонних переказів, особливо в ЄС та Азії, додають складності… Інструментарій юридичних відділів зосереджений на проактивній програмі, що охоплює всю компанію: настільні вправи, аудити, симуляції порушень, надійне забезпечення безперервності бізнесу/відновлення після аварій та кризові

комунікації для регуляторних органів, клієнтів і постачальників за допомогою платформ комплаєнсу, що забезпечують видимість у реальному часі в різних юрисдикціях. Пріоритети включають створення матриці юридичних ризиків (наприклад, майбутні нормативні акти, штучний інтелект, невідповідність даних), призначення керівника з управління даними в кожному регіоні (з CSIRT, що відповідає NIS2, та цілодобовою звітністю) та залучення глобальних партнерів, таких як CSC, для гармонізації дотримання нормативних вимог, захисту цифрових активів та налагодження зв'язків між юридичними департаментами, IT-відділами та командами з управління ризиками у 140 юрисдикціях…» ***(Mark Flegg and David Franklin. Why General Counsels are Now Playing a Leading Role in Cybersecurity and Data Protection // Corporation Service Company (https://blog.cscglobal.com/why-general-counsels-are-now-playing-a-leading-role-in-cybersecurity-and-data-protection/). 08.09.2025).***

***

«Кіберризики стали однією з головних проблем бізнесу: у 2024 році 75% ланцюгів постачання програмного забезпечення зазнали атак, а до 2031 року глобальні збитки, за прогнозами, сягнуть 138 млрд доларів США (108 млрд фунтів стерлінгів), що ставить юридичні команди в центр організаційної стійкості… Їхній вплив є найбільшим, коли вони залучаються на ранній стадії закупівлі для встановлення практичних заходів захисту, узгоджених з постачальниками, до остаточного узгодження умов, після оцінки чинного законодавства та нормативно-правової бази, місця розташування рішення в екосистемі, його зв'язності (часто це більший ризик, ніж критичність), обізнаності постачальника про непрямі залежності та відповідальності на всіх технологічних рівнях, особливо в хмарних середовищах, керуючись чітким рівнем прийнятного ризику, який визначає управління, інструменти, кадрове забезпечення, шаблони контрактів та перевірку постачальників… Контракти повинні виходити за рамки загального дотримання політики безпеки та включати управління, прозорість, реагування на інциденти та технічні заходи контролю: права на аудит із виправленням недоліків та спрощені анкети для менших постачальників; повне відображення ланцюга постачання з обов'язками передачі інформації; структуроване управління з визначеними контактними особами та циклами звітності; обробка вірусних сповіщень відповідно до визнаних кодексів практики; обов'язкове своєчасне встановлення виправлень та заборона використання непідтримуваного програмного забезпечення (основний напрямок діяльності ICO); визначені терміни виявлення, повідомлення та реагування на інциденти та потенційні інциденти; надійний контроль доступу (мінімальні привілеї, розподіл обов'язків); чітке посилання на стандарти (ISO 27001, Cyber Essentials/Plus, NIST, CAF) та їх відповідність; перевірка та навчання персоналу (наприклад, BPSS) з урахуванням тактик найму інсайдерів… Добре сформульовані положення задають тон для конструктивної співпраці, зміцнюючи довіру та покращуючи результати з часом. Щоб забезпечити стійкість, організації повинні картографувати ризики, пов'язані з третіми сторонами, по всьому ланцюжку поставок, визначити, де закінчується юридичне управління і починається оперативна відповідальність,

узгодити умови з ризиками, пов'язаними з активами та постачальниками, розробити дизайн для повного життєвого циклу (моніторинг та виведення з експлуатації) та ставитися до постачальників як до стратегічних партнерів у сфері кіберзахисту…» ***(Jocelyn Paulley. How to strengthen cyber resilience through supply chain contracts // Gowling WLG (https://gowlingwlg.com/en/insights-resources/articles/2025/how-to-strengthen-cyber-resilience-through-supply-chain-contracts). 15.09.2025).***

***

«…Морська галузь швидко цифровізується — судна, порти та логістика тепер покладаються на взаємопов'язані IT/OT-системи, такі як AIS, навігація та робота кранів з GPS-навігацією, ECDIS, ARPA, VDR та складні вантажні платформи, що забезпечує ефективність, але й підвищує кіберризики. Загрози охоплюють атаки на судна та штаб-квартири корпорацій, які керують глобальними флотами, що може призвести до крадіжки даних, порушення роботи, інцидентів з безпекою та шкоди репутації. Морське страхування може допомогти у відшкодуванні збитків, але недооцінка, складність кількісної оцінки ризиків та широта покриття «кібернебезпек» змусили багатьох страховиків застосовувати широкі виключення (наприклад, CL 380), що підкреслює необхідність спеціалізованих знань у сфері страхування та більш чітких визначень. Галузеві органи дійшли згоди щодо загальної картини: кіберризик — це ймовірність того, що збої в роботі IT/OT можуть спричинити операційні, безпекові, фінансові або репутаційні збитки; кібератаки спрямовані на мережі та пристрої з метою отримання доступу, пошкодження або виведення з ладу систем суден і компаній; причини варіюються від зовнішнього шкідливого програмного забезпечення та вторгнень у мережу до внутрішніх помилок або несправностей обладнання… Керівні принципи BIMCO щодо кібербезпеки на борту суден, розроблені спільно з провідними морськими асоціаціями, визначають учасників (держави, злочинців, активістів, інсайдерів) та мотиви (фінансова вигода, порушення роботи, шкода репутації) конкретних цілей атак — від знищення даних, вимагання викупу та блокування послуг до маніпулювання GPS/AIS, шахрайських перевезень вантажів та збору розвідувальної інформації — та забезпечують основу для оцінки ризиків. Кібербезпека зараз є невід'ємною частиною морської безпеки: уряди (наприклад, Великобританії) включили її до національних стратегій; цифровізовані нафтогазові мережі стикаються з ризиками, описаними в IEC 62443; а гучні порушення, включаючи атаку NotPetya на Maersk у 2017 році (~300 мільйонів доларів) та атаку на індійський JNPT у 2021 році, демонструють економічні ризики. Стратегічні торговельні шляхи Індійського океану підвищують ризики, що спонукає до оновлення законодавства (наприклад, індійських законів про інформаційні технології та адміралтейство), посилення регіональної співпраці (IORA, BIMSTEC) та розширити практичні засоби захисту — виявлення на основі штучного інтелекту, відстеження вантажів за допомогою блокчейну, етичні хакерські аудити — за підтримки таких ініціатив, як зусилля QUAD у сфері кібербезпеки в Індо-Тихоокеанському регіоні, розширення уваги IFC-IOR до кібербезпеки та військово-морські навчання (MILAN, Malabar), що включають кібертренінги…

Керівні принципи ІМО доповнюють існуючу систему управління безпекою високим рівнем управління кіберризиками, що акцентує увагу на сегрегації мереж, постійному моніторингу, багаторівневому контролі за межами брандмауерів, офіційних політиках і процедурах безпеки, а також навчанні екіпажу та берегового персоналу відповідно до таких рамок, як NIST; в ЄС директиви NIS2 та галузеві директиви щодо бортових систем (E26/E27) посилюють вимоги до нових суден. Ефективні програми визначають ролі та критично важливі активи, впроваджують технічні засоби захисту та заходи забезпечення безперебійної роботи, підвищують стійкість за допомогою технічного обслуговування, контролю доступу та роботи з носіями інформації, а також готують до реагування на інциденти. У міру взаємопроникнення технологій і торгівлі морська кібербезпека — а також більш зріла та прозора система страхового реагування — стануть ключовими факторами захисту глобальних морських перевезень…» ***(Anika Tarar. Marine Insurance Law in the Age of Cyber Piracy // Khurana & Khurana (https://www.khuranaandkhurana.com/marine-insurance-law-in-the-age-of-cyber-piracy). 02.09.2025).***

***

«…Останній звіт Insight Partners показує, що глобальний ринок кібербезпеки швидко розширюється, оскільки все більш витончені атаки, більш жорсткі регуляторні вимоги та необхідність захисту цифрових активів змушують організації модернізувати засоби захисту. Інтеграція штучного інтелекту стає найбільш руйнівною силою на ринку: механізми машинного навчання тепер в режимі реального часу просівають величезні потоки даних, виявляють аномалії та автоматизують реагування на інциденти, надаючи постачальникам, які використовують ШІ, вирішальну перевагу проти експлойтів нульового дня, APT та поліморфного шкідливого програмного забезпечення. Запуск Honeywell у 2025 році Cyber Proactive Defense та OT Security Operations Center є типовим прикладом цього переходу від пасивного захисту до автономної, адаптивної безпеки…

Статистика щодо зростання загроз підкреслює нагальність проблеми. Робоча група з боротьби з фішингом зареєструвала 1,9 мільйона фішингових сайтів у період з травня 2023 року по квітень 2024 року, а у звіті IBM «Вартість порушення безпеки даних» за 2024 рік середня вартість порушення становить 4,88 мільйона доларів США, що на 10 % більше, ніж у попередньому році. Такі цифри змушують компанії інвестувати значні кошти у стратегії захисту даних та комплексні кіберпрограми.

У регіональному розрізі Північна Америка залишається найбільшим ринком кібербезпеки, за нею йде Європа, але, за прогнозами, найшвидше зростання протягом прогнозованого періоду продемонструє Азіатсько-Тихоокеанський регіон. За складовими, більшу частину витрат зараз становлять рішення з безпеки (програмне забезпечення та платформи); серед них переважають засоби мережевої безпеки, хоча безпека кінцевих точок, додатків та інфраструктури також зростає. Великі підприємства як і раніше складають найбільший сегмент клієнтів, а банківські/фінансові послуги лідирують за вертикальним попитом, випереджаючи

IT-телекомунікації, державний сектор, охорону здоров'я, виробництво та роздрібну торгівлю/електронну комерцію…

Серед основних постачальників, що формують конкурентне середовище, є IBM, Oracle, SAP, Cisco, Microsoft, Broadcom, Palo Alto Networks, CrowdStrike та Fortinet. Актуальні теми в їхніх портфелях варіюються від запобігання втраті даних і багатофакторної автентифікації до перевірки ідентичності та архітектур нульової довіри. Разом ці динамічні зміни вказують на те, що ринок продовжуватиме розширюватися у міру зростання кіберризиків і поширення стандартної практики використання адаптивних засобів захисту на основі штучного інтелекту…» ***(Cybersecurity Market Is Projected To Reach US$552.35 Billion By 2031 With CAGR Of 13.8% | The Insight Partners // Yahoo (https://finance.yahoo.com/news/cybersecurity-market-projected-reach-us-140100083.html?fr=sycsrp_catchall). 16.09.2025).***

***

«…Сьогоднішній кіберзахист ґрунтується на двох окремих підходах: квантовому розподілі ключів (QKD), що пасивно спирається на «заборонні» теореми квантової механіки, та пост-квантовій криптографії (PQC), яка покладається на складність певних математичних задач. Обидва методи потрібні, та обидва залишаються реактивними й не поєднані спільною теорією. Концепція QIQD (Quaternary Interpretation of Quantum Dynamics) пропонує подолати цей розрив: вона розглядає нинішню квантову теорію як «тінь» глибшої, чотирьохкомпонентної геометричної структури. Якщо ця структура справді визначає поведінку квантової інформації, то обмеження, які ми сьогодні сприймаємо як даність, перетворюються на параметри конструювання. Безпека стає не побічним ефектом фізики, а інженерною властивістю…

Для QKD це означає можливість створювати квантові стани, які не лише виявляють спробу спостереження, а й підсилюють навіть найменший натяк на втручання, зводячи шпигування нанівець ще на етапі наміру. Для PQC – перехід від «практичної складності» до структурної неможливості: певні задачі можуть бути принципово нерозв’язними жодним квантовим алгоритмом, оскільки їх розв’язання суперечило б геометрії інформації, описаній QIQD. Уніфікуючи фізичний і математичний виміри, QIQD формує основу, де криптографічна стійкість доводиться не емпірично, а строго — подібно до того, як неможливо побудувати чотирикутний трикутник…

Таким чином, майбутнє безпеки полягає не у нарощуванні «вищих мурів», а у переосмисленні самого фундаменту: створенні систем, у яких порушення структурально неможливе. Для фінансів, оборони та критичної інфраструктури це відкриває перспективу детермінованого, доказового захисту даних — і ця епоха вже розпочинається…» ***(Pravir Malik. The Future Of Cybersecurity Is Structural // Forbes (https://www.forbes.com/councils/forbestechcouncil/2025/09/19/the-future-of-cybersecurity-is-structural/). 19.09.2025).***

***

«…Традиційне поняття периметра кібербезпеки, яке колись було адекватним, коли офіси розміщували комп'ютери та сервери за брандмауерами та VPN, більше не відповідає світу, перетвореному веб-технологіями, мобільністю, хмарними технологіями, SaaS та штучним інтелектом. Замість того, щоб нарощувати периметр захисту, організації повинні захищати всю екосистему, зосередившись на взаємодії людей, даних та технологій… Людей часто не беруть до уваги, але вони мають широкий доступ і стикаються з найбільшою кількістю атак. Команди з безпеки повинні знати, хто вони, де працюють, до яких даних мають доступ і які інструменти використовують, а потім застосовувати засоби спостереження, управління та захисту, які супроводжують їх у різних місцях і на різних пристроях. Дані, які стають дедалі важливішими в епоху штучного інтелекту, вимагають відображення потоків, ретельного ведення журналів та аудиту — вкладень електронної пошти, завантажень із SharePoint, завантажень на зовнішні сервіси — адже неможливо захистити те, чого не бачиш. Технології залишаються критично важливими, але сучасні децентралізовані, швидко впроваджувані інструменти SaaS та AI випереджають традиційні засоби контролю, розширюючи площу атаки навіть за допомогою EDR та шлюзів електронної пошти. У цьому майбутньому без кордонів — з віддаленою роботою скрізь, даними поза силосами, користувачами, що входять в додатки з будь-якого пристрою — периметральне мислення не працює; тільки цілісна програма, яка постійно спостерігає та керує людьми, даними та технологіями, може йти в ногу з часом та зменшувати ризики…» ***(Cody Pierce. Why Cybersecurity Is About People, Data And Technology—Not Perimeters // Forbes (https://www.forbes.com/councils/forbestechcouncil/2025/09/16/why-cybersecurity-is-about-people-data-and-technology-not-perimeters/). 16.09.2025).***

***

«…У 2025 році кібербезпека стала необхідною не тільки для великих підприємств, але й для малих і середніх підприємств як засіб захисту діяльності, співробітників і клієнтів, а також як ознака зрілості, підтверджена визнаними сертифікатами кібербезпеки. Такі сертифікати, отримані підприємством та/або його персоналом, підтверджують дотримання стандартів захисту цифрових активів і можуть бути конкурентною перевагою, особливо для електронної комерції. Вони формують довіру та авторитет, сприяють дотриманню нормативних вимог, зменшують ризики завдяки найкращим практикам контролю та сприяють постійному вдосконаленню завдяки суворим оцінкам… І навпаки, відмова від інвестицій у безпеку може призвести до витоку даних, втрати інтелектуальної власності, штрафів за недотримання вимог та дорогих перебоїв у роботі бізнесу. Найбільш визнаним сертифікатом є ISO 27001, глобальний стандарт для створення та постійного вдосконалення системи управління інформаційною безпекою (ISMS); він вимагає визначення політик та цілей, проведення надійної оцінки ризиків, впровадження заходів контролю та постійного моніторингу, а сертифікація зазвичай відбувається після аналізу недоліків, впровадження, внутрішнього аудиту та зовнішнього аудиту акредитованим органом. Хоча інші стандарти, такі як SOC 2 та NIST, також мають великий вплив, багато з них є

специфічними для певних регіонів; ISO 27001 широко визнаний у всьому світі. Для малих та середніх підприємств будь-якого розміру пріоритетність кібербезпеки та підтвердження її за допомогою сертифікації допомагає захистити дані, відповідати нормативним вимогам та підтримувати довіру клієнтів, одночасно зменшуючи ризик інцидентів, які можуть зашкодити репутації та прибутковості…» ***(Lungile Msomi. Cybersecurity Certification for SMEs // SME South Africa (https://smesouthafrica.co.za/cybersecurity-certification-for-smes/). 15.09.2025).***

***

«Швидке зростання популярності онлайн-казино, зумовлене глобальним поширенням смартфонів, швидким мобільним широкосмуговим доступом до Інтернету та імерсивними технологіями, такими як віртуальна реальність та штучний інтелект, створило прибуткову цілодобову ігрову індустрію, яка пропонує все: від ігрових автоматів і покеру до рулетки в прямому ефірі. Однак цей успіх також привернув увагу досвідчених кіберзлочинців. Зараз зловмисники націлюються на платформи казино з трьома основними цілями: викрадення даних клієнтів, які можна продати або використовувати для крадіжки особистих даних; розгортання програм-вимагачів, які блокують операторам доступ до критично важливих систем до моменту здійснення платежу; та запуск руйнівних атак, які виводять з ладу веб-сайти або вимикають ігрові автомати та платіжні мережі, що призводить до дорогого простою. Інцидент 2023 року в MGM Resorts ілюструє, про що йдеться: ключ-карти, банкомати та системи бронювання в знакових об'єктах Лас-Вегаса вийшли з ладу, що спричинило збитки на суму близько 100 мільйонів доларів США, колективні позови та підірвало довіру клієнтів…

Щоб уникнути подібних наслідків, оператори казино повинні впровадити багаторівневі засоби захисту кібербезпеки. Основні заходи включають наскрізне шифрування (SSL/TLS) для всього трафіку, безпечні платіжні шлюзи, що відповідають GDPR та іншим правилам захисту даних, постійні тестування на проникнення та аудити, складні системи виявлення вторгнень, а також багатофакторну та біометричну аутентифікацію для запобігання захопленню облікових записів. Підтримка цих заходів контролю не тільки захищає доходи, але й зберігає репутацію бренду, від якої залежить лояльність гравців. У перспективі нові інструменти, особливо реєстри транзакцій на основі блокчейну, обіцяють ще більш надійні заходи захисту завдяки забезпеченню захищених від фальсифікації записів та децентралізованої верифікації. Коротко кажучи, у міру розширення онлайн-ігор, настільки ж просунута кібербезпека стала критично важливою передумовою для бізнесу, а не розкішшю…» ***(The Role of Cybersecurity in Online Casinos // RADAR ONLINE™ (https://radaronline.com/p/role-of-cybersecurity-online-casinos/). 17.09.2025).***

***

«…Національний тест на конфіденційність NordVPN 2025 року, в якому взяли участь 30 792 респонденти з 186 країн, показує, що глобальні знання в галузі онлайн-безпеки погіршуються: середній бал склав лише 57/100, що

нижче за 61 у 2023 році, і лише 10 % користувачів можна вважати «кіберзірками»… Учасники найкраще знають основи — 96 % можуть створити надійний пароль, 95 % відхилять сумнівні пропозиції щодо потокового передавання даних, а 94 % знають, які дозволи для додатків слід надавати, — але вони погано справляються з більш глибокими питаннями конфіденційності, такими як метадані, які збирають постачальники інтернет-послуг (13 % правильних відповідей), як захистити домашню мережу Wi-Fi (16 %) або які ризики, пов'язані з даними штучного інтелекту, існують на роботі (6 %). Усвідомлення необхідності своєчасного оновлення додатків також знизилося з 56 % до 54 %. Литва очолює рейтинг країн (62/100), за нею йдуть Сінгапур та Індія (61), а потім Польща та Фінляндія (60), тоді як вікова група 30-54 років та IT-фахівці мають найкращі загальні показники. Технічний директор NordVPN Маріюс Брієдіс попереджає, що загрози, пов'язані з штучним інтелектом, посилюють ці прогалини в знаннях, і закликає користувачів вживати основних заходів безпеки: використовувати унікальні паролі, які зберігаються в сховищі або ключах доступу, багатофакторну автентифікацію, своєчасно оновлювати програмне забезпечення, використовувати шифрування VPN, регулярно перевіряти налаштування конфіденційності та постійно навчатися кібергігієні…» ***(Global cybersecurity and online privacy awareness stalls // it-online (https://it-online.co.za/2025/09/18/global-cybersecurity-and-online-privacy-awareness-stalls/). 18.09.2025).***

***

«…Опитування Claroty, в якому взяли участь 1100 фахівців з безпеки, інженерії та експлуатації, показало, що економічна нестабільність, зміна тарифів і посилення геополітичної напруженості підвищують ризики для кіберфізичних систем (CPS) швидше, ніж багато організацій можуть до цього адаптуватися. Майже половина респондентів (49%) стверджують, що переформатування ланцюгів поставок, спричинене цими глобальними факторами, безпосередньо підвищило вразливість промислових, медичних та інших активів CPS. Сорок п'ять відсотків сумніваються у своїй здатності оцінити або зменшити цей ризик, а 67% активно переглядають географію своєї бази постачальників, щоб його зменшити.

Віддалений доступ третіх сторін став найслабшою ланкою: 46% компаній за останній рік зазнали порушення безпеки CPS через зовнішнього постачальника, а 54% виявили прогалини в контрактній безпеці лише після інциденту. Як наслідок, 73% компаній зараз переоцінюють спосіб підключення зовнішніх партнерів до заводів і лікарень, навіть попри впровадження нових інструментів віддаленого доступу для забезпечення безперебійної роботи складних систем…

Зусилля з дотримання вимог також перебувають у стані змін. Близько 70% організацій вже дотримуються таких стандартів, як NIST та ENISA, проте 76% побоюються, що майбутні нормативні вимоги змусять їх переглянути свої програми безпеки CPS, що порушить ефективність роботи в той час, коли напруга в ланцюгах постачання вимагає більшої гнучкості. Ендрю Лінтелл з Claroty зазначає, що компанії повинні перейти «від мислення, орієнтованого на дотримання вимог, до мислення, орієнтованого на стійкість», інтегруючи безпеку як основну функцію

бізнесу, одночасно справляючись із більшою кількістю змін постачальників за шість місяців, ніж вони мали за останні десятиліття…» ***(Ian Barker. Economic uncertainty adds to cyber-physical systems risk // BetaNews, Inc. (https://betanews.com/2025/09/17/economic-uncertainty-adds-to-cyber-physical-systems-risk/). 17.09.2025).***

***

«У міру того як підприємства проходять цифрову трансформацію, їхні поверхні атаки різко розширюються, піддаючи їх все більш складним кіберзагрозам, які виходять далеко за межі традиційних вірусів і спаму. Сучасний ландшафт загроз охоплює програми-вимагачі, внутрішні загрози, складні фішингові кампанії, атаки на ланцюги поставок, експлойти нульового дня та операції на рівні держав. Ця складність вимагає не тільки засобів безпеки, а й експертних рекомендацій у вигляді консультаційних послуг з кібербезпеки, які допомагають подолати розрив між бізнес-цілями та результатами в галузі безпеки…

Консультації з кібербезпеки надають спеціалізовані знання, які допомагають організаціям оцінити свою поточну інфраструктуру, виявити вразливі місця та розробити стратегічні плани дій для забезпечення кіберстійкості. Консультанти працюють над впровадженням та оптимізацією технологій безпеки, забезпечуючи при цьому відповідність вимогам таких стандартів, як HIPAA, PCI-DSS, GDPR, SOC 2 та ISO 27001. За допомогою комплексних аудитів кібербезпеки вони проводять структурований аналіз політик, процесів і систем, відображаючи поверхні атаки в IT-, OT-, IoT- та хмарних середовищах. Ці аудити виявляють неправильні налаштування, слабкі паролі та застарілі системи, одночасно тестуючи засоби захисту за допомогою тестів на проникнення та вправ «червоної команди», що в кінцевому підсумку дає практичні рекомендації, які створюють базу для визначення пріоритетності ризиків…

Діапазон рішень з кібербезпеки, що пропонуються в рамках консалтингу, охоплює кілька сфер. Мережева безпека включає брандмауери, запобігання вторгненням та безпечне проектування архітектури. Безпека кінцевих точок захищає ноутбуки, мобільні пристрої, сервери та обладнання Інтернету речей. Хмарна безпека захищає SaaS, IaaS, PaaS та гібридні хмарні робочі навантаження, тоді як безпека додатків зосереджується на безпечному кодуванні, тестуванні та захисті під час виконання. Управління ідентифікацією та доступом реалізує багатофакторну автентифікацію та контроль привілейованого доступу. Центри безпеки забезпечують кероване виявлення та реагування, а також можливості пошуку загроз. Управління відповідністю забезпечує постійне дотримання нормативних вимог, а планування відновлення після аварій підтримує безперервність бізнесу під час інцидентів.

Основні консультаційні послуги є основою будь-якої надійної програми безпеки. Оцінка ризиків дозволяє визначити загрози за ймовірністю та впливом, а планування реагування на інциденти дозволяє розробити та перевірити сценарії реагування. Управління вразливостями забезпечує постійне виправлення та моніторинг, а інтеграція інформації про загрози використовує потоки даних у

реальному часі для проактивної оборони. Навчання співробітників дозволяє навчити персонал розпізнавати спроби фішингу та шахрайства, а послуги з управління, ризиків та дотримання вимог дозволяють узгодити політику організації з законодавчими вимогами та галузевими стандартами. Ці послуги дозволяють організаціям перейти від реагування на проблеми до проактивного запобігання їм…

Компанія Seceon Inc. демонструє, як сучасні платформи доповнюють консультаційні послуги за допомогою своєї системи Open Threat Management. Платформа aiSIEM збирає та корелює журнали, потоки та події у всіх середовищах, а aiXDR-PMax розширює покриття на кінцеві точки, сервери та додатки для виявлення в режимі реального часу та автоматизованого реагування. Функція aiSecurityScore360 забезпечує безперервну оцінку ризиків та видимість вразливостей і зовнішніх загроз. Динамічне моделювання загроз виявляє невідомі загрози шляхом створення базових показників поведінки, а автоматизовані засоби виправлення можуть миттєво ізолювати кінцеві точки, блокувати IP-адреси та вимикати скомпрометовані облікові записи. Багатокористувацька конструкція, готова до MSSP, дозволяє постачальникам послуг пропонувати безпеку корпоративного рівня в необхідному обсязі…

Інтеграція штучного інтелекту та машинного навчання в послуги з кібербезпеки автоматизує виявлення загроз, зменшує кількість помилкових спрацьовувань, ідентифікує атаки «нульового дня» та забезпечує швидше реагування на інциденти. Ця технологія задовольняє зростаючий попит на фахівців, які мають навички пошуку загроз, реагування на інциденти, тестування на проникнення, експертизу GRC та аналіз безпеки на основі штучного інтелекту/машинного навчання. Поєднуючи консультаційний досвід із платформами на базі штучного інтелекту, організації досягають проактивного захисту від сучасних загроз, спрощення операцій SOC, постійної готовності до дотримання вимог та масштабованого захисту в гібридних, мультихмарних та OT-середовищах…

У сучасному світі загроз кібератаки можуть бути неминучими, але порушення безпеки — ні. Поєднання експертних консультацій та передових технологічних платформ на основі штучного інтелекту та машинного навчання створює потужну стратегію захисту, яка не тільки захищає організації сьогодні, але й готує їх до викликів завтрашнього дня. Завдяки комплексним аудитам, стратегічному плануванню, постійному моніторингу та можливостям автоматизованого реагування організації можуть побудувати справжню кіберстійкість, дотримуватися нормативних вимог та зберегти довіру зацікавлених сторін у світі, що стає дедалі більш цифровим…» ***(Pushpendra Mishra. Cybersecurity Consulting // Techstrong Group Inc. (https://securityboulevard.com/2025/09/cybersecurity-consulting/). 19.09.2025).***

***

«…У багатьох підприємствах IT-команди та команди з безпеки працюють у різних напрямках: керівники IT-відділів прагнуть інновацій, безперебійної роботи та продуктивності користувачів, тоді як керівники служб

інформаційної безпеки зосереджуються на зменшенні ризиків та запобіганні загрозам... Працюючи з окремими інструментами та наборами даних, кожна група має власне бачення активів та вразливостей, що призводить до критичних прогалин, незахищених систем, затримок у реагуванні на інциденти та прогалин у дотриманні вимог. Результатом є підвищення ризику порушення безпеки, операційні перешкоди, дублювання зусиль і марнування бюджетів. Щоб подолати цю прірву, керівники повинні просувати культуру, в якій кібербезпека є відповідальністю кожного, і узгоджувати цілі IT-безпеки з бізнес-цілями. Інтегрована платформа на базі штучного інтелекту, яка об'єднує виявлення активів, оцінку вразливостей, виправлення та спільні інформаційні панелі, забезпечує технічну єдність: вона руйнує ізольовані масиви даних, визначає пріоритетність виправлень за впливом на бізнес, автоматизує виправлення та забезпечує повну прозорість у режимі реального часу… Маючи єдину оперативну картину, обидві команди можуть діяти за однаковими пріоритетами, зменшувати ризики, прискорювати реагування, оптимізувати робочі процеси та посилювати готовність до дотримання нормативних вимог — і все це при підтримці інновацій та безперебійної роботи…» ***(Jeff Miller. Why IT/Security alignment is the key to efficient operations // FoundryCo, Inc. (https://www.computerworld.com/article/4060183/why-it-security-alignment-is-the-key-to-efficient-operations.html). 18.09.2025).***

***

«Нове опитування, проведене компанією Cytactic , яка спеціалізується на управлінні реагуванням на інциденти кібербезпеки (CIRM), показує, що 70 відсотків керівників у сфері кібербезпеки кажуть, що внутрішня неузгодженість після кібератаки спричинила їм більший хаос, ніж сам зловмисник, що паралізувало багато організацій через порушення повноважень, координації та чіткості.

У звіті також зазначається, що хоча 73 відсотки керівників описують свої плани реагування як «технічно вичерпні», багато хто визнає, що ці плани руйнуються під тиском реального світу. Крім того, 86 відсотків кажуть, що «час на перехід» між юридичною, комунікаційною та технічною командами призводить до дороговартісних затримок, підкреслюючи, що порушення часто зриваються радше внутрішніми збоями, ніж зловмисниками.

Лідерство є проблемою: 73 відсотки опитаних відчували напруженість між CISO та генеральним директором під час реагування на інциденти, що додало стресу до і без того хаотичного середовища. 54 відсотки кажуть, що відповідальність за прийняття рішень змістилася посеред інциденту, що призвело до затримок, тоді як 41 відсоток затримав критично важливі дії, оскільки ніхто не знав, хто має остаточне рішення.

Крім того, 67 відсотків кажуть, що фрагментовані або складні інструменти уповільнили їхню реакцію. 93 відсотки вважають, що допомога на базі штучного інтелекту могла б запобігти принаймні одній серйозній помилці, а 95 відсотків планують інвестиції в симуляції на основі штучного інтелекту для підвищення готовності…» ***(Ian Barker. Internal chaos after a cyberattack causes more damage***

than the attack itself // BetaNews, Inc. (https://betanews.com/2025/09/19/internal-chaos-after-a-cyberattack-causes-more-damage-than-the-attack-itself/). 19.09.2025).

***

Сполучені Штати Америки та Канада

«…Вашингтонські законодавці 3 вересня рішуче продовжили дію Закону про обмін інформацією з питань кібербезпеки (CISA) - закону десятирічної давнини, який дозволяє приватним компаніям ділитися розвідданими про кіберзагрози з федеральним урядом без юридичних наслідків. Перезатвердження закону, що перебував у стані невизначеності, було зустрінуте широким схваленням з боку лідерів кібербезпеки, які попереджали, що втрата чинності закону могла б дестабілізувати давні практики обміну інформацією про загрози…

Вперше прийнятий у 2015 році, CISA забезпечує важливі правові гарантії для організацій, які розкривають інформацію про порушення та індикатори кіберзагроз таким агентствам, як Агентство з кібербезпеки та безпеки інфраструктури (CISA). Рекс Бут, директор з інформаційної безпеки SailPoint, підкреслив його важливість: "Це дозволяє приватним організаціям ділитися розвідданими про загрози, не боячись відповідальності. Якщо організація виявляє шаблон атаки, який може допомогти іншим, вона може безпечно повідомити про це"…

Оновлене законодавство включає положення, що стосуються нових технологій, таких як штучний інтелект, що забезпечує його актуальність у сучасному мінливому ландшафті загроз. Даніель Крозе з Palo Alto Networks високо оцінив оновлення, заявивши, що вони "посилять колективну оборону, захищаючи вільний потік даних про кіберзагрози"…

Деякі законодавці та експерти, в тому числі генеральний директор Gray Space Strategies Корі Сімпсон, вказали на зростання кіберзагроз з боку Китаю як на ключову причину терміновості. Сімпсон попередив, що прогалина в CISA зробить США вразливими в період ескалації атак.

Однак Бут запропонував ширшу перспективу, стверджуючи, що хоча Китай є значною загрозою, цінність CISA полягає в його здатності протистояти всім кіберризикам національних держав. "Я не здивуюся, якщо Китай виділяють для того, щоб заручитися підтримкою, але закон спрямований на захист від усіх супротивників", - зазначив він…

Двопартійне оновлення CISA підкреслює його роль як наріжного каменю стратегії кібербезпеки США. Підтримуючи правовий захист обміну інформацією про загрози, закон гарантує, що бізнес та державні установи можуть продовжувати співпрацювати для виявлення, пом'якшення та запобігання атакам - критично важлива перевага в епоху невпинних кіберзагроз…» ***(Eoin Higgins. Experts hail likely renewal of important cybersecurity act // Morning Brew Inc. (https://www.itbrew.com/stories/2025/09/05/experts-hail-likely-renewal-of-important-cybersecurity-act). 05.09.2025).***

***

«Федеральне агентство з надзвичайних ситуацій США (FEMA) впровадило значні зміни в системі безпеки після кібервтручання, яке змусило міністра внутрішньої безпеки Крісті Ноем звільнити наприкінці серпня два десятки співробітників технічного відділу, включаючи керівників служби кібербезпеки. Порушення, виявлене під час планової перевірки, викрило вразливі місця, які дозволили хакерам проникнути в мережу FEMA, що становило загрозу для DHS і національної безпеки…

Джерела, обізнані з цим питанням (які висловилися анонімно), припустили, що порушення могло бути спричинене незахищеними інтернет-додатками та прогалинами в системі безпеки IT-середовища FEMA. У відповідь агентство заблокувало доступ до соціальних мереж, таких як X (Twitter), Facebook, YouTube та Reddit, посилаючись на міркування безпеки. Крім того, співробітники більше не можуть відключати служби інтернет-безпеки Zscaler без пароля — це значна зміна, оскільки раніше працівники могли обходити захист з мінімальним обґрунтуванням…

Ще одним потенційним слабким місцем був канал Slack, який використовував великий урядовий підрядник (його назва не розголошується з міркувань безпеки). На відміну від Microsoft Teams FEMA, Slack підрядника не мав засобів контролю безпеки мобільних пристроїв, а це означало, що вкрадені телефони могли надати хакерам постійний доступ до конфіденційної інформації…

Колишній CIO FEMA Чарльз Армстронг, який був серед звільнених, відмовився від коментарів. Раніше агентство наказало обов'язкове скидання паролів в середині серпня через загрози кібербезпеці, хоча подробиці були скупі. DHS звинуватило IT-персонал FEMA в опорі виправленням, пропусканні перевірок і применшенні вразливостей, включаючи невиконання багатофакторної аутентифікації (MFA) і виправлення критичних недоліків…

Хоча DHS постраждало від глобального хакерського нападу на Microsoft SharePoint у липні, залишається незрозумілим, чи пов'язаний цей інцидент із порушенням безпеки FEMA. Агентство та DHS не надали додаткових коментарів. Звільнення та зміни в політиці підкреслюють зростаючу стурбованість щодо готовності федеральної кібербезпеки в умовах ескалації загроз». ***(David DiMolfetta. FEMA begins security overhauls following cyber incident and employee firings // Government Executive Media Group LLC (https://www.govexec.com/management/2025/09/fema-begins-security-overhauls-following-cyber-incident-and-employee-firings/407956/). 08.09.2025).***

***

«Колишній співробітник WhatsApp, що належить Meta Platforms Inc., подав федеральний позов, стверджуючи, що він повідомляв своїм керівникам про проблеми з кібербезпекою, але його ігнорували і піддавали репресіям.

Колишній співробітник, Аттаулла Байг, заявив, що виявив «системні порушення кібербезпеки, які становили серйозну загрозу для даних користувачів», і що близько 1500 інженерів WhatsApp мали необмежений доступ до даних користувачів.

Байг стверджує, що компанія вжила проти нього заходів у вигляді негативних оцінок роботи та звільнення через низьку продуктивність після того, як він висловив занепокоєння своєму керівнику та іншим вищим посадовцям, зокрема генеральному директору Meta Марку Цукербергу…» ***(Andrew Martin and Jake Bleiberg. Former WhatsApp Employee Says Bosses Ignored Cybersecurity Flaws // Bloomberg L.P. (https://www.bloomberg.com/news/articles/2025-09-08/former-whatsapp-employee-says-bosses-ignored-cybersecurity-flaws). 09.09.2025).***

***

«…Ініціатива Міністерства юстиції США щодо боротьби з кібершахрайством перетворила Закон про неправдиві заяви (FCA) на універсальний інструмент боротьби з порушеннями кібербезпеки: підрядники, отримувачі грантів, а тепер навіть виробники медичного обладнання та їхні приватні інвестори стають об'єктами розслідувань FCA та багатомільйонних судових позовів просто за те, що не дотрималися необхідних заходів безпеки, навіть за відсутності фактичного порушення даних… У травні 2025 року Міністерство юстиції США уклало угоду на суму 1,75 млн доларів США з оборонним підрядником — і, що важливо, з його власником приватного капіталу — щодо невиконання компанією вимог NIST SP 800-171 та незабезпечення захисту контрольованої некласифікованої інформації, що стало першим випадком залучення спонсора приватного капіталу до вирішення справи про порушення FCA у сфері кібербезпеки. Кілька тижнів по тому біотехнологічна компанія виплатила 9,8 млн доларів США для врегулювання звинувачень у тому, що пристрої для секвенування геному, продані федеральним замовникам, містили невирішені вразливості. Це був перший випадок FCA, пов'язаний з правилами системи якості FDA та практиками кібербезпеки в секторі охорони здоров'я… Ці дії доповнюють розширювальну мережу федеральних і державних кіберправил (пункти DFARS Міністерства оборони, нова програма безпеки даних Міністерства юстиції, запропоновані зміни до HIPAA, вимоги до державних лікарень, указ Білого дому) і сигналізують, що будь-яка організація, яка обробляє конфіденційні дані про здоров'я, геномні дані або дані національної безпеки, може зіткнутися з потрійним збитком за FCA за «істотні недоліки» безпеки. Оскільки Міністерство юстиції США активізувало роботу спільної з Міністерством охорони здоров'я та соціальних служб робочої групи FCA, спрямованої, серед іншого, на «матеріально дефектні медичні пристрої», компанії та їхні інвестори повинні припустити, що неналежна кібергігієна, неточні засвідчення або затримка усунення вразливостей можуть спричинити позови інформаторів, руйнівні штрафи та обов'язкове розкриття інформації. Надійні, постійно оновлювані програми дотримання вимог, оперативне усунення недоліків, точні заяви та, за необхідності, своєчасне саморозкриття інформації та співпраця зі слідчими — це тепер необхідні заходи з управління ризиками для державних підрядників, постачальників медичних послуг та виробників медичного обладнання…» ***(Townsend L. Bourne, David T. Fischer, Calla Simeone. The Expanding Scope of FCA-Cybersecurity Liability // National Law Forum, LLC (https://natlawreview.com/article/expanding-scope-fca-cybersecurity-liability). 05.09.2025).***

***

«…Національний директор з кібербезпеки Шон Кернкросс заявив на саміті з кібербезпеки в Біллінгтоні, що Сполученим Штатам потрібна нова, централізовано координована кіберстратегія, яка «перекладає тягар ризику в кіберпросторі з американців на їхніх супротивників». Хоча адміністрація Байдена опублікувала національну стратегію кібербезпеки в 2023 році, Кернкросс заявив, що зусилля США залишаються розрізненими і реактивними: «Ми занадто довго милувалися проблемою». Він закликав до «стійкої переваги» над Китаєм та іншими «крихкими авторитарними режимами», які можуть інтегрувати свої інструменти влади більш злагоджено, ніж Сполучені Штати…
Кернкросс окреслив три найближчі пріоритети: 1) поновлення Конгресом Закону про обмін інформацією з питань кібербезпеки, термін дії якого закінчується цього місяця; 2) швидка модернізація федеральних мереж, включаючи підготовку до постквантового світу; та 3) безпека продуктів «за задумом», у поєднанні з оптимізованими нормами для галузі. Він також пообіцяв тіснішу співпрацю між Офісом національного директора з кібербезпеки, Радою національної безпеки та Агентством з кібербезпеки та безпеки інфраструктури, заявивши, що Білий дім покладе край «територіальним війнам і бюрократичним безглуздям», які заважали попереднім адміністраціям…» ***(Tim Starks. National cyber director: U.S. strategy needs to shift cyber risk from Americans to its adversaries // CyberScoop (https://cyberscoop.com/us-cybersecurity-strategy-sean-cairncross-shift-risk-china-trump-biden-cisa/). 09.09.2025).***

***

«…З 9 листопада будь-яка компанія, яка хоче співпрацювати з Пентагоном, повинна буде довести, що вона відповідає стандарту сертифікації моделі зрілості кібербезпеки (CMMC) Міністерства оборони. Остаточне правило Міністерства оборони вимагає, щоб кожен постачальник в оборонно-промисловій базі відповідав одному з трьох рівнів CMMC, обраних відповідно до чутливості несекретних даних, з якими буде працювати підрядник, перш ніж він зможе виграти контракт, оскільки ця вимога поступово впроваджується в тендери. CMMC вимагає таких заходів контролю, як обмежений доступ до даних, надійна аутентифікація користувачів, фізичні заходи безпеки для об'єктів, своєчасне виправлення та швидке повідомлення про інциденти. Рівень 1 дозволяє щорічну самооцінку; рівень 2, як правило, вимагає аудиту третьої сторони (самооцінка допускається тільки в обмежених випадках); рівень 3 вимагає перевірки, проведеної урядом. Контрактні офіцери повинні вказувати необхідний рівень у кожному запиті на пропозиції і можуть присуджувати роботи тільки компаніям, які мають чинну сертифікацію або оцінку. Це правило, яке є вдосконаленням попередньої версії, що піддавалася критиці з боку галузі, перекладає відповідальність за кібербезпеку безпосередньо на підрядників — крок відображає очікування, що постачальники «поставлять національну безпеку США на перше місце у своєму списку пріоритетів»…» ***(Brandon Vigliarolo. New cybersecurity rules land for Defense Department contractors // The Register***

(https://www.theregister.com/2025/09/09/new_cybersecurity_compliance_rules_dod/). 09.09.2025).

***

«Федеральний уряд стверджує, що в результаті кібератаки було отримано доступ до адрес електронної пошти та номерів телефонів осіб, пов'язаних з обліковими записами Податкового агентства Канади, Агентства зайнятості та соціального розвитку Канади та Агентства прикордонної служби Канади.

Секретаріат Ради казначейства Канади повідомляє, що уряд був повідомлений про кіберінцидент 17 серпня компанією 2Keys Corporation, постачальником застосунку для багатофакторної автентифікації, що використовується для облікових записів.

Уряд стверджує, що корпорація 2Keys виявила інцидент, негайно повідомила уряд і розпочала розслідування, яке проводиться за участю зовнішніх експертів з кібербезпеки.

Рада казначейства стверджує, що планове оновлення програмного забезпечення спричинило «вразливість», яка дозволила зловмиснику отримати доступ до номерів телефонів, пов’язаних з обліковими записами CRA та ESDC, а також до адрес електронної пошти, пов’язаних з обліковими записами CBSA, що стосуються людей, які користувалися послугою автентифікації між 3 та 15 серпня.

Уряд стверджує, що актор надсилав спам-повідомлення на деякі номери телефонів із посиланням на веб-сайт, оформлений під виглядом веб-сайту уряду Канади.

Рада фінансів США повідомляє, що послугу багатофакторної автентифікації відновлено, і немає жодних ознак розкриття будь-якої додаткової ідентифікованої особистої інформації або конфіденційних персональних даних». ***(Catherine Morrison. Federal government says emails, phone numbers accessed in cyberattack // CHEK Media (https://cheknews.ca/federal-government-says-emails-phone-numbers-accessed-in-cyberattack-1277085/). 09.09.2025).***

***

«Сенатор США Рон Вайден закликав Федеральну торгову комісію (FTC) розпочати розслідування щодо компанії Microsoft, стверджуючи, що «груба недбалість у сфері кібербезпеки» з боку компанії ставить під загрозу національну безпеку та сприяє атакам програм-вимагачів на критичну інфраструктуру. У листі від 10 вересня Вайден звинуватив незахищені налаштування Windows за замовчуванням, посилаючись на те, що Microsoft продовжує підтримувати застарілий протокол шифрування RC4, у тому, що це призвело до таких інцидентів, як атака програм-вимагачів у травні 2024 року на оператора лікарень Ascension, в результаті якої були викрадені конфіденційні дані 5,6 мільйона пацієнтів після того, як підрядник натиснув на шкідливий результат пошуку Bing, що в кінцевому підсумку дозволило хакерам отримати доступ до сервера Microsoft Active Directory Ascension… Вайден порівняв Microsoft з «підпалювачем, який продає послуги з пожежогасіння» і стверджував, що її майже

монопольне становище змушує урядові установи та підприємства покладатися на її продукти. FTC підтвердила отримання листа, але не надала жодних коментарів. Microsoft відповіла, що RC4 зараз становить менше 0,1 % її трафіку і буде вимкнено за замовчуванням у деяких продуктах Windows на початку 2026 року, хоча, за її словами, більш раннє вимкнення порушило б роботу багатьох систем клієнтів…» ***(AJ Vicens. US Senator Wyden pushes FTC to investigate Microsoft for 'gross cybersecurity negligence' // yahoo! finance (https://finance.yahoo.com/news/us-senator-wyden-pushes-ftc-181749655.html). 10.09.2025).***

***

«…У зв'язку зі скороченням федеральної підтримки кібербезпеки шкіл законодавці штатів намагаються заповнити цю прогалину. Дослідження Консорціуму шкільних мереж (CoSN) в Арканзасі, Массачусетсі, Орегоні, Пенсільванії та Техасі показало, що тільки в цих п'яти штатах у 2025 році було обговорено 18 законопроектів, безпосередньо спрямованих на захист систем K-12 від кібератак; сім з них вже стали законами. Нові заходи варіюються від створення в Техасі державного «Кіберкомандування», яке буде навчати шкільний персонал, до вимоги Арканзасу, щоб його страховий департамент пропонував кіберстрахування округам і фінансував команду реагування на кібератаки. Загалом п'ять штатів розглянули 61 додатковий законопроект, який опосередковано стосується цього питання, наприклад, ініціативи з розвитку робочої сили та скоординовані плани реагування на інциденти. Огайо, хоча і не входить до вибірки CoSN, нещодавно прийняв один з найсуворіших у країні законів про кібербезпеку в школах, який вимагає розробки планів безпеки округів, оперативного повідомлення про порушення та затвердження місцевою радою перед будь-якою виплатою викупу. Ці зусилля штатів з'явилися саме тоді, коли адміністрація Трампа скасувала кілька федеральних програм підтримки, зокрема консультативну групу з кібербезпеки в секторі освіти, програми K-12 в рамках Центру обміну та аналізу інформації між штатами та центр технічної допомоги з питань готовності та управління надзвичайними ситуаціями для шкіл. Округи не готові самостійно нести цей тягар: 61 % не мають спеціальних бюджетів на кібербезпеку, а 44 % передають ключові функції захисту на аутсорсинг. Прихильники попереджають, що за відсутності федерального керівництва у боротьбі з дедалі більш витонченими іноземними та внутрішніми зловмисниками, розширення «кібербезпекового розриву» залишить бідні на ресурси штати та шкільні системи незахищеними, навіть якщо інші будуть просуватися вперед, застосовуючи інноваційні, двопартійні засоби захисту…» ***(Alyson Klein. States Struggle to Fill K-12 Cybersecurity Gaps Left by Federal Cuts // e.Republic LLC (https://www.govtech.com/education/k-12/states-struggle-to-fill-k-12-cybersecurity-gaps-left-by-federal-cuts). 10.09.2025).***

***

«Палата представників у середу ухвалила законопроект про оборонну політику на суму 848 мільярдів доларів, який містить кілька положень щодо кібербезпеки та штучного інтелекту.

Члени парламенту проголосували 231 голосом проти 196 за схвалення версії Закону про національні оборонні повноваження (NDAA) , яка визначає політику Пентагону на рік, розробленої палатою.

Текст дорожньої карти політики щодо цифрової безпеки виглядає помірковано порівняно з останніми двома роками, коли в дебатах домінувала ідея вивчення кіберсил США.

Ось основні моменти:

- Законопроект вимагає від Адміністрації національної безпеки (NSA) надавати брифінг щодо своїх планів щодо Центру координації кібербезпеки. Він також просить усі об'єднані бойові командування щорічно подавати законодавцям звіти про «достатність підтримки», яку їм надає Кіберкомандування США.
- Створення «програмного переліку матеріалів» для технологій на базі штучного інтелекту, що використовуються Міністерством оборони.
- Ці заходи дозволяють Пентагону створити «до 12 генеративних напрямків зусиль у сфері штучного інтелекту» для того, щоб штучний інтелект міг покращити зусилля департаменту в галузі кібербезпеки, збору та аналізу розвідувальних даних.
- Поправка до законопроекту, яку було прийнято під час дебатів у палаті, дозволить NSA ділитися розвідувальними даними про загрози з приватним сектором для посилення цифрової безпеки в телекомунікаційному секторі США.
- Ще одна поправка вимагатиме від Міністерства оборони США вивчити роль Національної гвардії у реагуванні на кіберінциденти на федеральному та державному рівнях, зокрема, як служба може покращити власні можливості реагування.
- Дві основні поправки, які залишилися на розгляді, були запропоновані головою Комітету внутрішньої безпеки Палати представників Ендрю Гарбаріно (республіканець від штату Нью-Йорк), які мали б поновити Закон про обмін інформацією з кібербезпеки 2015 року та Програму грантів на кібербезпеку штатів та місцевих органів влади. Термін дії обох поправок, які минулого тижня схвалила комісія Гарбаріно , закінчується 30 вересня без прийняття рішень Конгресом…» ***(Martin Matishak. House moves ahead with defense bill that includes AI, cyber provisions // Recorded Future News (https://therecord.media/house-passes-defense-policy-bill-ai-cyber). 10.09.2025).***

***

«…Дженніфер Квейд, виконавчий директор Canadian Cyber Threat Exchange (CCTX), відстоює модель «поділися тим, що працює», яка ставить людей на перше місце і розглядає стійкість як командний вид спорту, а спільноту — як критичну інфраструктуру. Очолюючи майже десятирічну некомерційну організацію, що налічує понад 200 компаній з 16 секторів, які представляють 1,5 мільйона співробітників, вона зосереджує CCTX на подоланні ізольованості та перетворенні важко здобутих уроків на спільні активи. Хоча CCTX надає портали, відібрані звіти та канали індикаторів, його серцевиною є щотижневі дзвінки між колегами, під час яких члени відкрито обмінюються TTP, заходами щодо зменшення ризиків та посібниками в режимі реального часу — підхід, який

базується на довірі, дисциплінованому перекладі знань та співпраці конкурентів проти спільних супротивників… Квейд стверджує, що кібербезпека повинна перейти від IT до корпоративних ризиків, а керівники служб інформаційної безпеки (CISO) повинні стати основними лідерами у сфері ризиків, які перетворюють технічні реалії на бізнес-рішення. Справжня стійкість вимірюється швидкістю та якістю відновлення, а не відсутністю інцидентів, і залежить від розумних інвестицій у людей, процеси, інструменти та мережу, на яку можна покластися. Мотивована метою та щедрістю спільноти, а не гламуром, вона закликає практиків будувати міжгалузеві відносини, проявляти активність та ділитися досвідом, оскільки атаки та заходи щодо їхнього запобігання стосуються всіх галузей. Для новачків сертифікація може відкрити нові можливості, але просування по кар'єрних сходах залежить від глибини технічних знань і чіткого усвідомлення ризиків. Для майбутніх лідерів важливо приділяти пріоритетну увагу комунікації, інституціоналізації досвіду, наставництву та пошуку тих, хто вже вирішив подібну проблему. Типовий дзвінок до CCTX може усунути «сліпі зони» за годину, підкреслюючи, що цінність полягає не тільки в самих показниках, а й у судженнях членів про те, «що варто робити далі»… Її заключне повідомлення є одночасно імперативним і запрошенням: жодна організація не може зробити це самостійно; прийміть коаліційний підхід, підніміть кібербезпеку до рівня функції ризику та оцінюйте стійкість за тим, наскільки добре ви реагуєте…» ***(Francois Guay. Collaborative power in action: Jennifer Quaid and the future of cybersecurity in Canada // Postmedia Network Inc. (https://calgaryherald.com/technology/tech-news/collaborative-power-in-action-jennifer-quaid-and-the-future-of-cybersecurity-in-canada). 11.09.2025).***

***

«…CISA підтвердила свою прихильність до програми Common Vulnerabilities and Exposures (CVE), а керівник з питань кібербезпеки Нік Андерсен наголосив на необхідності створення спільної «карти» вразливих місць, які можна експлуатувати, щоб допомогти захисникам випередити супротивників. Програма, створена понад 25 років тому і спонсорована DHS через Національний відділ кібербезпеки (NCSD) CISA, керується Радою CVE і адмініструється MITRE. Після невизначеності щодо продовження підтримки, CISA в останній момент прийняла рішення про фінансування програми до березня 2026 року, зобов'язавшись зберегти дані CVE безкоштовними та відкритими для доступу, а також забезпечити безконфліктне, незалежне від постачальників управління з широким, прозорим та підзвітним керівництвом. Для зміцнення CVE CISA планує прискорити технічну модернізацію; розширити представництво міжнародних урядів, наукових кіл, постачальників інструментів, споживачів даних, дослідників у галузі безпеки, операційних технологій та спільнот з відкритим кодом; а також врахувати відгуки світової спільноти при розробці програми. Агентство також вивчає можливості диверсифікації фінансування та об'єднання механізмів збагачення даних, таких як Vulnrichment та функція Authorized Data Publisher, одночасно шукаючи підтримку з боку промисловості та міжнародних урядів для поліпшення повноти, точності та своєчасності записів CVE, особливо в

умовах триваючого відновлення NVD після періоду уповільнення. Згідно зі своїм стратегічним документом, CISA планує в майбутньому підвищити якість, вдосконалити схему CVE та інтегрувати автоматизацію, машинне навчання та штучний інтелект…» ***(Zeljka Zorz. CISA looks to partners to shore up the future of the CVE Program // Help Net Security (https://www.helpnetsecurity.com/2025/09/12/cisa-cve-program-future/). 12.09.2024).***

***

«…Управління урядової відповідальності (GAO) повідомляє, що Міністерство охорони здоров'я та соціальних служб США (HHS) ще не впровадило 82 рекомендації «високого ризику» щодо кібербезпеки та управління IT, принаймні 37 з яких є конфіденційними, спрямовані до головного інформаційного директора міністерства та інформаційних директорів на рівні підрозділів. Відкриті питання охоплюють кібербезпеку та придбання/управління IT, включаючи встановлення графіка прийняття цифрових форм доступу та згоди, їх розміщення на сайті HHS, повне виконання вимог Управління з питань управління та бюджету щодо реєстрації подій, поліпшення обробки цифрових записів та моніторингу мережі, а також завершення інвентаризації пристроїв Інтернету речей на підприємстві… GAO попереджає, що доки ці заходи не будуть вжиті, HHS ризикує неналежним розкриттям записів, неповним реєструванням для виявлення та усунення загроз, а також поганою видимістю активів IoT. HHS заявляє, що посилює системи під керівництвом CIO Кларка Мінора, який приєднався до компанії в лютому і став CIO в травні, посилаючись на стабільний прогрес. Останнє попередження є продовженням аналогічного звіту від листопада 2024 року і не уточнює, чи були закриті раніше позначені питання, включаючи ініціативи щодо відстеження заходів з мінімізації наслідків від програм-вимагачів. Зовнішні експерти з CHIME та HIMSS наголошують, що як розпорядник даних у Medicare, Medicaid, NIH, FDA, IHS, CDC та ASPR, а також як агентство з управління ризиками в секторі, HHS має подавати приклад; бездіяльність підвищує ризики від крадіжки особистих даних та шахрайства до загроз національній безпеці, порушення операційної діяльності та підриву довіри громадськості, тоді як усунення прогалин сприятиме підвищенню стійкості та захисту даних пацієнтів…» ***(Marianne Kolbasuk McGee. GAO Report Spotlights Unaddressed HHS Cyber, IT Concerns // Information Security Media Group, Corp. (https://www.databreachtoday.co.uk/gao-report-spotlights-unaddressed-hhs-cyber-concerns-a-29436). 12.09.2025).***

***

«Згідно з аудитом, опублікованим у четвер, Агентство з кібербезпеки та безпеки інфраструктури (CISA) неналежним чином управляло фондом, призначеним для допомоги у збереженні працівників у сфері кібербезпеки.

Згідно зі звітом генерального інспектора Міністерства внутрішньої безпеки (DHS), CISA «належним чином не розробила, не впровадила, не виконала та не керувала» вимогами до своєї програми стимулювання утримання працівників у сфері кібербезпеки.

З 2020 по 2024 рік CISA виплатила понад 138 мільйонів доларів США у вигляді кіберстимулів. Аудитори не змогли розібратися, як були витрачені всі ці кошти, оскільки Управління головного директора з управління персоналом (OCHCO) CISA «не вело облік одержувачів кіберстимулів та відповідних виплат», йдеться у звіті.

У звіті йдеться, що офіс генерального інспектора зміг виявити сумнівну заборгованість із заробітної плати 348 співробітникам на суму 1,4 мільйона доларів.

У звіті йдеться, що агентство не змогло належним чином визначити, хто має право на отримання стимулів, і платило працівникам, які не мали «критично важливих» навичок у сфері кібербезпеки, від 21 000 до 25 000 доларів США на рік.

Згідно зі звітом, агентство не дотрималося численних федеральних правил під час реалізації програми стимулювання.

«Ці проблеми виникли через те, що CISA розширила вимоги до участі в програмі, не створивши детальних процесів і процедур впровадження, і не здійснила централізованого управління програмою», – йдеться у звіті…

Управління CISA погодилося з усіма 8 рекомендаціями генерального інспектора щодо вирішення проблеми, повідомило відомство. Серед них – доручення директору CISA створити програму відстеження одержувачів кіберстимулів, щорічно перевіряти право працівників на отримання пільг та вивчати, чи може відомство відшкодувати вже здійснені помилкові платежі...» ***(Suzanne Smalley. DHS inspector general: CISA mismanaged multimillion-dollar employee incentives program // Recorded Future News (https://therecord.media/cisa-cybersecurity-retention-incentives-dhs-ig-audit). 12.09.2025).***

***

«15 серпня конгресмен Девід Швейкерт представив законопроект HR 4988, «Закон про санкціонування боротьби з шахрайськими фермами та репресалій», який дозволить президенту видавати приватним компаніям каперські листи для переслідування кіберзлочинців за кордоном, фактично санкціонуючи «активну оборону» та операції з хакерського відплати там, де правоохоронні органи не можуть вжити заходів. Цей захід дозволяє приватним суб'єктам «застосовувати всі розумно необхідні засоби» для затримання осіб або конфіскації майна за кордоном і надає їм екстериторіальний імунітет від судового переслідування в США, хоча він не забезпечує захисту згідно із законодавством країн, в яких проводяться операції. Хоча законопроект навряд чи буде прийнятий, він свідчить про зростаючий інтерес Вашингтона до агресивних, напівприватизованих кібероперацій і ще більше розмиває межу між діями держави та корпорацій…

Критики попереджають, що така необмежена влада може зірвати міжнародну поліцейську роботу, перешкодити розвідувальним операціям і спровокувати дипломатичні суперечки. Наприклад, приватна операція з виведення з ладу може призвести до збою сервера, який канадські або європейські слідчі таємно моніторять, що сповістить підозрюваних і поставить під загрозу більш масштабну, скоординовану операцію з арешту. Наступальні кіберкампанії зазвичай

обмежуються військовими або розвідувальними агентствами, такими як Канадська служба безпеки комунікацій, оскільки вони вимагають суворого нагляду та складного усунення конфліктів. HR 4988 обходить цю структуру, дозволяючи президенту самостійно визначати цілі та визначаючи «злочинну організацію» досить широко, щоб включити іноземні держави…

Ця пропозиція з'явилася в той час, коли великі технологічні компанії обговорюють ідею створення корпоративних підрозділів з протидії зловмисникам: на нещодавній конференції Google оголосив про створення «підрозділу з протидії зловмисникам», який буде попереджувально ліквідовувати інфраструктуру, що становить загрозу. Прихильники стверджують, що такі ініціативи стримуватимуть зловмисників і заповнять прогалину, створену повільними діями уряду; противники заперечують, що без чітких правил і міжнародної координації приватні удари можуть бути помилково сприйняті як злочинна діяльність, спровокувати помсту і підірвати і без того крихкі кібернорми. Навіть якщо H.R. 4988 застрягне, дискусія, яку він викликає, показує, як швидко кіберполітика США схиляється до приватизованих, наступальних дій…» ***(Alexander Rudolph. Will the next cyber threat actors be American corporations? // (https://www.digitaljournal.com/tech-science/will-the-next-cyber-threat-actors-be-american-corporations/article). 13.09.2025).***

***

«Зараз конфіденційність та кібербезпека є одними з головних ризиків для канадських організацій, але занадто часто вони залишаються ізольованими технічними проблемами; ради директорів, які не в змозі впоратися з цими ризиками, наражаються на репутаційні збитки, розслідування з боку регуляторних органів, критику інвесторів та порушення операційної діяльності. Очікування щодо нагляду з боку ради директорів зростають, оскільки регуляторні органи посилюють контроль, страхові компанії перевіряють управління, протоколи реагування та освіту ради директорів, а інституційні інвестори оцінюють управління ризиками, пов'язаними з даними, в рамках ESG… З огляду на частоту та вплив інцидентів, ради директорів та керівництво повинні надавати пріоритет чіткій відповідальності на рівні ради директорів (головний директор або комітет та кібербезпека як постійний пункт порядку денного з регулярними брифінгами), корпоративному управлінню, яке виходить за межі IT і поширюється на юридичні питання, дотримання нормативних вимог, управління персоналом, ризики та комунікації, плануванню сценаріїв та моделюванню з керівниками та зовнішніми консультантами для виявлення прогалин, а також надійній прозорості та розкриттю інформації в комунікаціях щодо інцидентів, звітах ESG та матеріалах для інвесторів, щоб уникнути неправдивих тверджень. Постійне навчання членів ради директорів та зовнішній бенчмаркінг мають важливе значення. Ради директорів, які беруть на себе відповідальність за захист конфіденційності та кібербезпеку, зміцнюють стійкість, зменшують ризики та формують довіру — що на сьогодні є основним обов'язком відповідального корпоративного управління…» ***(Hélène Deschamps Marquis. Privacy and cybersecurity are no longer IT issues, they are board issues // Borden Ladner Gervais LLP (https://www.blg.com/en/insights/perspectives/12-strategic-priorities-for-privacy-***

cybersecurity-and-ai-risk-management/privacy-and-cybersecurity-are-no-longer-it-issues-they-are-board-issues). 10.09.2025).

***

«…Новий звіт Канадської мережі кібербезпеки (CCN) попереджає, що найнагальнішою цифровою вразливістю Канади більше не є викрадені паролі чи витік корпоративних даних, а системи операційних технологій (OT), які забезпечують функціонування критичної інфраструктури країни. Ці промислові системи управління забезпечують роботу електромереж, трубопроводів, автоматизують роботу шахт, регулюють очищення води, керують залізничним рухом та забезпечують функціонування обладнання лікарень. У міру злиття традиційних IT-мереж з OT, один фішинговий лист або штам програм-вимагачів може зупинити розподіл палива, затримати операції або залишити регіони без електроенергії. У 2024 році 73 % зареєстрованих кіберінцидентів у Канаді сталися в середовищах OT, що на 49 % більше, ніж у попередньому році…

Інші країни — США, Велика Британія та Німеччина — вже фінансують національні стратегії OT, проте Канада все ще не має обов'язкової правової бази. Законопроект C-8 (Закон про захист критичних кіберсистем) накладає обов'язкові зобов'язання з безпеки на операторів енергетики, телекомунікацій, банківської справи та транспорту, що регулюються на федеральному рівні, але досі не прийнятий. Тим часом багато заводів використовують застаріле обладнання без оновлень, а невеликі комунальні підприємства часто не мають ані бюджету, ані досвіду для захисту. Канада також не має національного реєстру активів OT, що ускладнює будь-які скоординовані заходи реагування…

Секторальна вразливість є значною: оператори енергомереж щодня стикаються з 60 новими вразливостями; лікарні зазнають атак на системи опалення, вентиляції та кондиціонування повітря, а також хірургічні прилади; віддалені гірничодобувні установки, порти, залізниці, аеропорти і навіть світлофори в «розумних» містах є частими цілями атак. Основні рекомендації звіту полягають у модернізації інфраструктури з урахуванням принципів безпеки при проектуванні; інтеграції команд з IT- та OT-безпеки; відкритому обміні інформацією про загрози; та прискоренні розвитку навичок для наступного покоління кіберзахисників. CCN робить висновок, що без рішучих дій атаки програм-вимагачів та державні спроби проникнення в критичну інфраструктуру «майже напевно» продовжаться, загрожуючи не тільки грошам, а й життю людей та довірі громадськості. Захист OT, як стверджується у звіті, зараз є надзвичайно важливим для економічної стійкості, безпеки та способу життя Канади…» ***(Charlie Tsao. Keeping the lights on: Canada's OT cybersecurity wake-up call // Postmedia Network Inc. (https://financialpost.com/technology/tech-news/keeping-the-lights-on-canadas-ot-cybersecurity-wake-up-call). 17.07.2025).***

***

«…Федеральні агентства США опинилися в пастці парадоксу кібербезпеки: обсяг і складність атак стрімко зростають, тоді як засоби безпеки, призначені для боротьби з ними, генерують більше телеметричних

даних, ніж команди можуть зберігати, об'єднувати або собі дозволити. Впровадження хмарних технологій, Інтернету речей та генеративної штучної інтелекту, а також більш суворі вимоги до дотримання нормативних вимог призвели до стрімкого зростання витрат на управління даними, проте бюджети та штатні одиниці скорочуються. Щоб подолати цю прірву, агентства повинні перейти на модель, орієнтовану на штучний інтелект та дані, яка може обробляти інформацію про безпеку зі швидкістю машини та діяти на її основі… Важливими є три кроки: (1) віддавати перевагу платформам, розробленим на основі вбудованого штучного інтелекту, а не застарілим продуктам з додатковими аналітичними функціями, щоб забезпечити їхню здатність розвиватися відповідно до майбутніх загроз; (2) картографувати та пріоритезувати всі дані безпеки, фільтруючи або збагачуючи їх на верхньому рівні, щоб уникнути зайвих витрат на зберігання, створюючи при цьому єдиний практичний огляд; та (3) ретельно перевіряти «безкоштовні» або вбудовані в пакети додатки безпеки, які можуть заощадити гроші на початку, але становлять ризик для виконання місії, якщо їхні можливості відстають. При правильному застосуванні ця стратегія забезпечує єдину видимість, звільняє агентства від залежності від застарілих інструментів і значно скорочує витрати на дані завдяки інтелектуальному об'єднанню, фільтруванню та недорогому гарячому зберіганню. Такі постачальники, як SentinelOne та його партнерство з AWS, ілюструють цей підхід: хмарна архітектура, виявлення та реагування на основі штучного інтелекту, інтеграція з такими сервісами, як GuardDuty та Security Lake, а також локальні опції для секретних робочих навантажень. Застосовуючи захист на основі штучного інтелекту та даних, урядові лідери можуть створити більш стійкий та ефективний захист навколо критично важливих активів країни…» ***(Andrew Howell. Drowning in security data: Why federal cybersecurity demands an AI-first future // FedScoop (https://fedscoop.com/drowning-in-security-data-why-federal-cybersecurity-demands-an-ai-first-future/). 19.09.2025).***

***

«На піку свого впливу Департамент урядової ефективності (DOGE) епохи Трампа працював з імпровізованої штаб-квартири, яку сенатори-демократи описували як хаотичну і небезпечну, з озброєною охороною, імпровізованими житловими приміщеннями і навіть дитячими іграшками, розкиданими по всьому приміщенню. У новому звіті демократів DOGE звинувачується в необережному поводженні з найбільш конфіденційними особистими даними американців, з посиланням на свідчення інформаторів про те, що департамент мав «безперешкодний доступ» до записів соціального страхування і завантажував їх на хмарні сервери, що не мали перевірених засобів контролю безпеки, створюючи гострий ризик серйозного порушення безпеки даних. Інформатори також стверджували про нерегулярні спроби передати дані соціального страхування до Міністерства внутрішньої безпеки поза звичайними каналами…

Окрім проблем із безпекою даних, у звіті описано безлад у роботі: молоді помічники живуть і працюють у тісних умовах, іноді підключають кілька ноутбуків до мереж Starlink, які захищають їхню діяльність, і часто працюють у різних

агентствах без постійного нагляду. Коли слідчі Конгресу спробували дізнатися більше, вони зіткнулися з постійним ухиленням від відповідей — агентства не могли або не хотіли вказати, які проекти DOGE реалізуються або навіть які співробітники до них приписані. Запити про надання інформації часто ігнорувалися взагалі…

Висновок демократів є двояким: DOGE поставив під загрозу дані американців, обійшовши основні заходи безпеки, а його таємнича, незрозуміла структура практично унеможливила ефективний контроль з боку Конгресу. За їхніми словами, департамент поставив під загрозу конфіденційну особисту інформацію, «тоді як його співробітники працюють в умовах секретності, що захищає їх від ефективного контролю та відповідальності». ***(Karoun Demirjian and Nicholas Nehamas. Democratic Report Says Disorder at DOGE Jeopardized Americans' Data // The New York Times Company (https://www.nytimes.com/2025/09/25/us/politics/democratic-report-disorder-doge.html). 25.09.2025).***

***

«…Військово-повітряні сили розробляють новий план кампанії з оборонних операцій у кіберпросторі (DCO), спрямований на захист американських баз та комунальних служб, що їх підтримують, від дедалі більш витончених цифрових загроз, особливо тих, що пов'язані з Китаєм. Генерал-лейтенант Томас Хенслі, командувач 16-ї повітряної армії/повітряних сил кібербезпеки, попередив, що групи, пов'язані з Пекіном, такі як Volt Typhoon і Salt Typhoon, протягом багатьох років таємно утримують позиції в американських мережах водопостачання, енергетики, транспорту та телекомунікацій — доступ, який, на його думку, призначений для «руйнівних кібератак» у разі виникнення конфлікту навколо Тайваню. Такі удари по критичній внутрішній інфраструктурі, за його словами, призведуть до «тотальної війни» у всіх сферах…

Хенслі навів як доказ того, що атаки на операційні технології (OT) можуть безпосередньо впливати на умови на полі бою, саботаж іранських центрифуг вірусом Stuxnet та синхронізовані кібер- та кінетичні атаки Росії на Україну. Він додав, що американські об'єкти зазвичай розраховані на ракети, а не на шкідливе програмне забезпечення, проте більшість з них можуть працювати на резервних генераторах лише тиждень-два, якщо місцеві комунальні служби будуть виведені з ладу…

Щоб подолати цю прогалину, ВПС США тісніше об'єднають свої дві основні кіберсили: постачальників послуг з кібербезпеки під егідою 688-го кібервійськового крила, які цілодобово здійснюють моніторинг мережі та реагують на інциденти, та команди кіберзахисту під егідою 67-го кібервійськового крила, які проводять глибоке «точкове» вистежування та усунення загроз. Майбутній план кампанії поєднає постійний моніторинг із заходами швидкого реагування, підкріпленими єдиною стратегією використання датчиків і даних…

Оскільки бази залежать від цивільних мереж, служба також укладає угоди про спільні дослідження та розробки (CRADA) з комунальними підприємствами в ключових місцях. Ці угоди охоплюють широкий спектр питань — від обміну

розвідданими про діяльність супротивника до спільного розгортання датчиків ВПС всередині комунальних мереж — завдання, яке часто виконують підрозділи Національної гвардії, що мають необхідні повноваження на території країни…» ***(Jon Harper. Air Force cyber leader warns threats like Volt Typhoon could enable China to wage 'total war' against US // defensescoop (https://defensescoop.com/2025/09/23/volt-typhoon-china-us-air-force-cyber-defensive-operations/). 23.09.2025).***

***

«Новий звіт від RS, глобального постачальника продуктів і послуг для промислових клієнтів, виявляє тривожні прогалини в обізнаності та підготовці американських працівників у сфері кібербезпеки. Дослідження, в якому взяли участь 1000 співробітників різних галузей промисловості США, показало, що чверть (26%) працівників ніколи не проходили навчання з кібербезпеки від свого роботодавця, включаючи інструктаж щодо спроб хакерських атак і фішингових шахрайств…

Дослідження виявило поширену ризиковану поведінку серед співробітників: майже половина (46%) використовує один і той самий пароль на декількох платформах, а 31% зберігає паролі на робочих пристроях або в блокнотах. Інші поширені порушення безпеки включають залишення робочих місць без блокування комп'ютерів (28%), уникнення двофакторної аутентифікації (26%), несвоєчасне оновлення програмного забезпечення (25%) та використання паролів, що містять особисту інформацію, таку як імена або дати народження (24%). Крім того, 20% працівників використовували незахищені джерела Wi-Fi або натискали на посилання з неперевірених джерел, 18% відкривали документи з неперевірених джерел, а 9% надсилали конфіденційні дані неправильним адресатам.

Опитування показало, що третина американців (32%) вважають себе нейтральними або непідготовленими до загроз кібербезпеки. Дані також підкреслили поширеність використання особистих пристроїв для робочих цілей: 72% співробітників, ймовірно, використовують свої особисті пристрої для роботи. Ця тенденція особливо виражена серед молодих працівників віком 16-24 роки (78%) порівняно з тими, хто старше 55 років (60%).

Дистанційна робота створює додаткові вразливості, оскільки понад половина (62%) американців не використовують брандмауер під час роботи з дому, а менше третини (32%) підключаються до робочої VPN. Ці висновки підкреслюють розширення спектру загроз у міру того, як політика роботи з дому та використання власних пристроїв (BYOD) стає все більш поширеною…» ***(US employees 'unprepared' for cybersecurity threats - New Study // Cision US Inc. (https://www.prweb.com/releases/us-employees-unprepared-for-cybersecurity-threats---new-study-302560203.html). 19.09.2025).***

***

«…Зіткнувшись з дефіцитом майже 20 000 фахівців у галузі кібербезпеки — частина загальнонаціонального дефіциту, який оцінюється в 700 000 осіб — Міністерство оборони США поспішає оптимізувати процес найму, прагнучи

скоротити час заповнення вакансій у сфері кібербезпеки з нинішніх 70 днів у середньому до всього 25 днів… Марк Горак, який керує 245 000 співробітників кібербезпеки Міністерства оборони, заявив, що нова мета буде базуватися на наймі на основі навичок, а не на традиційних вимогах щодо ступеня, сертифікації або стажу роботи. Кандидати будуть доводити свою компетентність за допомогою 30-хвилинних оцінювань «кібердіапазону», які перевіряють реальні завдання… У зв'язку з швидким розвитком штучного інтелекту та інших технологій, міністерство кожні 90 днів оновлює посадові інструкції та вимоги до знань, навичок, умінь і завдань, а також заохочує співробітників до ширшого використання інструментів штучного інтелекту. Горак, який зараз очолює новостворене Управління з питань кіберакадемічної взаємодії, підкреслив, що для подолання дефіциту талантів необхідна тісна співпраця з промисловістю, науковими колами та іншими урядовими партнерами, незважаючи на обмеженість фінансування та ресурсів, оскільки «для вирішення наших завдань нам потрібні промисловість, наукові кола, цивільне населення та військові». ***(Greg Otto. DOD official: We need to drop the cybersecurity talent hiring window to 25 days // cyberscoop (https://cyberscoop.com/dod-cyber-workforce-hiring-25-days-mark-gorak-fedtalks/). 19.09.2025).***

***

Країни ЄС та Великобританія

«Хоча NIS2, оновлена Директива Європейського Союзу з кібербезпеки, набула чинності в жовтні 2024 року, багато організацій досі мають труднощі з дотриманням вимог. Станом на липень 2025 року лише 14 з 27 держав-членів ЄС імплементували цю директиву в національне законодавство. І, хоча NIS2 є регламентом ЄС, багато британських компаній, які вже ведуть діяльність в ЄС, можуть зіткнутися зі штрафами або потенційними юридичними наслідками за невиконання вимог.

NIS2 спочатку було запроваджено для посилення безпеки «життєво важливих послуг», зокрема таких галузей, як транспорт, фінансові послуги та енергетика. Для цих галузей, які часто мають застарілі системи та розподілену інфраструктуру, захист від кібератак залишається значним викликом.

Хоча NIS2, оновлена Директива Європейського Союзу з кібербезпеки, набула чинності в жовтні 2024 року, багато організацій досі мають труднощі з дотриманням вимог. Станом на липень 2025 року лише 14 з 27 держав-членів ЄС імплементували цю директиву в національне законодавство. І, хоча NIS2 є регламентом ЄС, багато британських компаній , які вже ведуть діяльність в ЄС, можуть зіткнутися зі штрафами або потенційними юридичними наслідками за невиконання вимог.

NIS2 спочатку було запроваджено для посилення безпеки «життєво важливих послуг», зокрема таких галузей, як транспорт, фінансові послуги та енергетика. Для цих галузей, які часто мають застарілі системи та розподілену інфраструктуру, захист від кібератак залишається значним викликом…

Бізнес може спокуситися розглядати NIS2 як виснажливу процедуру «перевірки відповідності». Але NIS2 слід розглядати як значну можливість: каталізатор для бізнесу, який допоможе йому зміцнити свою позицію в галузі кібербезпеки та забезпечити майбутнє своєї діяльності.

Подолання розриву у відповідності може здатися складною перспективою для IT-стратегів, які вже перебувають під тиском прийняття важливих рішень щодо впровадження та інтеграції нових технологій на тлі буму штучного інтелекту . Однак такі рішення, як платформи безпеки ідентифікаційних даних, можуть допомогти полегшити цей тиск, надаючи IT-лідерам комплексний огляд усього ланцюга поставок.

Ці інструменти ідентифікації є важливими для компаній, яким потрібно контролювати та керувати складними дозволами доступу, включаючи дозволи третіх сторін, з більшою точністю та контролем. В умовах, коли успіх бізнесу дедалі більше залежить від цифрових послуг, автоматизовані засоби контролю ідентифікації та доступу повинні бути основою стратегії кібербезпеки кожної організації». ***(Steve Bradford. Why are so many organizations dragging their feet on NIS2 compliance? // Future US, Inc. (https://www.techradar.com/pro/why-are-so-many-organizations-dragging-their-feet-on-nis2-compliance). 04.09.2025).***

***

«У Північно-Східній Англії запускається нова програма навчання, яка допоможе вирішити проблему зростаючого дефіциту фахівців з кібербезпеки.

Кібербезпека залишається однією з найбільш затребуваних галузей технологій у Великобританії, а попит на кваліфікованих фахівців за останні два роки зріс більш ніж удвічі.

Однак багато малих і середніх підприємств стикаються з проблемами при наймі та навчанні персоналу, враховуючи необхідність володіння спеціальними знаннями.

У відповідь на це, PlanBEE Cyber, створена Gateshead College за підтримки CyberNorth, запрошує регіональних роботодавців взяти участь у формуванні майбутніх талантів для цього швидкозростаючого сектору.

Ініціатива базується на успіху оригінальної програми навчання PlanBEE, вперше запущеної в 2016 році, яка стала піонером у створенні моделі навчання під керівництвом роботодавців.

На відміну від традиційних програм навчання, за словами офіційних представників, PlanBEE Cyber дозволяє учням чергуватися між декількома підприємствами, забезпечуючи широку і практичну базу в галузі.

Вони додають, що модель спільного навчання має на меті усунути бар'єри для малих і середніх підприємств, надаючи їм доступ до фахівців на початку кар'єри, а також надаючи учням навички, необхідні для успішної роботи в різних бізнес-середовищах…» ***(Bdaily Business. Cyber drive launched to plug skills gap // Bdaily (https://bdaily.co.uk/articles/2025/09/04/cyber-drive-launched-to-plug-skills-gap). 04.09.2025).***

***

«…Енергетична трансформація Європи перетворила сонячну енергію на критично важливу інфраструктуру, але швидке децентралізоване зростання цієї технології випередило її захисні механізми. На відміну від старої, централізовано керованої аналогової мережі, сучасна система покладається на тисячі невеликих фотоелектричних станцій, більше половини з яких мають потужність менше 25 МВт кожна, і багато з яких підключають інвертори до загальнодоступного Інтернету для дистанційного моніторингу та оновлення. Слабкі або стандартні паролі та відсутність контролю безпеки роблять ці пристрої легкою здобиччю для хакерів, які можуть маніпулювати виробництвом електроенергії або порушувати роботу мережі.

Регулюючі органи починають реагувати. Загальні правила щодо Інтернету речей, такі як Директива ЄС про радіообладнання (RED) та Закон Великобританії про безпеку інформаційних систем (PSTI), тепер вимагають дотримання таких основних вимог, як унікальні облікові дані та заходи захисту даних. З'являються більш жорсткі інструменти: Закон ЄС про кіберстійкість підвищить планку для всіх виробників підключених пристроїв, а Директива NIS2 покладе юридичну відповідальність за кіберінциденти на власників, операторів і навіть інвесторів у «важливі» послуги, включаючи сонячні батареї, EPC та O&M-компанії. Кілька країн розробляють правила, що стосуються саме сонячної енергетики; Німеччина проводить консультації з представниками галузі, Литва вже ввела суворі обмеження на підключення, а Брюссель планує провести спеціальну оцінку ризиків у фотоелектричній галузі…

Проте залишаються значні прогалини: в ЄС немає загальноєвропейських стандартів, що регулюють спосіб забезпечення безпеки трафіку між пристроями та хмарними сервісами виробниками інверторів, невеликі комунальні підприємства не підпадають під дію правил щодо брандмауерів, а застарілі активи можуть потребувати дорогого модернізування. Доки не будуть прийняті чіткіші нормативні акти, учасники галузі повинні діяти першими. Власники будинків та комерційні користувачі повинні купувати інвертори з надійним шифрованим контролем доступу або додавати до старих пристроїв локальні пристрої управління енергоспоживанням. Власники енергетичних об'єктів повинні провести інвентаризацію всіх компонентів, вимагати від EPC-підрядників та підрядників з експлуатації та технічного обслуговування включення кібербезпекових положень до договорів, а також передбачити в бюджеті кошти на захист апаратного та програмного забезпечення, що виходить за межі простої VPN. Виробники повинні вбудовувати засоби безпеки в дизайн продуктів — QR-коди, обмін криптографічними ключами, аутентифікацію без паролів — при цьому зберігаючи простоту установки…

Висновок очевидний: розглядати кібербезпеку як необов'язкову статтю витрат так само застаріло, як економити на ременях безпеки. З посиленням регуляторного контролю та очікуваним терміном експлуатації фотоелектричних об'єктів протягом десятиліть, забезпечення їхньої надійності вже зараз дозволить уникнути штрафів, відкликань продукції та потенційних катастроф у масштабах енергосистеми в майбутньому». ***(Uri Sadot. The Cybersecurity gap in solar and how***

to close it // pv magazine (https://www.pv-magazine.com/2025/09/05/the-cybersecurity-gap-in-solar-and-how-to-close-it/). 05.09.2025).

***

«…Згідно з повідомленням Агентства з інформаційної безпеки Франції, 3 вересня 2025 року компанія Apple надіслала французьким громадянам чергову серію попереджень про безпеку, що стало четвертою кампанією лише цього року. Попередні хвилі повідомлень були надіслані 5 березня, 29 квітня та 25 червня…

Як пояснює агентство (переклад наш):

«З 2021 року Apple розсилає сповіщення особам, які постраждали від атак шпигунського програмного забезпечення.

Ці інструменти, такі як Pegasus, Predator, Graphite або Triangulation, є особливо складними та їх важко виявити.

Ці складні атаки спрямовані на окремих осіб через їхній статус чи роль: журналістів, юристів, активістів, політиків, високопосадовців, членів комітетів зі стратегічного управління секторами тощо.

Отримання сповіщення означає, що принаймні один із пристроїв, пов'язаних з обліковим записом iCloud, став ціллю атаки та потенційно може бути скомпрометований.

Далі в документі пояснюється, що ці сповіщення надходять через iMessage з перевірених адрес та контактів Apple, і користувачам, які отримали сповіщення, пропонується:

- зв'яжіться https://cert.ssi.gouv.fr/contact) ; швидко (- FR Щоб , CERT з отримати технічну допомогу
- Зберігайте сповіщення електронною поштою, надіслані Apple;
- Уникайте внесення змін до пристрою (скидання налаштувань, видалення програм, оновлення, перезапуску тощо). Ці дії можуть перешкодити розслідуванню.

Також у ньому наведено поширені рекомендації щодо безпеки, такі як не натискати на підозрілі посилання, використовувати надійні та унікальні паролі та вмикати двофакторну аутентифікацію (2FA) «коли це можливо».

Наразі немає жодних подробиць про те, хто стояв за цією конкретною шпигунською кампанією або хто був мішенню, включаючи користувачів за межами Франції». ***(Marcus Mendes. France confirms new Apple spyware campaign alert // 9to5 (https://9to5mac.com/2025/09/11/france-confirms-new-apple-spyware-campaign-alert/). 11.09.2025).***

***

«У звіті Clusit 2025 підкреслюється різке зростання кількості кібератак в Італії за останні п'ять років, причому середня кількість інцидентів на місяць майже подвоїлася з 156 у 2020 році до 295 у 2024 році, а з травня по листопад 2024 року було зафіксовано 1193 випадки, які особливо торкнулися державного управління та університетських досліджень. Ескалація геополітичної напруженості (Росія–Україна, Близький Схід) та поширення

генеративної штучної інтелектуальної системи (AI) призвели до посилення та збільшення кількості атак, зокрема DDoS-кампаній. Зловмисники варіюються від злочинців до хактивістів, таких як Anonymous, причому зростає підозра щодо операцій, що підтримуються державою і спрямовані на дезінформацію, психологічну війну та системний саботаж, що робить Італію однією з країн, які найчастіше стають об'єктом таких атак. Посилений моніторинг з боку Національного агентства з кібербезпеки (ACN) дозволив виявити часті та потенційні цілі, викривши раніше непомічені вторгнення… У звіті кіберзлочинність визначається як експлуатація технічних недоліків і людських помилок, часто за допомогою соціальної інженерії та фішингу; до пов'язаних з цим явищ належать кібертероризм (наприклад, атака іранської кіберармії на Baidu в 2010 році) та кібервійна проти критичної інфраструктури (наприклад, Stuxnet). Шкідливе програмне забезпечення, особливо трояни та програми-вимагачі, залишається основною зброєю, а великі компанії та державні органи є головними цілями через високу вартість втрати даних… Ефективний захист вимагає комплексного управління ризиками: оцінки ризиків, посилення контролю, розгляду можливості страхування від кіберзагроз і, що найважливіше, навчання персоналу — найслабшої ланки. Таким чином, кібербезпека є стратегічним пріоритетом: організації повинні своєчасно виявляти загрози, швидко реагувати на них і мінімізувати збитки, щоб зберегти переваги цифрової трансформації та зміцнити національну безпеку…» ***(Ylenia Minnella. The rise of Cybercrime // LEXIA (https://www.lexia.it/en/2025/09/02/rise-of-cybercrime/). 02.09.2025).***

***

«Перший проект Закону ЄС про космос, оприлюднений 25 червня 2025 року, має на меті зробити європейську космічну галузь чистішою, безпечнішою та конкурентоспроможнішою завдяки трьом основним принципам: безпеці, стійкості та сталості. Безпека стосується зростаючої загрози космічного сміття завдяки вдосконаленому відстеженню та суворішим вимогам щодо утилізації супутників після закінчення терміну експлуатації. Стійкість спрямована на зростаючі ризики кібербезпеки шляхом постійної оцінки ризиків, повідомлення про інциденти та гармонізованих правил для захисту інфраструктури, що залежить від космосу, від кібератак… Сталий розвиток зосереджується на зменшенні впливу на довкілля шляхом оцінки життєвого циклу та інновацій у сфері обслуговування в космосі з метою подовження терміну експлуатації супутників. Щоб подолати розрізнені національні правила, які гальмують інновації та збільшують витрати, закон пропонується як безпосередньо застосовний нормативний акт, що охоплює всі держави-члени ЄС і поширюється на компанії, які не є членами ЄС, але здійснюють діяльність у ЄС… 150-сторінкова пропозиція включає пропорційні вимоги, що залежать від розміру компанії та ризику, а також цільову підтримку для підприємств та урядів під час перехідного періоду. Комісія також опублікувала разом із проектом «Бачення європейської космічної економіки», підкресливши амбіції ЄС стати глобальною космічною потугою…» ***(Louisa Spillman, Phil Merchant. EU Space Act drafted by European***

Commission // Marks & Clerk (https://www.marks-clerk.com/insights/latest-insights/102l1aa-eu-space-act-drafted-by-european-commission/). 03.09.2025).

***

«…вимоги щодо кібербезпеки в Законі ЄС про штучний інтелект, згідно з яким положення щодо високоризикового штучного інтелекту набувають чинності у серпні 2026 року.

Закон ЄС про штучний інтелект, Розділ 2, Статті 9-15 під назвою «Вимоги до систем штучного інтелекту високого ризику» окреслюють вимоги до систем штучного інтелекту високого ризику. Багато з цих вимог призведуть до вдосконалення програми кібербезпеки організації. Зокрема, у Розділі 2 Закону ЄС про штучний інтелект, статті 9-15 вимагають наступного:

- **Стаття 9** зобов'язує постачальників впроваджувати документовані системи управління ризиками, враховуючи потенційні ризики та зловживання за допомогою протоколів тестування.
- **Стаття 10** зосереджена на управлінні даними, вимагаючи протоколів для навчання, валідації та тестування моделей для усунення упередженостей та прогалин у даних.
- **Стаття 11** вимагає технічної документації для забезпечення відповідності перед розміщенням на ринку.
- **Стаття 12** визначає автоматичну реєстрацію подій для систем високого ризику, включаючи час використання, посилання на бази даних та збіги вхідних даних.
- **Стаття 13** наголошує на прозорості, вимагаючи від систем надання чітких інструкцій для користувачів, документуючи точність, надійність та кібербезпеку.
- **Стаття 14** вимагає можливості людського нагляду, що гарантує, що користувачі можуть розуміти, інтерпретувати та контролювати системи штучного інтелекту.
- **Стаття 15** Закону ЄС про штучний інтелект визначає вимоги до систем штучного інтелекту з високим рівнем ризику для забезпечення точності, надійності та кібербезпеки протягом усього їхнього життєвого циклу. Ці системи повинні бути розроблені для досягнення належного рівня точності, заявленого в інструкціях з використання, та бути стійкими до помилок та невідповідностей, що виникають внаслідок взаємодії систем або факторів навколишнього середовища. Надійність можна підвищити за допомогою заходів технічного резервування, таких як резервне копіювання або плани безпеки. Системи, які продовжують навчання після розгортання, повинні враховувати цикли зворотного зв'язку для зменшення упереджених результатів. Крім того, системи штучного інтелекту з високим рівнем ризику повинні бути захищені від несанкціонованих спроб використання вразливостей за допомогою технічних рішень, адаптованих до конкретних ризиків та обставин. Заходи повинні включати запобігання та контроль таких атак, як отруєння даних, приклади змагання або недоліки моделей, для підтримки цілісності та продуктивності систем штучного інтелекту.

Підходи до впровадження безперервного моніторингу моделей штучного інтелекту

Щоб відповідати вимогам Закону ЄС про штучний інтелект, організації повинні запровадити надійні рішення для кібербезпеки, які сприяють комплексному тестуванню, виявленню інцидентів та постійному моніторингу їхніх систем штучного інтелекту. Ключову увагу слід зосередити на впровадженні стратегій, які ефективно запобігають атакам зловмисників, таким як атаки швидкого впровадження, вставка бекдорів, отруєння даних та вилучення навчальних даних. Для забезпечення ретельного відстеження, ефективного реагування та швидкого відновлення після інцидентів ці рішення повинні доповнюватися детальними показниками та звітами про порівняльні аналізи». ***(Andre Ludwig, David Manek, Ryan Rubin, Kenric Tom and Ahsan Qureshi. How to Achieve Cybersecurity Compliance with the EU AI Act // Ankura Consulting Group, LLC. (https://angle.ankura.com/post/102kyi7/how-to-achieve-cybersecurity-compliance-with-the-eu-ai-act). 04.09.2025).***

***

«У щорічному звіті та фінансовій звітності Пенсійного регулятора Великої Британії (TPR) за 2024–2025 роки змальовується в основному позитивна картина — узгодженість із програмою уряду щодо економічного зростання та прогрес у 27 із 32 ключових показників ефективності — при цьому відверто вказується на кібербезпеку як на найістотніший недолік. Єдиний ключовий показник ефективності, який «значно не досягнуто», стосується кіберризиків та пенсійних технологій; TPR співпрацює з експертами, щоб визначити свою роль, толерантність та заходи щодо зменшення ризиків, а також узгодити свою діяльність з урядом та партнерами з галузі, враховуючи швидкозмінну ситуацію з загрозами в цьому секторі. Декілька суміжних KPI (ключові показники ефективності) були «незначно пропущені», оскільки адміністрація, технології, інновації та кіберстійкість все ще перебувають у стадії вивчення, а система управління ризиками ще не остаточно сформована. TPR зміцнює свою позицію — перевірка стану кібербезпеки IT не виявила критичних проблем, але виявила чотири серйозні недоліки; компанія набирає більш сильну кіберкоманду, вдосконалює управління та розвиває відкладені можливості відновлення після аварій, але визнає, що, з огляду на загострення ситуації, ризик шкоди для вкладників від кібератак «залишається поза межами прийнятного». Цей акцент збігається з більш широкими заходами щодо програм-вимагачів (включаючи пропозиції заборонити виплати викупу в державному секторі) та переходом до більш офіційного повідомлення про кіберінциденти, де TPR, ймовірно, допоможе сформувати та забезпечити дотримання вимог до схем. Тим часом схеми повинні діяти відповідно до оновлених рекомендацій TPR, надаючи пріоритет регулярним перевіркам стану, надійному управлінню та постійному навчанню, визнаючи, що кіберризики будуть зберігатися, а прозорість TPR свідчить про подальший розвиток регулювання та очікування проактивної участі галузі…» ***(Ben Jonsmyth, Samantha Howell and Richard Pettit. Cyber risk: an area of focus for TPR following its Annual Report and Accounts // Burges Salmon LLP***

(https://www.burges-salmon.com/articles/102l4lu/cyber-risk-an-area-of-focus-for-tpr-following-its-annual-report-and-accounts/#page=1). 11.09.2025).

***

«Федеральний уряд Німеччини зробив ще один крок вперед у законодавчому процесі щодо імплементації Директиви NIS2 у Німеччині. 8 вересня 2025 року було внесено новий законопроект , який ознаменував початок парламентської процедури щодо створення нової правової бази для кібербезпеки в Німеччині. Тепер цей проект буде розглянуто та обговорено Бундестагом, федеральним парламентом Німеччини.

Останній проект не вносить суттєвих змін порівняно з попередньою версією . Одним із найбільш примітних елементів є подальше включення суперечливого положення щодо сфери застосування закону. Зокрема, проект зберігає правило, що під час визначення того, чи застосовується закон, слід виключати лише ту діяльність, яка вважається « *незначною* » стосовно загальної діяльності суб'єкта господарювання. Такий підхід викликав значні дискусії серед зацікавлених сторін, деякі з яких ставлять під сумнів повну відповідність цього положення вимогам Директиви NIS2.

Залишається з'ясувати, чи буде це положення включено до остаточної версії законодавства. Парламентський процес надасть подальші можливості для обговорення та потенційних поправок. Законодавці та представники галузі продовжують висловлювати занепокоєння щодо проекту, зокрема щодо його відповідності Директиві NIS2 та його практичних наслідків для організацій, яких це стосується…» ***(Johannes Berchtold. NIS2: German Federal Government Presents Draft Legislation // Reed Smith LLP (https://viewpoints.reedsmith.com/post/102l4k8/nis2-german-federal-government-presents-draft-legislation#page=1). 11.09.2025).***

***

«Франція швидко стала осередком інновацій у сфері кібербезпеки, що зумовлено стрімким зростанням попиту в таких секторах, як охорона здоров'я, банківська справа та виробництво, загальнонаціональним поштовхом до цифрової трансформації та поширенням дистанційної роботи. Програми-вимагачі, фішинг, порушення безпеки даних, DDoS-атаки та атаки «людина посередині» домінують у ландшафті загроз, що спонукає підприємства та урядові установи шукати передові засоби захисту на основі штучного інтелекту. У цю нішу увійшло нове покоління французьких стартапів, чиї продукти варіюються від технологій обману та моніторингу співробітників у реальному часі до безключового хмарного зберігання даних та обміну даними, захищеного блокчейном.

Серед відомих стартапів, на які варто звернути увагу, є: MokN, який використовує технологію обману (наприклад, «приманки» для введення облікових даних) для перехоплення викрадених логінів; Riot Security, платформа для моніторингу кібербезпеки співробітників у режимі реального часу, яка перетворює персонал на першу лінію захисту в епоху загроз, пов'язаних із штучним інтелектом;

Astran.io, що надає безключове хмарне сховище даних за допомогою фрагментації даних для забезпечення конфіденційності, доступності та стійкості; Bastion Technologies, що поєднує інструменти корпоративного рівня та практичний досвід для захисту кінцевих точок, електронної пошти та більш широкого захисту, що також підтримує сертифікацію; Arsen Cybersecurity, що використовує штучний інтелект для складних симуляцій соціальної інженерії та постійної обізнаності з питань безпеки; Command AI, що застосовує підкріплювальне навчання та дані в режимі реального часу для генерації тактичних маневрів для планування та захисту; Nucleon Security, що пропонує автономний захист кінцевих точок на основі штучного інтелекту з принципами нульової довіри; Dastra, платформа SaaS для управління даними та дотримання вимог GDPR, яка допомагає DPO відображати обробку та управляти ризиками; LePhish, що забезпечує реалістичні симуляції фішингу та індивідуальні тренінги для зміцнення захисту співробітників; та Droon, що забезпечує безпечну передачу даних та надійну співпрацю за допомогою легко розгортаємого SaaS на основі блокчейну…

Завдяки підтримці широкої європейської технологічної екосистеми та високому внутрішньому попиту ці стартапи надають Франції надзвичайно важливу роль у глобальній кіберзахисті, пропонуючи рішення, що поєднують гнучкість хмарних технологій, штучний інтелект та відповідність нормативним вимогам, щоб відповідати мінливим цифровим загрозам». ***(Laliq Schuman. Top Cybersecurity Startups in France // TechRound (https://techround.co.uk/startups/top-cybersecurity-startups-in-france/). 15.09.2025).***

***

«Польща збільшує свій бюджет на кібербезпеку до рекордних 1 млрд євро у відповідь на сплеск російських хакерських атак, особливо на лікарні та міські водопровідні системи, порівняно з 600 млн євро у 2024 році. За словами офіційних осіб, Польща є головним об'єктом атак в ЄС, щодня стикаючись з 20–50 спробами саботажу, і хоча близько 99% з них вдається запобігти, деякі все ж завдають шкоди — особливо в галузі охорони здоров'я, де на короткий час були припинені операції та викрадені медичні дані, включаючи інцидент у Кракові, що спричинив значні збитки. Нещодавнє порушення роботи IT-системи водопостачання великого міста було зупинено до того, як крани були відключені, але це є продовженням серії атак на водопровідну інфраструктуру, включаючи малу гідроелектростанцію та очисні споруди в Шчитно, Сєраково, Віткуві та каналізаційну станцію в Кузніці. Щоб посилити захист, уряд виділяє цього місяця додаткові 80 мільйонів євро на захист водопровідних систем, мереж місцевих органів влади та іншої критичної інфраструктури. Кібернапад відбувається паралельно з іншими провокаціями — минулого тижня Польща збила 19 російських дронів, один дрон був збитий поблизу президентської резиденції у Варшаві, а перешкоди GPS з російського Калінінграда впливають на регіональні рейси — що підкреслює більш широке гібридне середовище загроз, яке спонукає Варшаву до інтенсифікації інвестицій…» ***(Izabelė Pukėnaitė. Poland boosts cybersecurity to €1B after Russian hacks on hospitals and water systems // Cybernews***

(https://cybernews.com/cybercrime/poland-cybersecurity-eur1b-russian-hacks-hospitals-water-systems/). 16.09.2025).

***

«Європейська Комісія оголосила про початок збору доказів для дослідження та найкращих практик щодо спрощення законодавства в майбутньому цифровому омнібусі, особливо в питаннях даних, кібербезпеки та штучного інтелекту (ШІ).

Це повністю відповідає програмі спрощення процедур Комісії та її зусиллям щодо створення більш сприятливого бізнес-середовища шляхом полегшення адміністративного навантаження та зниження витрат для компаній. Ініціатива також підтримує ціль Комісії, викладену в «Компасі конкурентоспроможності», щодо скорочення адміністративного навантаження щонайменше на 25 % для всіх компаній і щонайменше на 35 % для малих і середніх підприємств…

Цей заклик до надання доказів є результатом широкого залучення зацікавлених сторін, що включало публічні консультації щодо Стратегії Союзу даних, перегляду Закону про кібербезпеку та Стратегії застосування штучного інтелекту. Це перший крок до спрощення цифрових правил ЄС, який залишається відкритим до 14 жовтня 2025 року». ***(Commission collects feedback to simplify rules on data, cybersecurity and artificial intelligence in the upcoming Digital Omnibus // European Commission (https://digital-strategy.ec.europa.eu/en/news/commission-collects-feedback-simplify-rules-data-cybersecurity-and-artificial-intelligence-upcoming). 16.09.2025).***

***

«…Європейський план дій щодо кібербезпеки лікарень та постачальників медичних послуг був викладений у Політичних настановах Європейської комісії на 2024–2029 роки як одна з пріоритетних ініціатив, які мають бути представлені протягом перших 100 днів нового мандата Комісії. План дій був прийнятий як повідомлення Комісії 15 січня 2025 року, в якому визначено заходи щодо запобігання, виявлення, реагування, відновлення та запобігання інцидентам у сфері кібербезпеки в секторі охорони здоров'я.

Відповідно, з 7 квітня по 14 липня 2025 року було проведено цільове консультаційне обговорення Плану дій. Його метою було зібрати думки громадян, медичних працівників, органів охорони здоров'я, пацієнтів, фахівців з питань дотримання вимог та захисту даних, фахівців з кібербезпеки, організацій та наукових кіл тощо. Це обговорення дало можливість респондентам висловити свої думки як щодо загальних аспектів кібербезпеки в секторі охорони здоров'я, так і щодо конкретних елементів Плану дій.

У рамках цільової консультації було отримано 328 відповідей. Цей фактичний підсумковий звіт містить основні кількісні результати консультації. Крім того, Комісія оцінить якісну інформацію, отриману через поля для відкритого тексту та документи, додані респондентами як додатки до своїх відповідей на опитування. Комісія врахує результати цільової консультації, а також інших консультацій, проведених у рамках Плану дій, при формулюванні подальших

рекомендацій з метою вдосконалення Плану дій…» ***(Factual summary report: Targeted consultation on the Action Plan on the cybersecurity of hospitals and healthcare providers // European Commission (https://digital-strategy.ec.europa.eu/en/library/factual-summary-report-targeted-consultation-action-plan-cybersecurity-hospitals-and-healthcare). 12.09.2025).***

***

«Європейська Комісія оголошує новий конкурс для закладів вищої освіти, закладів професійної освіти та навчання, європейських університетських альянсів та промисловості, які бажають приєднатися до мережі промисловості та академічних кіл Академії навичок у сфері кібербезпеки (Industry-Academia Network of the Cybersecurity Skills Academy)…

Згідно з останнім дослідженням ISC2, хоча загальна потреба в робочій силі в ЄС залишалася стабільною, коливаючись між 1,14 млн і 1,25 млн, дефіцит робочої сили в галузі кібербезпеки зріс з приблизно 274 000 у 2023 році до 299 000 у 2024 році, що становить 9% зростання.

На цьому тлі мережа «Industry-Academia Network of the Cybersecurity Skills Academy» має на меті налагодити конкретну співпрацю та встановити партнерські відносини між своїми членами – усіма ключовими учасниками з промисловості та академічних кіл, міждисциплінарними, щоб відповісти на всі вимоги до набору навичок у сфері кібербезпеки; і, зрештою, збільшити кількість європейських фахівців у сфері кібербезпеки.

Це включає такі можливі заходи, як надання студентам доступу до найсучасніших тренінгів та сертифікацій, розробка та оновлення навчальних програм та пропозицій з кібербезпеки, надання курсів з кібербезпеки на робочому місці, відкриття можливостей для навчання, стажування та практики, розробка програм наставництва, розробка мікросертифікатів з кібербезпеки та проведення цільових ярмарків вакансій…» ***(Call to industry and academia: join the Industry-Academia Network of the Cybersecurity Skills Academy // European Commission (https://digital-skills-jobs.europa.eu/en/latest/news/call-industry-and-academia-join-industry-academia-network-cybersecurity-skills-academy). 12.06.2025).***

***

«Згідно з новим опитуванням, понад половина ірландських споживачів припинили б купувати в інтернет-магазині після кібератаки.

Трохи більше третини покупців кажуть, що вони прийняли б обґрунтоване рішення, виходячи з обставин, тоді як кожен десятий каже, що був би готовий повернутися, якби продавець швидко вирішив проблему.

Дослідження, проведене для страхового брокера Gallagher в Ірландії, показує, що жінки більш поблажливі, ніж чоловіки.

Було виявлено, що 38% жінок-покупців «зважать обставини», перш ніж прийняти рішення про розірвання зв'язків, порівняно з 29% чоловіків.

9% чоловіків кажуть, що вони «точно» не повернуться до продавця, який постраждав, порівняно з 4% жінок.

У той час як 16% респондентів чоловічої статі заявили, що вони «абсолютно» припинили б робити покупки в цьому продавці, порівняно з 10% жінок.

В рамках дослідження наслідків кіберзлочинності було опитано 1000 дорослих по всій країні…» ***(Fergal O'Brien. Cyber attacks impacting consumer trust in online retailers – survey // Ireland's National Public Service Media (https://www.rte.ie/news/2025/0923/1534796-retail-cyber-attacks/). 23.09.2025).***

***

«…Британські організації зафіксували приблизно 7,8 мільйона кіберзлочинів за минулий рік, що нагадує про те, що статичні, календарні засоби захисту не можуть встигати за зловмисниками, які автоматизують і адаптуються в режимі реального часу. Ніде ця зміна не є такою помітною, як у тестуванні на проникнення. Традиційно тестування на проникнення, яке проводилося вручну раз на рік, зараз перетворюється на платформи штучного інтелекту, які безперервно сканують, миттєво перевіряють виправлення та класифікують недоліки за рівнем ризику для бізнесу. Ця еволюція породжує підписки на тестування на проникнення як послугу (PTaaS), які роблять тестування на вимогу доступним — це критично важливо на ринку, де лише 8 % британських компаній замовляли тестування на проникнення у 2024 році…

Хмарні та гібридні середовища додають терміновості: сорок три відсотки організацій вже використовують як локальні, так і хмарні ресурси, тому тестувальники повинні володіти обома середовищами та застосовувати інструменти, специфічні для хмарних технологій. Проте штучний інтелект не замінює людей, а підсилює їх. Досвідчені тестувальники забезпечують інтуїцію, нестандартне мислення та розуміння бізнес-контексту, яких бракує машинам, а також навчають моделі на реальних прикладах атак. Цей гібридний підхід — штучний інтелект для розпізнавання шаблонів, люди для нюансів — стане ще більш цінним, оскільки британська програма TechFirst вартістю 187 мільйонів фунтів стерлінгів намагається подолати дефіцит кібернавичок, який зачіпає 30% компаній, що займаються безпекою.

Тому керівництво повинно перейти до гнучких моделей безпеки, які включають постійне тестування на проникнення на основі ризиків у процес розробки; використовувати штучний інтелект для автоматизації повторюваних перевірок, залишаючи експертів для складних сценаріїв; та централізувати результати, щоб команди розробників, фахівців з безпеки та операторів могли швидко вживати заходів для усунення недоліків. Застосування цієї методології, доповненої штучним інтелектом і постійно активної, перетворить тестування на проникнення з періодичної перевірки на інтелектуальну, проактивну захисну систему, придатну для сучасного безжального середовища загроз…» ***(Conor O'Neill. How AI augmentation is revolutionizing penetration testing in cybersecurity // Future US, Inc. (https://www.techradar.com/pro/how-ai-augmentation-is-revolutionizing-penetration-testing-in-cybersecurity). 22.09.2025).***

***

«Керівникам вищої ланки австралійської авіакомпанії Qantas було скорочено річні бонуси на 15% після кібератаки в липні , яка спричинила низку проблем для компанії.

У своєму останньому звіті про прибутки компанія повідомила про прибуток у розмірі 1,5 мільярда доларів за останній фінансовий рік. Але у звіті голова правління Qantas Group Джон Маллен заявив, що компанія мусить визнати наслідки кіберінциденту, який розкрив інформацію 5,7 мільйона людей.

«Хоча керівництво вжило негайних заходів для стримування порушення, підтримки клієнтів та впровадження додаткових заходів захисту, визнаючи серйозність інциденту, ми вирішили зменшити короткострокові бонуси за 2024/25 рік на 15 процентних пунктів для генерального директора та виконавчого керівництва», – сказав Маллен.

У Qantas пояснили, що це дорівнює зменшенню зарплати генерального директора Qantas Group Ванесси Хадсон на 250 000 доларів.

Маллен додав, що штраф «відображає їхню спільну відповідальність, водночас визнаючи постійні зусилля щодо підтримки клієнтів та запровадження додаткових засобів захисту для них».

У своєму щорічному звіті Qantas заявила, що спостерігає зростання загроз соціальної інженерії та враховує отримані знання з кіберінциденту у своїй системі управління ризиками.

Криміналістичне розслідування інциденту все ще триває, але раніше Qantas заявляла, що у 2,8 мільйона клієнтів було розкрито імена, адреси електронної пошти та номери карток часто літаючих пасажирів Qantas. Щонайменше 1,7 мільйона інших клієнтів мали розкриту певну комбінацію цієї інформації з домашніми адресами, датами народження, номерами телефонів, уподобаннями щодо страв або статтю.

У повідомленні йдеться, що жодних даних кредитних карток чи паспортів не було розголошено. У компанії додали, що викраденої інформації недостатньо для злому облікових записів постійних пасажирів Qantas…» ***(Jonathan Greig. Qantas penalizes executives for July cyberattack // Recorded Future News (https://therecord.media/qantas-airline-reduces-bonuses-executives-data-breach). 05.09.2025).***

***

«За даними опитування, проведеного Радою аудиту Японії у п’ятницю, загалом 58 інформаційних систем у 12 урядових установах Японії виявилися вразливими до кібератак.

Аудиторська рада закликала установи вжити заходів відповідно до урядових стандартів.

Єдині стандарти заходів кібербезпеки країни були встановлені такими організаціями, як Національне управління кібербезпеки, створене в липні шляхом

реорганізації Національного центру готовності до інцидентів та стратегії кібербезпеки.

Опитування аудиторської ради, проведене протягом трьох років до 2023 фінансового року, охопило 356 інформаційних систем у 40 державних установах, включаючи міністерства та відомства.

У відповідних системах аудиторська рада виявила, що управління правами доступу та процесами автентифікації паролів не відповідало стандартам, розробленим для запобігання кібератак, таким як крадіжка та знищення важливої інформації». ***(12 Japan Agencies Found Vulnerable to Cyberattacks // Jiji Press (https://jen.jiji.com/jc/eng?g=eco&k=2025091200926). 12.09.2025).***

***

«…3 вересня 2025 року Агентство з кібербезпеки Сінгапуру (CSA) опублікувало звіт «Кіберпростір Сінгапуру 2024/2025», в якому зазначило, що місцеві тенденції відображають глобальну ескалацію загроз: кількість випадків фішингу зросла на 49% до понад 6100 повідомлень, причому 12% електронних листів було створено за допомогою штучного інтелекту, а підробка адрес була зосереджена на банківських/фінансових послугах, уряді та електронній комерції, тоді як зловмисники все частіше використовували HTTPS і поширені домени верхнього рівня (.com, .cn), щоб виглядати легітимними; кількість випадків використання програм-вимагачів зросла на 21 %, вразивши транснаціональні корпорації та виробників, що котируються на біржі, і непропорційно вплинувши на малі та середні підприємства, що надають професійні послуги, причому для порушення роботи переважно використовувалося шифрування; кількість інфікованих інфраструктур зросла на 67% до приблизно 117 300 систем через застарілі або не оновлені активи; підозрювана активність APT зросла в чотири рази з 2021 року, причому такі групи, як UNC3886, націлюються на високоцінні стратегічні активи, включаючи критичну інфраструктуру… Соціальна інженерія поширилася через фішинг та підробку служб технічної підтримки, атаки на ланцюги постачання використовували слабкі місця постачальників (дефектне оновлення CrowdStrike завдало збитків компаніям з рейтингу Fortune 500 на суму близько 5,4 млрд доларів США та спричинило майже 40 000 скасувань рейсів), а DDoS-атаки зросли в масштабах і складності, що зробило Сінгапур сьомою країною за кількістю атак у IV кварталі 2024 року і третім за величиною джерелом DDoS-трафіку, причому найбільше атакували телекомунікаційні компанії, інтернет-провайдери та BFSI. У звіті вказано, що штучний інтелект, залежність від хмарних технологій, поширення Інтернету речей та нові атаки на гіпервізори є двоякими технологічними драйверами, а також підкреслено системні виклики, пов'язані з кіберфізичною конвергенцією, вразливістю ланцюгів постачання (включно з відкритим кодом), людським фактором, постійним дефіцитом талантів та швидкозмінними ризиками (штучний інтелект, квантова технологія). Відповідь CSA зосереджена на основних напрямках стратегії на 2021 рік — стійкій інфраструктурі, безпечнішому кіберпросторі та міжнародній співпраці — підкріплених розвитком екосистеми та розвитком талантів, а також заходами на 2024 рік, включаючи розширення повноважень Закону про кібербезпеку (STCC,

ESCI, FDI), Генеральний план кібербезпеки ОТ та форум OTCEP, майбутній Кодекс практики хмарних технологій, рекомендації щодо безпеки штучного інтелекту, публічні ініціативи з кібербезпеки та маркування пристроїв, програми для стартапів та талантів». ***(CyberSG TIG, CyberBoost/Growth, SG Cyber Talent), а також рекомендації SBOM щодо зміцнення ланцюгів постачання… (Sumyutha Sivamani. CSA's Singapore Cyber Landscape 2024/2025 Report // Clyde & Co LLP (https://www.clydeco.com/en/insights/2025/09/csa-s-singapore-cyber-landscape-2024-2025-report). 09.09.2025).***

***

«…На тлі ескалації геополітичної напруженості, економічних труднощів та швидких технологічних змін кібербезпека залишається одним з головних ризиків для підприємств. Австралійські компанії намагаються підвищити свою стійкість в умовах фінансових обмежень і борються з двома постійними викликами: як максимізувати інвестиції в кібербезпеку та як запобігти «кібервтомі», коли важко довести рентабельність інвестицій, а інциденти зникають з заголовків новин… Третє опитування HSF Kramer Cyber Risk Survey, в якому взяла участь найбільша група генеральних юрисконсультів з різних секторів, підтверджує центральну роль юридичних лідерів, а підвищення рівня освіти, участь у моделюванні та практичне реагування на інциденти відображають складні вимоги до регулювання, комунікацій та виправлення ситуації, а також тривалі юридичні наслідки серйозних інцидентів. Хоча 68% респондентів стверджують, що за останній рік кіберзагрози зросли (у порівнянні з 80% у 2024 році), дані ASD показують, що кількість випадків використання програм-вимагачів та CVE зросла, що свідчить про звикання або втому, а не про зниження ризику. При цьому 75% тих, хто бачить підвищення ризику, пов'язують це з більш витонченими, технологічними загрозами, включаючи соціальну інженерію на основі штучного інтелекту, тоді як багато організацій все ще борються з базовими проблемами безпеки. Опитування підкреслює вирішальний перехід назад до людського фактору — розподіл відповідальності за захист між усіма співробітниками — і закликає до застосування принципів нульової довіри та впровадження управління кіберризиками в повсякденну діяльність усіх підрозділів, оскільки ризики, пов'язані з третіми сторонами та даними, зараз є головними ризиками в умовах цифрової трансформації та складних ланцюгів постачання… Відповідальність за ризики поширюється за межі CISO на керівників у сферах управління даними, кадрової політики, закупівель, юридичних та фінансових питань, а також на правління, де звітність відходить від технологічних показників типу «світлофор» на користь узагальнених оцінок ризиків для всього підприємства; оцінка технологічних ризиків тепер включає штучний інтелект як можливість і загрозу для всієї компанії, нерозривно пов'язану з безпекою. Однак готовність правління відстає: лише 45% вважаються «кіберзрілими», менше 40% проводили симуляцію протягом минулого року, а освіта правління знизилася з 70% (2024) до 59% (2025)…

У звіті закликають до постійного міжфункціонального контролю та вдосконалення, щоб уникнути самозаспокоєння, і підкреслюють, що кібербезпека залишатиметься центральним елементом управління ризиками в організаціях, а

юридичні лідери будуть на передовій у відповіді Австралії на ці виклики». ***(Cameron Whittfield. Are you cyber ready? The cyber challenge through the eyes of Australia's legal leaders // Herbert Smith Freehills Kramer LLP (https://www.hsfkramer.com/insights/reports/cyber-risk-report-2025). 18.09.2025).***

***

«У країнах Азіатсько-Тихоокеанського регіону (APAC), які швидко переходять на цифрові технології, керівники служб інформаційної безпеки тепер ставлять безпеку ідентифікації в центр своїх стратегій кіберзахисту. Опитування SailPoint, в якому взяли участь понад 100 керівників служб інформаційної безпеки та віцепрезидентів з питань безпеки, показує, що 78 % підприємств вважають контроль ідентичності — що охоплює кожну людину, систему та обліковий запис машини — «надзвичайно» або «дуже» важливим, а 90 % вже впровадили основні заходи, такі як контроль доступу на основі ролей, самообслуговування запитів на доступ та автоматизоване надання доступу…

Причиною цього є різке зростання кількості атак, спрямованих на особисті дані, — крадіжка облікових даних, фішинг, захоплення облікових записів — які стали набагато потужнішими завдяки використанню зловмисниками штучного інтелекту для створення приманок у режимі реального часу. 60 % респондентів «дуже стурбовані» цими загрозами, пов'язаними зі штучним інтелектом; головними цілями є фінансові та технологічні компанії на Філіппінах і в Азіатсько-Тихоокеанському регіоні. Щоб протидіяти їм, організації починають застосовувати штучний інтелект. Виділяються дві можливості: аналіз ролей на основі штучного інтелекту, який постійно аналізує права доступу, щоб позбавити надмірних або ризикованих привілеїв, та виявлення аномалій/відхилень, яке позначає незвичайні моделі доступу до того, як буде завдано шкоди. 62% компаній планують впровадити такі інструменти…

Ця зміна означає перехід від статичних систем захисту периметра до динамічних архітектур з нульовим рівнем довіри, в яких права доступу оцінюються, надаються та переоцінюються майже в режимі реального часу. Виклики залишаються — гібридні хмари, величезна кількість ідентичностей третіх сторін і машин, а також все більш розумні супротивники — але майбутні інвестиції будуть зосереджені на оцінці ризиків на основі штучного інтелекту, автоматизованому оновленні політик та більш тісній взаємодії між командами з безпеки, IT та бізнесу. Коротко кажучи, в гіперпідключеному середовищі Азіатсько-Тихоокеанського регіону ідентичність стала новою площиною контролю, а безпека ідентичності на основі штучного інтелекту тепер є необхідною для запобігання порушенням, захисту критично важливих активів та підтримки цифрового зростання…» ***(Eric Kong. Identity security: The core of cyber resilience // The Manila Times (https://www.manilatimes.net/2025/09/21/business/sunday-business-it/identity-security-the-core-of-cyber-resilience/2187643). 20.09.2025).***

***

«...Кількість кіберінцидентів, пов'язаних із системами третіх сторін, які використовує уряд штату Новий Південний Уельс (NSW), за два роки зросла

більш ніж у чотири рази: у 2023-2024 фінансовому році було зафіксовано 17 інцидентів, що більш ніж удвічі перевищує показник попереднього року (8 інцидентів) і більш ніж у чотири рази перевищує показник 2021–2022 фінансового року, згідно з даними, отриманими iTnews відповідно до закону штату про доступ до інформації (GIPA Act). Cyber Security NSW почала систематично збирати дані про інциденти в 2021 році і зараз узагальнює їх у щорічному звіті про загрози, доступному тільки для агентств; у публічному блозі, що підсумовує звіт за листопад 2024 року, зазначено, що кількість інцидентів із залученням третіх сторін «майже потроїлася» у 2024 фінансовому році, і ця цифра також включає місцеві ради. Департамент обслуговування клієнтів, який контролює Cyber Security NSW, заявив, що агентства зобов'язані управляти ризиками, пов'язаними з третіми сторонами, шляхом включення вимог безпеки в контракти та проведення оцінки ризиків постачальників. Загалом, Cyber Security NSW відреагувала на понад 200 інцидентів у 2024 фінансовому році. Для підвищення стійкості державний бюджет виділяє Cyber Security NSW 87,7 млн доларів протягом чотирьох років, додаючи до 20,3 млн доларів, інвестованих минулого року, та 15 млн доларів з Digital Restart Fund для зменшення екстремальних кіберризиків…» ***(Eleanor Dickinson. NSW gov third party-linked cyber incidents quadruple in two years // nextmedia Pty Ltd. (https://www.itnews.com.au/news/nsw-gov-third-party-linked-cyber-incidents-quadruple-in-two-years-620328). 18.09.2025).***

***

«За останні шість років корейські компанії повідомили про понад 7000 випадків витоку даних, що викликає занепокоєння щодо кібербезпеки країни на тлі нещодавньої серії хакерських атак на телекомунікаційні та фінансові компанії, свідчать дані, опубліковані в неділю.

Згідно з даними… між 2020 роком та минулою неділею до влади було подано 7198 заяв про кіберзагрози.

Кількість випадків становила 603 у 2020 році та дещо зросла до 640 у 2021 році, а потім майже подвоїлася до 1142 у 2022 році.

У 2023 році було зареєстровано загалом 1277 випадків, у 2024 році – 1887, а з початку року – 1649.

Малі та середні фірми повідомили про 5907 таких випадків, що становить 82 відсотки від загальної кількості, далі йдуть середні фірми з 592 випадками та конгломерати з 242 випадками. Некомерційні організації також повідомили про 457 випадків, згідно з даними.

Більшість випадків стосувалися злому систем, що становило 4354 випадки, або 60,5% від загальної кількості, тоді як зараження та поширення шкідливого програмного забезпечення становили 20,9%, а DDoS-атаки – 18,6%.

Якщо детальніше, кількість інцидентів зі злому систем становила 250 у 2020 році, що становить 41,4% від загальної кількості випадків за той рік, але цей показник зріс до 72,8% минулого року та 61,3% з початку року, згідно з тими ж даними». ***(Corporate cybersecurity threats exceed 7,000 cases in past 6 years: data // The Korea Times***

(https://www.koreatimes.co.kr/southkorea/society/20250921/corporate-cybersecurity-threats-exceed-7000-cases-in-past-6-yrs-data). 21.09.2025).

***

Китай та Індія

«Китайські законодавці почали розглядати проект поправки до Закону про кібербезпеку з метою посилення юридичної відповідальності.

Проект було подано в понеділок на перше читання на поточній сесії Постійного комітету Всекитайських зборів народних представників, національного законодавчого органу.

Проект передбачає кращу відповідність із відповідними законами, включаючи Закон про безпеку даних, Закон про захист персональних даних та Закон про адміністративні покарання, для забезпечення більш узгодженої правової бази…» ***(China mulls amendment to cybersecurity law to strengthen legal responsibilities // XINHUANET.com (https://english.news.cn/20250908/38620393c8564f488567412bc0c55abb/c.html). 08.09.2025).***

***

«Залежність Індії від американського програмного забезпечення, хмарних сервісів та платформ соціальних мереж створює серйозну економічну та безпекову вразливість у часи геополітичної напруженості, заявив у неділю аналітичний центр Глобальної ініціативи з дослідження торгівлі (GTRI).

Вашингтон має можливість припинити надання послуг або доступ до даних, порушуючи роботу банківської справи, управління та оборонних систем, одночасно контролюючи публічний дискурс через іноземні платформи, йдеться у повідомленні…

Щоб вирішити цю проблему, уряд повинен запустити «Місію цифрового свараджа», в основі якої лежать суверенна хмара, власна ОС (операційна система), власна кібербезпека та лідерство штучного інтелекту, засноване на даних», – сказав засновник GTRI Аджай Шрівастава…

У короткостроковій перспективі (1-2 роки) Індія повинна запровадити обов'язковий хмарний хостинг для критично важливих даних, запустити національну програму ОС та провести пілотний перехід на Linux у ключових міністерствах, сказав він, додавши, що в середньостроковій перспективі (3-5 років) урядові системи повинні повністю перейти на індійське програмне забезпечення, а державно-приватні консорціуми з кібербезпеки повинні запрацювати.

У довгостроковій перспективі (5-7 років) Індія повинна досягти хмарного паритету, замінити іноземні ОС в оборонному та критично важливому секторах, а також створити конкурентоспроможні на світовому рівні платформи відкритих мереж...» ***(India's reliance on US software, cloud services, social media platforms poses economic vulnerability: GTRI // Bennett, Coleman & Co. Ltd. (https://economictimes.indiatimes.com/tech/technology/indias-reliance-on-us-software-***

cloud-services-social-media-platforms-poses-economic-vulnerability-gtri/articleshow/123881413.cms). 14.09.2025).

***

«Індійська служба фінансової розвідки (FIU-IND) тепер вимагає, щоб кожна платформа віртуальних цифрових активів (VDA) — біржі криптовалют, зберігачі, служби переказу та оплати — пройшла аудит кібербезпеки, проведений оцінювачем, затвердженим CERT-In, перш ніж вона зможе зареєструватися або продовжити діяльність як суб'єкт звітності відповідно до Закону про запобігання відмиванню грошей (PMLA). У циркулярі, виданому 15 вересня 2025 року, FIU повідомила директорам, головним посадовим особам та головним спеціалістам з питань дотримання нормативних вимог, що аудиторський сертифікат є «обов'язковим з негайним вступом в силу», та попередила, що недотримання вимог може спричинити штрафні санкції відповідно до розділу 13(2) Закону…

Цей наказ з'явився після низки гучних хакерських атак — WazirX втратив 235 мільйонів доларів США в липні 2024 року, а CoinDCX — близько 368 крор рупій в 2025 році — і має на меті посилити перевірку клієнтів, зберігання журналів та повідомлення про підозрілі транзакції, щоб слідчі могли відстежувати вкрадені або відмиті криптовалютні кошти. Він замінює колишній тест «Fit & Proper» для нових заявників на більш широкий сертифікат «Partner Accreditation for Compliance & Trust» (PACT)…

Криптосектор Індії, який налічує приблизно 55 зареєстрованих постачальників VDA і приніс понад 700 крор рупій прямих податкових надходжень у 2023-24 фінансовому році, все ще не має спеціального закону; Верховний суд нещодавно звернув увагу на цю прогалину в законодавстві. Хоча обов'язкові аудити та акредитація PACT повинні посилити захист інвесторів та прозорість правоохоронних органів, вони також підвищують витрати, що може тиснути на менші стартапи або спонукати їх до перенесення діяльності за кордон, залишаючи галузь у суворо контрольованій, але все ще юридично неоднозначній «сірій зоні» до прийняття комплексного законодавства…» ***(Rohit Singh. Cybersecurity Audits Become Mandatory For Virtual Digital Asset Providers In India // Mixed Bag Media Pvt. Ltd. (https://www.medianama.com/2025/09/223-cybersecurity-audits-virtual-digital-asset-providers-india/). 19.09.2025).***

***

«…З 1 листопада Китай вимагатиме від організацій повідомляти Адміністрацію кіберпростору Китаю (CAC) протягом години про будь-які інциденти кібербезпеки, класифіковані як «особливо серйозні» або «серйозні». Найвищий рівень охоплює події, які порушують роботу критично важливих служб для понад 10 мільйонів жителів, виводять з ладу портали урядових органів провінційного рівня або зачіпають понад половину населення провінції. До «серйозних» інцидентів належать порушення, що призводять до витоку даних щонайменше 10 мільйонів громадян, відключення, що зачіпають 50 % мешканців міста або щоденні потреби одного мільйона людей, відключення урядових сайтів

на шість годин, зупинка критичної інфраструктури на понад одну годину, економічні збитки понад 100 мільйонів ієн або будь-які епізоди, що ставлять під загрозу соціальну стабільність або національну безпеку.

Протягом 60 хвилин жертва повинна надати детальну інформацію про системи, що зазнали атаки, тип і час атаки, попередню причину, початкові збитки, вимоги щодо викупу, можливі більш широкі ризики та будь-які запити про державну допомогу. Несвоєчасні, неповні, неправдиві або приховані повідомлення, що призводять до «серйозних шкідливих наслідків», спричинять суворі юридичні санкції як для організації, так і для відповідальних осіб…

Пекін заявляє, що більш суворі правила відображають зростання кількості атак з використанням програм-вимагачів та викрадення даних і відповідають глобальним тенденціям, таким як нові стандарти для підрядників у сфері оборони США, що роблять швидке розкриття інформації про інциденти основним елементом національного управління кіберризиками…» ***(Ellen Jennings-Trace. The countdown is on - Chinese firms now have just an hour to report cybersecurity incidents // Future US, Inc. (https://www.techradar.com/pro/security/the-countdown-is-on-chinese-firms-now-have-just-an-hour-to-report-cybersecurity-incidents). 16.09.2025).***

***

Інші країни

«…Кабінет Міністрів Молдови схвалив постанову про порядок виконання зобов'язань щодо кібербезпеки постачальниками послуг у критичних секторах. За даними Міністерства економічного розвитку та цифровізації, це рішення є важливим кроком для захисту громадян та життєво важливої інфраструктури в умовах зростання глобальних ризиків. Кібератака може порушити роботу таких життєво важливих послуг, як енергетика, водопостачання, транспорт, телекомунікації, банківська справа чи охорона здоров'я, що безпосередньо вплине на повсякденне життя населення. Нові вимоги встановлюють чіткі стандарти, узгоджені з європейськими та міжнародними нормами, зміцнюючи стійкість державних та приватних постачальників. Головна мета — забезпечити високий рівень захисту мереж та інформаційних систем, що використовуються для надання життєво важливих послуг… Затверджені правила будуть впроваджуватися поступово. Вони передбачають 12 місяців для ключових постачальників, які керують критично важливими послугами, та 18 місяців для важливих постачальників. Постанова, прийнята Кабінетом Міністрів, також запроваджує додаткові механізми: процедуру повідомлення про кіберінциденти, чіткі критерії визначення рівня впливу та правила оцінки вже вжитих постачальниками заходів». ***(The Moldovan government has approved minimum cybersecurity requirements for service providers in critical sectors // AP "InfoMarket Media" SRL. (https://infomarket.md/en/analitics/380428). 03.09.2025).***

***

«…Міністр комунікацій, цифрових технологій та інновацій Гани Самуель Нартей Джордж попередив про зростання кіберзагроз для підприємств, державних установ та домогосподарств, закликавши громадян ставитися до безпеки в Інтернеті так само серйозно, як і до фізичної безпеки, та оголосивши про кроки щодо внесення змін до Закону про кібербезпеку 2020 року (Закон 1038) з метою усунення нових ризиків. Під час відкриття Національного місяця обізнаності з питань кібербезпеки 2025 року в Аккрі він повідомив про збитки від кіберзлочинності в розмірі 23,3 млн ганських седі в 2024 році та 14,94 млн ганських седі в першій половині 2025 року, а також зазначив, що облікові дані 35 організацій — міністерств, банків, лікарень та університетів — з'явилися в даркнеті... Виконуючий обов'язки генерального директора Управління з питань кібербезпеки Дівайн Селасі Агбеті зазначив, що кількість інцидентів зросла з 1317 у 2024 році до 2008 у першому півріччі 2025 року, а збитки були спричинені шахрайством та підробкою особи, і додав, що цьогорічна інформаційна кампанія буде спрямована на залучення дітей, підприємств, уряду та громадян до захисту цифрових прав та зміцнення національної стійкості…» ***(Dickson Worlanyo Dotse. Alert! Cyber threats increasing - Minister warns // Graphic Communications Group Ltd. (https://www.graphic.com.gh/news/general-news/ghana-news-alert-cyber-threats-increasing-minister-warns.html). 05.09.2025).***

***

«Азербайджан зараз майже щодня стикається з кіберзагрозами, які варіюються від звичайного фішингу та DDoS-атак до складних вторгнень з політичною мотивацією, спрямованих на захоплення контролю над критично важливими серверами. За даними Державної служби спеціального зв'язку та інформаційної безпеки (SCIS), спеціалізовані команди щодня фіксують розподілені атаки типу «відмова в обслуговуванні», шкідливе програмне забезпечення, що поширюється електронною поштою, та операції на базі Telegram; з січня по серпень 2025 року вони зафіксували 612 ознак атак на урядові установи та понад тисячу інцидентів у 2024 році. Людські втрати також зростають: протягом перших чотирьох місяців 2025 року громадяни втратили понад шість мільйонів манати через онлайн-шахрайство, а понад 6000 осіб, серед яких майже 100 державних службовців, стали жертвами кіберзлочинів…

Високопоставлені чиновники SCIS попереджають, що понад 40 відсотків глобальних атак на державні мережі зараз спрямовані на критичну інфраструктуру, і вони визнають, що управлінські та культурні слабкості всередині установ часто відкривають двері для таких атак. Щоб посилити захист, Баку запустив програму «Bug Bounty» для залучення незалежних дослідників і наголошує на необхідності співпраці між міністерствами у разі серйозних порушень. Однак загроза не є суто технічною чи фінансовою. У серпні 2025 року, після інтерв'ю президента Ільхама Алієва на телеканалі Al-Arabiya, інформаційні операції російського походження заполонили заборонені соціальні мережі антиазербайджанською дезінформацією, продемонструвавши, як кібердіяльність, пропаганда та гібридна війна об'єднуються, щоб підірвати національну згуртованість…

Недавні атаки також викрили стратегічні вразливості в системі зв'язку Азербайджану. Масштабна DDoS-атака в серпні на магістрального провайдера Delta Telecom змусила перенаправити трафік через Azertelecom і Aztelecom — цей епізод продемонстрував цінність конкурентної інфраструктури, але також підкреслив залежність від маршрутів, які все ще проходять через Росію. Тому спостерігачі закликають прискорити створення транскаспійського оптоволоконного коридору та подальшу диверсифікацію міжнародних зв'язків для зміцнення цифрового суверенітету…» ***(Nazrin Abdul. Cyber intrusions in S Caucasus: Azerbaijan at frontline of hybrid conflict // azernews (https://www.azernews.az/analysis/247036.html). 06.09.2025).***

***

«Державна нафтова компанія Казахстану відкинула заяви індійської компанії з кібербезпеки Seqrite про те, що вона стала мішенню нової хакерської групи, пов'язаної з Росією, заявивши, що інцидент насправді був внутрішніми навчаннями з фішингу.

Минулого тижня Seqrite Labs опублікувала дослідження про так звану нововиявлену групу NoisyBear, яка, за її словами, діяла з квітня і зосереджувалася на енергетичному секторі Центральної Азії. Компанія заявила, що NoisyBear у травні зламала поштову скриньку співробітника фінансового відділу KazMunayGas і використовувала її для розсилки фішингових листів, замаскованих під оновлення корпоративної політики, коригування зарплат та повідомлення IT-відділу. У цих листах містилися шкідливі архівні файли, призначені для встановлення додаткових шкідливих програм.

Seqrite приписала цю діяльність Росії, посилаючись на використання зловмисниками російської мови та інфраструктури, що належить санкціонованому провайдеру Aeza Group, а також на схожість із попередніми кампаніями, пов'язаними з дійовими особами з Москви. У липні Aeza була піддана санкціям з боку Міністерства фінансів США за нібито підтримку операторів програм-вимагачів та онлайн-ринків наркотиків.

Однак KazMunayGas відкинула висновки Seqrite. У коментарі казахстанському виданню Orda компанія заявила, що інцидент був запланованою симуляцією.

«У травні 2025 року KMG організувала та провела заплановані внутрішні навчання з метою перевірки, оцінки та підвищення обізнаності співробітників з питань інформаційної безпеки», — повідомила компанія. Вона додала, що деякі її співробітники були попереджені заздалегідь, а кампанія була використана для надання рекомендацій персоналу.

Докази у власному звіті Seqrite, здається, підтверджують це твердження: на одному з скріншотів фішингової кампанії були показані тестові акаунти серед одержувачів, наприклад адреси у форматі «test@kmg[.]kz», зазначив російський експерт з кібербезпеки Олег Шакіров. Seqrite не відповіла на запит Recorded Future News про коментарі…» ***(Daryna Antoniuk. Kazakh oil giant denies cyberattack, says incident was 'planned' phishing drill // Recorded Future News***

(https://therecord.media/kazakstan-oil-company-kazmunaygas-phishing-simulation-not-cyberattack). 08.09.2025).

***

«…На національному семінарі з питань боротьби з кіберзлочинністю та **фінансовими злочинами, що відбувся в Абуджі, голова Комітету Палати представників з фінансових злочинів, шановний Джинджер Онвусібе, повідомив, що Нігерія щороку втрачає приблизно 500 мільйонів доларів США через онлайн-шахрайство та інші кіберзлочини.** Виступаючи через секретаря комітету Остіна Адесоро, Онвусібе зазначив, що захід, організований у партнерстві з Комісією з економічних та фінансових злочинів (EFCC) і в якому взяли участь понад 100 представників державного та приватного секторів, має на меті зміцнити економічне, соціальне та безпекове зростання шляхом навчання учасників розпізнавати та боротися з інтернет-загрозами. Він привітав створення EFCC спеціального Центру з боротьби з кіберзлочинністю, назвавши його життєво важливим для захисту громадян, бізнесу та національної стабільності. Онвусібе підкреслив, що безконтрольна кіберзлочинність псує глобальну репутацію Нігерії та підриває її інститути, і привітав поточну співпрацю між парламентом та EFCC з метою розробки більш жорстких законів, навчання фінансових менеджерів та розвитку обережних фіскальних практик. Він також зазначив, що Палата розробляє законодавство для регулювання транзакцій з криптовалютою відповідно до міжнародних стандартів…» ***(Sanni Onogu. Nigeria loses $500m annually to cyber crimes, says Reps panel // The Nation Newspaper Ltd. (https://thenationonlineng.net/nigeria-loses-500m-annually-to-cyber-crimes-says-reps-panel/). 10.09.2025).***

***

«Національний центр кредитної інформації В'єтнаму (CIC), що працює під егідою Державного банку В'єтнаму, підтвердив кібератаку, в результаті якої, можливо, було розкрито конфіденційну інформацію кредиторів.

…масштаби порушення поки що залишаються незрозумілими.

Слідчі заявили: «Початкове розслідування виявило ознаки несанкціонованого доступу, спрямованого на крадіжку персональних даних, при цьому масштаби порушення все ще оцінюються».

В'єтнамський центр реагування на надзвичайні ситуації з кібербезпеки (VNCERT) повідомив, що отримав повідомлення від CIC про інцидент 11 вересня.

«Інцидент не порушив роботу та не завдав жодної шкоди, а система кредитної інформації залишається повністю функціональною», – йдеться у листі, надісланому фінансовим установам, від CIC.

У листі також натякається, що атаку могла здійснити Shiny Hunters, хакерська група, відома зламом систем великих компаній, включаючи Google, Microsoft і Qantas…

Влада В'єтнаму продовжує стежити за ситуацією, працюючи над визначенням масштабу нападу». ***(Wayne Williams. Vietnam creditors hit by cyberattack - sensitive data at risk // Future US, Inc.***

(https://www.techradar.com/pro/security/vietnam-creditors-hit-by-cyberattack-sensitive-data-at-risk). 13.09.2025).

***

«Нещодавній сплеск кібератак спрямований на ключові міністерства та силові структури Іраку, що викликає занепокоєння щодо цифрової інфраструктури та захисту даних країни.

Згідно з повідомленням лондонської газети Al-Araby Al-Jadeed, в останні роки електронні зломів були здійснені в Міністерстві внутрішніх справ, Міністерстві національної безпеки, Розвідувальному агентстві та інших важливих установах.

У суботу Об'єднане оперативне командування Іраку підтвердило серйозність ситуації, заявивши, що Національний центр кібербезпеки виявив «обмежену систему» в декількох федеральних урядових органах, в які було здійснено вторгнення.

Влада пояснила, що це не вплинуло на надання основних послуг і не спричинило жодних операційних збоїв, але ця інформація підкреслила постійну вразливість Іраку в галузі кібербезпеки.

У звіті зазначено, що вебсайти основних безпекових установ, зокрема Комісії з питань доброчесності та Міністерства охорони здоров'я, були успішно зламані.

Хоча іракська влада відтоді відновила контроль над зламаними сайтами, частота та масштаби таких інцидентів залишаються тривожними…» ***(Cyberattacks Target Iraqi Government Ministries, Security Agencies // BasNews.com (https://www.basnews.com/en/babat/894476). 14.09.2025).***

***

«…Нове опитування показує, що пакистанські фахівці наражають свої компанії на підвищений кіберризик через слабку безпеку пристроїв та ризиковану поведінку: хоча 70% використовують мобільні телефони для роботи поряд з комп'ютерами, а майже третина також використовує планшети, лише 70,8% стверджують, що встановили захист кібербезпеки на всіх пристроях, які мають доступ до бізнес-даних, а 7% не впевнені, чи їхні пристрої взагалі захищені. Така зростаюча залежність від численних, часто незахищених кінцевих точок створює легкі точки входу для зловмисників, які хочуть викрасти конфіденційну інформацію, поширити програми-вимагачі або порушити роботу. Ризиковані звички є широко поширеними: майже половина респондентів використовували робочі пристрої для особистих цілей, таких як перегляд відео, ігри, покупки або бронювання відпусток протягом останнього року; 49,5% підключали робочі пристрої до незахищених публічних мереж Wi-Fi; втрата та крадіжка пристроїв є поширеним явищем (22% втратили пристрій, 23% — стали жертвами крадіжки). Експерти з безпеки попереджають, що такі практики збільшують ризик атак — особисте використання підвищує вразливість до шкідливих веб-сайтів і неавторизованих додатків, а слабке або відсутнє шифрування в публічних мережах Wi-Fi дозволяє перехоплювати дані та встановлювати шкідливе програмне забезпечення». ***(Cybersecurity gaps expose***

businesses to attacks // The Express Tribune (https://tribune.com.pk/story/2567899/cybersecurity-gaps-expose-businesses-to-attacks). 20.09.2025).

***

«Рада з кібербезпеки ОАЕ попереджає, що недостатньо захищені посилання на віртуальні зустрічі є «відкритим запрошенням» для шахраїв, які можуть непомітно проникнути в сесії, підслуховувати, записувати розмови та красти спільні файли. Порушення, які різко зросли під час пандемії і зберігаються як у зустрічах державного, так і приватного сектору, часто виникають через повторне використання ідентифікаторів зустрічей, публічно розміщені або неправильно адресовані запрошення, слабкі або відсутні паролі та надто щедрі привілеї організатора… Щоб усунути ці прогалини, Рада закликає організаторів створювати новий випадковий ідентифікатор зустрічі та надійний унікальний пароль для кожної сесії; вмикати режими очікування та допускати учасників лише після перевірки їхніх імен; обмежувати доступ до офіційних зустрічей лише для автентифікованих облікових записів; а також заздалегідь встановлювати дозволи для обмеження спільного використання екрану, мікрофона та камери. Користувачам слід обережно ділитися посиланнями, завантажувати програми для відеоконференцій тільки з офіційних магазинів, увімкнути двофакторну автентифікацію та ретельно перевіряти дозволи програм, оскільки деякі шкідливі програми можуть таємно записувати дзвінки або активувати камери. Коротко кажучи, суворий контроль доступу, оновлені облікові дані та дисциплінованe управління посиланнями є необхідними для того, щоб конфіденційні обговорення та документи залишалися недоступними для хакерів…» ***(Abdulla Rasheed. UAE Cybersecurity Council warns of virtual meeting scams // Al Nisr Publishing LLC (https://gulfnews.com/uae/crime/uae-cybersecurity-council-warns-of-virtual-meeting-scams-1.500276703). 20.09.2025).***

***

«Ринок кібербезпеки Саудівської Аравії досяг 15,2 млрд саудівських ріалів у 2024 році, що на 14% більше, ніж у попередньому році, що відображає сукупні державні та приватні витрати на продукти та послуги. Приватний сектор становив 10,3 млрд саудівських ріалів (68%), а державний сектор — 4,8 млрд саудівських ріалів (32%). Попит зосереджений у основних економічних центрах — Ер-Ріяді, Мецці та Східній провінції, де розташовано 73% підприємств; пропозиція відображає цю концентрацію, оскільки 98% зареєстрованих у NCA постачальників мають штаб-квартири в цих регіонах (Ер-Ріяд — 77%, Мекка — 11%, Східна провінція — 10%). Цей сектор вніс 18,5 млрд саудівських ріалів (4,9 млрд доларів) у ВВП — 9,0 млрд саудівських ріалів безпосередньо (49%) і 9,5 млрд саудівських ріалів опосередковано (51%) — що еквівалентно 0,40% загального ВВП і 0,71% ненафтового ВВП. Витрати були майже рівномірно розподілені між продуктами (7,7 млрд саудівських ріалів, 51%) і послугами (7,5 млрд саудівських ріалів, 49%), а ключовими напрямками рішень були мережева безпека, захист і управління кінцевими точками, платформи для забезпечення безпеки, консультації

з управління кібербезпекою та безпека даних…» ***(Cybersecurity market size tops SAR 15B; private sector contributes 68% of total spending: NCA // Argaam Investment (https://www.argaam.com/en/article/articledetail/id/1844293). 19.09.2025).***

***

«Підполковник у відставці Годфі Стерлінг, директор відділу кібербезпеки Ямайки (CIRT), закликає організації по всій країні негайно посилити свої заходи з кіберзахисту. Стерлінг підкреслив, що проактивні заходи, такі як усунення вразливостей, швидке виправлення даних про порушення та обов'язкове повідомлення про інциденти, мають вирішальне значення для захисту цифрової інфраструктури Ямайки.

Він наголосив на важливості того, щоб системні адміністратори, ради директорів та керівництво ретельно контролювали весь життєвий цикл своїх систем — від закупівлі та встановлення виправлень до обслуговування та безпечного знищення — щоб «закрити прогалини, перш ніж буде завдано шкоди». Стерлінг також звернув увагу на часто ігноровані вразливості повсякденних пристроїв, таких як підключені до мережі принтери, які часто викидають без належного очищення даних, що може призвести до витоку конфіденційної інформації…

Стерлінг висловив серйозну стурбованість з приводу тривожної статистики, згідно з якою понад 70% атак програм-вимагачів у 2023 році були здійснені за допомогою скомпрометованих привілейованих облікових записів, які зловмисники потім використовували для проникнення в сторонні системи та повторного входу в основні мережі. Він підкреслив необхідність вжиття швидких заходів у разі компрометації даних, будь то через внутрішні мережі чи сторонні канали. Навіть якщо дані вже циркулюють у глибокій та темній мережі, організації повинні вжити необхідних захисних заходів, таких як зміна паролів та видалення скомпрометованих облікових записів…» ***(Organisations urged to take immediate steps to strengthen cyber security defences // The Gleaner Company (Media) Limited. https://jamaica-gleaner.com/article/news/20250926/organisations-urged-take-immediate-steps-strengthen-cyber-security-defences). 26.09.2025).***

***

Кіберстрахування

«…Попит на кіберстрахування стрімко зростає у фінансовому секторі Індії, де кооперативні та невеликі фінансові банки, небанківські фінансові компанії (NBFC) та фінтех-компанії приєднуються до давніх покупців у великих технологічних компаніях, оскільки цифровізація, зростання кількості атак, більш суворий регуляторний контроль та перспектива впровадження Закону про захист даних (DPDP) підвищують усвідомлення ризиків. Агрегатори та брокери, такі як Policybazaar, Plum та Nova Benefits, розширюють свою пропозицію на ринку, який оцінюється в 300–400 крор рупій і зростає приблизно на 50% у порівнянні з попереднім роком, з очікуванням, що зростання може прискоритися після набрання чинності законом про дані… Банки та платіжні

мережі спонукають своїх партнерів з фінтех-сектору придбати страховку як запобіжний захід для захисту від ризиків, пов'язаних з постачальниками, та для посилення внутрішньої безпеки. Ціноутворення все більше базується на ризиках: премії з 2018 року зросли приблизно втричі, оскільки сектори з вищим рівнем ризику (небанківські фінансові компанії, фінтех-компанії, охорона здоров'я) купують страховку; одна небанківська фінансова компанія, яка оцінювала поліс на суму 200 млн рупій, отримала пропозицію приблизно 800 тис. рупій на рік. Директива Резервного банку Індії від листопада 2023 року, яка закликає регульовані суб'єкти впроваджувати механізми зменшення ризиків, включаючи відповідне страхування, додає імпульсу цій тенденції. Щоб отримати право на кращі ціни, компанії проводять симуляції фішингу, навчання керівників, сканування безпеки та залучають експертів у цій галузі. Загалом, така зміна відображає як тиск зверху з боку великих фінансових гравців та регуляторних органів, так і усвідомлення знизу, що кіберінциденти становлять істотний фінансовий ризик та ризик для репутації…» ***(Pratik Bhakta, Ajay Rag. Fintechs, NBFCs run for cyber insurance cover amid rising threats // Bennett, Coleman & Co. Ltd. (https://economictimes.indiatimes.com/tech/technology/fintechs-nbfcs-run-for-cyber-insurance-cover-amid-rising-threats/articleshow/123793810.cms). 10.09.2025).***

***

«З огляду на те, що частота та вартість випадків використання програм-вимагачів, судових позовів щодо порушення безпеки та загроз для ланцюгів постачання зростають, покупці технологій, SaaS та аутсорсингових послуг посилюють вимоги до страхування кібервідповідальності, роблячи страхове покриття стандартною — і часто спірною — умовою контракту. Типові поліси покривають реагування на інциденти, повідомлення про порушення та регуляторні/юридичні витрати, переривання бізнесу через програми-вимагачі або порушення системи, відновлення даних та відповідальність перед третіми сторонами; ліміти відповідають профілю ризику, зазвичай 2–5 мільйонів доларів для постачальників малого та середнього бізнесу та 10 мільйонів доларів і більше для більших або високоризикових постачальників… Переговори зосереджуються на мінімальних необхідних лімітах і покритті, обсязі дії (наприклад, включаючи кібер-вимагання та порушення ланцюга поставок), на тому, чи є покупець додатково застрахованим і чи має право на сертифікати/перегляд полісу, на тому, як страхування взаємодіє з відшкодуваннями та обмеженнями відповідальності (наприклад, збереження покриття, рівного ризику, або обмеження відповідальності застрахованими сумами), а також на повідомленні про претензії та зобов'язаннях щодо співпраці. Транскордонні угоди додають складності: страхування часто доводиться оформляти у місцевих ліцензованих страховиків, доступність і страхові премії сильно різняться, поліси повинні забезпечувати покриття на всій території світу, а сторони повинні вирішити, як довго триватиме покриття після припинення договору, з огляду на різні строки позовної давності… У міру зростання кількості інцидентів і жорсткості ринкових умов — підвищення премій, звуження умов — клієнти чинять опір стандартним умовам, а постачальники стикаються з підвищенням витрат, що робить необхідним усунення прогалин у покритті без

надмірних витрат, які збільшують витрати або гальмують угоди…» ***(Anastasia Dergacheva and Michael R. Pfeuffer. Cyberinsurance Requirements in Tech Transactions: Balancing Risk and Market Practice // Morgan Lewis & Bockius LLP (https://www.morganlewis.com/blogs/sourcingatmorganlewis/2025/09/cyberinsurance-requirements-in-tech-transactions-balancing-risk-and-market-practice). 15.09.2025).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«Китай десятиліттями зламував американські енергомережі та компанії, викрадаючи конфіденційні файли та інтелектуальну власність, таку як розробка мікросхем, прагнучи отримати перевагу над Сполученими Штатами.

Але масштабна кібератака групи під назвою «Соляний тайфун» (Salt Typhoon) є найамбітнішою з усіх, що здійснила Китай, як дійшли висновку експерти та чиновники після року розслідування. За словами чиновників, вона була спрямована проти понад 80 країн і, можливо, вкрала інформацію майже в кожного американця. Вони розглядають це як доказ того, що можливості Китаю можуть конкурувати зі Сполученими Штатами та їхніми союзниками.

Атака «Соляного тайфуну» була багаторічною скоординованою атакою, яка проникла у великі телекомунікаційні компанії та інші, повідомили слідчі у вкрай незвичайній спільній заяві минулого тижня. Масштаб атаки був набагато більшим, ніж вважалося спочатку, і представники служби безпеки попередили, що викрадені дані можуть дозволити китайським розвідувальним службам використовувати глобальні комунікаційні мережі для відстеження цілей, включаючи політиків, шпигунів та активістів.

У заяві йдеться, що хакери, яких спонсорує китайський уряд, «націлені на мережі по всьому світу, включаючи, але не обмежуючись, телекомунікаційні, урядові, транспортні, житлові та військові інфраструктурні мережі».

Британські та американські чиновники назвали напад «нестримним» та «невибірковим». Канада, Фінляндія, Німеччина, Італія, Японія та Іспанія також підписали заяву, яка була частиною зусиль з метою очорнення китайського уряду… Не було зрозуміло, чи хакерська атака «Соляний тайфун» мала на меті збереження даних звичайних людей, чи ці дані були випадково викрадені під час атаки. Але її масштаб був ширшим, ніж попередні хакерські атаки, в яких Китай більш вузько націлювався на західних фахівців, що працюють у сфері безпеки або інших чутливих урядових питаннях…» ***(Adam Goldman. 'Unrestrained' Chinese Cyberattackers May Have Stolen Data From Almost Every American // The New York Times Company (https://www.nytimes.com/2025/09/04/world/asia/china-hack-salt-typhoon.html). 04.09.2025).***

***

«Кібершпигуни, пов'язані з урядом Китаю, видавали себе за ключового законодавця-республіканця з Палати представників у рамках змови з метою підриву національної безпеки...

«Хакери надіслали електронні листи, нібито від імені конгресмена Джона Муленаара (республіканець від штату Мічиган), ключовим лідерам напередодні зустрічі між представниками США та Китаю в Швеції цього літа, просячи надати коментарі щодо законопроекту», — йдеться у звіті. «Однак доданий документ, надісланий з недержавної електронної адреси, містив шпигунське програмне забезпечення, яке заражало комп'ютер жертви».

Муленаар є головою Спеціального комітету Палати представників з питань Китаю. Згідно зі звітом, слідчі пов'язали хакерів з Міністерством державної безпеки Китаю.

«Це ще один приклад агресивних кібероперацій Китаю, спрямованих на викрадення американської стратегії та використання її проти Конгресу, адміністрації та американського народу», – заявив Муленаар у заяві, опублікованій у понеділок…» ***(Matthew Chapman. Chinese spies impersonated key House Republican to infect US government with malware // Raw Story Media, Inc. (https://www.rawstory.com/chinese-spies/). 08.09.2025).***

***

«…Війна стає децентралізованою і технологічною, з використанням дронів і шкідливого коду, що вражають критичну інфраструктуру далеко від традиційних ліній фронту, змушуючи західні уряди захищатися одночасно на всіх фронтах і переосмислювати поняття «оборони» з точки зору кібербезпеки та стійкості. НАТО продемонструвало цю зміну на своєму нещодавньому саміті, прийнявши рішення збільшити видатки на оборону до 5% ВВП і підтвердивши статтю 5, тоді як США тиснуть на Велику Британію та Європу, щоб вони стали більш самодостатніми, а останній огляд Великої Британії визнає нагальність цього питання… Кібератаки набувають все більшого розмаху — Україна повідомляє про їхнє збільшення приблизно на 70% у 2024 році, причому більшість з них спрямована проти урядових систем і все більше зосереджується на системах управління та контролю, а руйнівні операції зараз загрожують енергомережам, трубопроводам і підводним кабелям у всьому Західному світі. Паралельно з цим, автономність на основі штучного інтелекту змінює обличчя поля бою: недорогі дрони України проникли глибоко в територію росії — 343 дрони навколо Москви в березні та операція «Павутина», в рамках якої було запущено понад 100 дронів на відстань до 4500 км — продемонстрували масштабовані, точні удари, але також викрили дешеві, підключені до мережі системи, які можуть бути зламані та використані зловмисними державами або терористами, випереджаючи застарілі засоби захисту. Члени НАТО починають адаптуватися: Великобританія співпрацює з промисловістю з метою зміцнення енергетичної інфраструктури та прискорення відновлення комунікацій, але для надійної реакції зараз потрібні більші бюджети, що включають кібербезпеку та інфраструктуру, прискорення технологічних інновацій та тіснішу співпрацю між урядом і промисловістю для підвищення гнучкості та національної стійкості…» **(*Toby Wilmington.* I built NATO's incident response capabilities before becoming a cyber CEO. My business is becoming the new defense sector // Fortune Media IP Limited**

(https://fortune.com/2025/09/07/cyber-is-turning-into-the-new-defense-former-nato-turned-ceo/). 07.09.2025).

***

«Кіберзапобігання набуває все більшого значення, оскільки лідери НАТО поставили за мету до 2035 року витратити 5% ВВП на оборону та запобігання, включаючи кіберзапобігання, а Комітет Сенату США з питань збройних сил доручив Пентагону розробити стратегію відновлення надійного запобігання кібератакам на критичну інфраструктуру з використанням усього спектру військових операцій. Ці кроки підкреслюють стримування шляхом покарання — урядові наступальні кіберможливості та надійне правозастосування — але не менш важливим, хоча й часто недооціненим, є стримування шляхом відмови від вигоди: зміцнення стійкості, щоб атаки зазнавали невдачі або ставали надто дорогими… Державні суб'єкти все частіше націлюються на критичну інфраструктуру напередодні конфлікту, щоб відволікти увагу урядів і порушити логістику, транспорт і комунікації, і більшість їхніх атак є опортуністичними, використовуючи незахищені системи та прогалини в базовій гігієні для досягнення економічно ефективного порушення роботи цілого сектора. Оскільки супротивники стикаються з обмеженнями ресурсів і ризиками викриття, добре підготовлені організації мають більше шансів виявити, відлякати і уникнути атак, які будуть спрямовані на більш вразливі цілі…

Побудова стійкості охоплює зміцнені мережі, навчання кінцевих користувачів та інструменти, а також галузеві ініціативи, що підвищують базовий рівень безпеки в секторах, захист яких є настільки сильним, наскільки сильним є його найслабша ланка. Це також приносить бізнес-дивіденди — економію витрат та оперативну гнучкість, наприклад, кілька програмно-визначених мережевих шляхів замість одноточкової надмірності, — що робить стійкість стратегічною необхідністю як для держав, критичної інфраструктури, так і для компаній, орієнтованих на прибуток…» ***(Jim Richberg. Cyber Resilience: The Underappreciated Side Of Deterrence // Forbes (https://www.forbes.com/councils/forbestechcouncil/2025/09/08/cyber-resilience-the-underappreciated-side-of-deterrence/). 08.09.2025).***

***

«…Великобританія публічно звинувачує лише чотири країни у ворожих хакерських атаках — Росію, Китай, Іран та Північну Корею — проте дипломати та представники розвідки приватно визнають, що багато друзів і партнерів також займаються шпигунством, купують шпигунське програмне забезпечення або закривають очі на вторгнення місцевих компаній. Небажання Лондона «викривати» союзників пояснюється торговою дипломатією та побоюванням розриву партнерських відносин у сфері безпеки, тому міністри публічно звинувачують лише так звану «велику четвірку»…

Ця практика контрастує з більш сміливим підходом Вашингтона: Сполучені Штати вперше звинуватили Китай у 2014 році, пізніше внесли до чорного списку ізраїльського постачальника шпигунського програмного забезпечення NSO Group і

заборонили федеральним органам використовувати комерційні засоби спостереження з високим рівнем ризику. Великобританія вперше звинуватила державу (Росію) лише у 2018 році і досі не наклала санкцій на жодного постачальника шпигунського програмного забезпечення…

Тим часом бурхливий розвиток приватного ринку перетворив хакерство на послугу, доступну за одним кліком миші. За повідомленнями, щонайменше 80 країн придбали комерційне шпигунське програмне забезпечення; дослідження показують, що основні кластери постачальників знаходяться в Ізраїлі, Індії та Італії. Такі держави, як Індія та Ізраїль — близькі партнери Великої Британії — були пов'язані через витоки інформації та дослідження з наступальними кіберкампаніями, але Лондон зберігає мовчання. Офіційні особи визнають, що зараз більша загроза походить не від традиційних розвідувальних агентств, а від приватних фірм, які продають готові експлойти будь-якому уряду, готовому за них заплатити…

Щоб зупинити цю торгівлю, Велика Британія та Франція започаткували «Pall Mall Process» — добровільний кодекс поведінки, покликаний обмежити поширення шпигунського програмного забезпечення. Однак жодна з провідних країн-експортерів та великих постачальників не підписала цей кодекс, що обмежує його ефективність. З огляду на те, що нова адміністрація США виявляє поновлений інтерес до використання комерційного шпигунського програмного забезпечення, розрив між жорсткими санкціями Вашингтона та м'якшою дипломатією Лондона може збільшитися…

Аналітики стверджують, що балансування Великобританії — підтримання союзів, забезпечення торговельних угод після Brexit та очолювання глобальної боротьби зі шпигунським програмним забезпеченням — стає дедалі складнішим: «Велика четвірка» домінує в заголовках новин, але тихіша кібердіяльність друзів та процвітаючий глобальний ринок, який їх оснащує, є загрозою, з якою Великобританія бореться або навіть не може назвати…» ***(Mason Boycott-Owen. The rogue hacker states Britain doesn't want to talk about // POLITICO (https://www.politico.eu/article/when-the-whole-world-is-hacking-how-does-britain-uk-say-stop/). 10.09.2025).***

***

«Дослідники попереджають , що китайський зловмисник атакував філіппінську військову компанію за допомогою раніше невідомої безфайлової системи шкідливого програмного забезпечення .

Раніше цього тижня компанія з кібербезпеки Bitdefender опублікувала детальний звіт про EggStreme, «багатоетапний набір інструментів, який досягає малопомітного шпигунства шляхом впровадження шкідливого коду безпосередньо в пам'ять та використання завантаження DLL для виконання корисних навантажень».

Він налічує шість різних компонентів: EggStremeFuel (початкова DLL-бібліотека завантажувача, що завантажується непрямим способом через легітимний бінарний файл та встановлює зворотну оболонку), EggStremeLoader (зчитує зашифровані корисні навантаження та вставляє їх у процеси),

EggStremeReflectiveLoader (розшифровує та вставляє кінцеве корисне навантаження), EggStremeAgent (основний імплант бекдора з 58 командами), EggStremeKeylogger (перехоплює натискання клавіш та конфіденційні дані користувача) та EggStremeWizard (додатковий бекдор для резервування).

Bitdefender спробував пов’язати фреймворк із відомими китайськими гравцями APT, але не зміг знайти правдоподібного зв’язку...

Цілями цієї операції, схоже, є кібершпигунство, розвідка та довгострокова, маловідома наполегливість, чим відомі китайські актори – не лише на Філіппінах, а й в інших частинах регіону (В'єтнам, Тайвань та інші сусідні країни), а також у всьому світі…» ***(Sead Fadilpašić. China-related threat actors deployed a new fileless malware against the Philippines military // Future US, Inc. (https://www.techradar.com/pro/security/china-related-threat-actors-deployed-a-new-fileless-malware-against-the-philippines-military). 11.09.2025).***

***

«27 серпня 2025 року Агентство з кібербезпеки та безпеки інфраструктури (CISA) у координації з Агентством національної безпеки (NSA), Федеральним бюро розслідувань (FBI) та Центром боротьби з кіберзлочинністю Міністерства оборони США (DC3) опублікували спільну рекомендацію, співавторами та прихильниками якої виступили партнери з Австралії, Канади, Нової Зеландії, Великої Британії, Чехії, Фінляндії, Німеччини, Італії, Японії, Нідерландів, Польщі та Іспанії. У ній міститься попередження про посилення активності з боку спонсорованих державою КНР зловмисників, які націлені на мережі по всьому світу в таких секторах, як телекомунікації, уряд, транспорт, житло та військова інфраструктура… Зловмисники використовують загальновідомі вразливості в периферійних пристроях, особливо в маршрутизаторах, які часто не мають надійного моніторингу, щоб отримати початковий доступ, а потім використовують скомпрометовані пристрої та надійні з'єднання, щоб проникнути глибше, змінюють конфігурації маршрутизаторів для поперечного переміщення, використовують нестандартні порти, щоб уникнути виявлення, «живуть за рахунок ресурсів» за допомогою викрадених облікових даних та інструментів з відкритим кодом, які обходять AV/EDR, а також маніпулюють або видаляють журнали, щоб приховати свої сліди. Посилаючись на нещодавні операції таких груп, як Salt Typhoon (інфільтрація американських телекомунікаційних агентств), Volt Typhoon (вторгнення в критичну інфраструктуру США, включаючи електричні та водопровідні системи) та Flax Typhoon (санкціонована за діяльність ботнету), у рекомендаціях зазначається розширення фокусу за межі телекомунікацій та критичної інфраструктури. Він закликає захисників активно виявляти зловмисну діяльність і розуміти весь масштаб порушення безпеки перед усуненням, щоб максимізувати шанси на повне виведення з ладу, а також рекомендує перевіряти журнали та конфігурації маршрутизаторів на наявність аномалій; застосовувати суворе управління змінами та періодичні аудити; оцінку масштабів інцидентів перед вжиттям заходів; відключення вихідних з'єднань з інтерфейсів управління та всіх невикористовуваних портів/протоколів; використання лише зашифрованих,

автентифікованих протоколів управління (SSH, SFTP/SCP, HTTPS) з відключенням Telnet/FTP/HTTP; зміну стандартних облікових даних адміністратора; перевагу автентифікації за допомогою відкритого ключа та обмеження спроб введення пароля; а також підтримку мережевих пристроїв на рекомендованих виробником, повністю оновлених версіях, замінюючи обладнання, що не підтримується. Організаціям рекомендується зберігати підвищену готовність в умовах міжнародної напруженості...» ***(Kim Peretti, Lance Taubin and Andrew Rice. United States, International Coalition Issue Joint Warning of Increasing PRC Backed Threat Activity // Alston & Bird (https://www.alstonprivacy.com/united-states-international-coalition-issue-joint-warning-of-increasing-prc-backed-threat-activity/). 10.09.2025).***

***

«Бюлетень Управління директора національної розвідки (ODNI) «Захист академічної спільноти» (25 серпня 2025 р.), опублікований через Національний центр контррозвідки та безпеки (NCSC) та партнерські агентства, попереджає, що іноземні супротивники використовують відкриту культуру співпраці американських університетів, загрожуючи дослідженням, репутації та дотриманню нормативних вимог, і пропонує конкретні рекомендації щодо зменшення ризиків. У ньому детально описано систематичні зусилля з витоку даних до публікації, інтелектуальної власності, лабораторних протоколів та технічних ноу-хау, причому Китай виділяється як країна, яка постійно націлена на штучний інтелект, квантові технології, напівпровідники, гіперзвукові технології, біотехнології та інші ключові технології для досягнення економічних і військових цілей. Державні програми залучення талантів заманюють викладачів, аспірантів та студентів фінансуванням, зарплатами та візами, створюючи ризики, що охоплюють порушення експортного контролю та санкцій, економічне шпигунство, конфлікти інтересів, суперечки щодо власності на інтелектуальну власність, шахрайство з грантами та податками, а також потенційну втрату федерального фінансування. Нерозкриті іноземні гранти та партнерства можуть надати супротивникам доступ до досліджень, що фінансуються за рахунок платників податків, та наражати установи та дослідників на адміністративні санкції, скасування грантів та кримінальну відповідальність. Супротивники також примушують студентів та дослідників або вбудовують своїх агентів, ставлячи під загрозу академічну свободу та створюючи можливості для шантажу, тоді як внутрішні та кіберзагрози — фішинг, шкідливе програмне забезпечення, соціальна інженерія та поширення інформації в соціальних мережах — збирають облікові дані та викрадають величезні масиви даних. ODNI закликає університети формувати культуру безпеки, ретельно оцінювати ризики, пов'язані з дослідженнями та фінансуванням, забезпечувати суворе дотримання правил щодо подорожей, кібербезпеки та гігієни використання пристроїв, посилювати звітність та використовувати державні ресурси, а також проводити спеціалізовані тренінги з питань безпеки та етики. Установи повинні збалансувати відкритість та безпеку шляхом розкриття інформації, забезпечення дотримання політик, технічного контролю та навчання всього співтовариства, а також підготуватися до посиленого контролю з боку Конгресу, особливо щодо зв'язків з Китаєм, у міру посилення двопартійних

розслідувань та розширення нагляду…» ***(Ricardo Brandon Rios, Nadia Asancheyev, Andrew Binstock, Victoria Busch. ODNI's "Safeguarding Academia" bulletin: Key implications for higher education institutions // DLA Piper (https://www.dlapiper.com/en/insights/publications/2025/09/odni-safeguarding-academia-bulletin-key-implications-for-higher-education-institutions). 09.2025).***

***

«…Google виявив триваючу, дуже складну кампанію кібершпигунства, в рамках якої хакери, пов'язані з китайською державою, — головним чином група, відома як UNC5221 — проникають у системи американських постачальників технологій, провайдерів SaaS та великих юридичних фірм, а потім переходять у мережі клієнтів цих компаній. Зловмисники прочісують електронні поштові скриньки в пошуках інформації про питання національної безпеки та торгівлі США, переглядають листування юридичних фірм і викрадають вихідний код підприємств, щоб знайти в ньому невідомі вразливості, які можуть бути використані для майбутніх атак.

Їхній ключовий імплант, бекдор під назвою «Brickstorm», встановлюється на пристрої, які не можуть запускати засоби виявлення кінцевих точок або антивірусні інструменти (гіпервізори VMware ESXi, шлюзи електронної пошти, сканери вразливостей), що дозволяє зловмисникам залишатися невиявленими в середньому протягом 393 днів — надзвичайно довгого часу перебування. UNC5221 також уникає повторного використання IP-інфраструктури, що робить порушення надзвичайно важкими для відстеження, і є провідним експлуатувальником вразливостей Ivanti Connect Secure VPN та інших вразливостей периферійних пристроїв для початкового доступу…

Google порівнює цю операцію з кампанією по ланцюжку поставок à la SolarWinds: компрометуючи постачальників послуг, шпигуни можуть «вибирати» цілі нижчого рівня. Щоб допомогти потенційним жертвам, Google випускає утиліту для сканування Brickstorm і правила YARA, попереджаючи, що багато організацій виявлять історичні або активні компрометації. Оскільки журнали з початкового доступу часто зникають, повне виправлення буде складним, і Google очікує, що протягом наступних двох років з'явиться більше жертв…» ***(Eric Geller. China-linked groups are using stealthy malware to hack software suppliers // TechTarget, Inc. (https://www.cybersecuritydive.com/news/china-espionage-supply-chain-cyberattack-backdoor-malware/760917/). 24.09.2025).***

***

Створення та функціонування кібервійськ

«Королівська армія Нідерландів розгортає хакерів на передовій у складі новосформованого 101-го батальйону CEMA, повідомили офіційні особи у четвер. …підрозділ …об'єднує компанії, що спеціалізуються на радіоелектронній боротьбі та кіберопераціях.

Електронна війна включає порушення зв'язку противника та відстеження супротивників за допомогою виявлення сигналів...

Під час ранніх експериментів солдати зламували веб-камери, розумні дверні дзвінки та роботизовані пилососи, щоб збирати розвідувальні дані про будівлі, де утримуються заручники. В Україні хакери можуть брати під контроль розвідні мости, щоб блокувати просування противника, не руйнуючи інфраструктуру назавжди.

Польова хакерська атака — це новіша можливість. «У нас могло б бути більше, якби дозволяв військовий бюджет», — сказав підполковник Пітер Масселінг, командир 101-ї CEMA...

Обмеження на фінансування вже знято. Наразі в батальйоні працює 20 хакерів, і планується збільшити їхню кількість до 50 у підрозділі з 250 осіб. Протягом наступних п'яти років, як повідомляється, у відділ кібербезпеки та електронної боротьби будуть інвестовані мільйони. Кінцева мета — три батальйони, щоб кожна бригада мала спеціалістів з кібербезпеки...

101-й батальйон CEMA безпосередньо впроваджує хакерів у бойові підрозділи, на відміну від Кіберкомандування, яке діє з баз для порушення роботи ворожих систем. Більшість членів навчені для розгортання на передовій, тоді як підрозділ також включає кваліфікований персонал, який працює в тилу та не відповідає фізичним військовим вимогам». ***(Dutch army to deploy hackers to front lines to gain battlefield advantage // NL Times (https://nltimes.nl/2025/09/13/dutch-army-deploy-hackers-front-lines-gain-battlefield-advantage). 13.09.2025).***

***

Кіберзахист закладів охорони здоров'я

«…Сільські лікарні стикаються з гострими проблемами кібербезпеки — обмеженим фінансуванням, труднощами із залученням та утриманням кваліфікованого IT-персоналу в галузі охорони здоров'я, а також значною залежністю від сторонніх постачальників, що збільшує ризики. Тому багато хто з них звертається до стратегічних партнерств, щоб підвищити свою стійкість. Лікарня Натана Літтауера (Гловерсвілл, штат Нью-Йорк) ілюструє такий підхід: партнерство з Clearwater Security для посилення невеликої команди за допомогою vCISO та SOC, приведення у відповідність до 405(d) Практик кібербезпеки в галузі охорони здоров'я для малих організацій та формалізації реагування на інциденти, використовуючи оцінку ризиків для визначення пріоритетності інвестицій відповідно до Закону штату Нью-Йорк про кібербезпеку лікарень. Вимоги закону — MFA, засоби аудиту, оновлення застарілої інфраструктури та операційних систем, а також додаткове управління (звітування на рівні правління, щорічне затвердження політик) — підвищують рівень безпеки, але обтяжують бюджети та збільшують адміністративне навантаження поряд з безперебійною щоденною роботою, що робить управління змінами та комунікацію з кінцевими користувачами критично важливими для уникнення перебоїв у роботі. Оцінка ризиків лікарні підкреслила необхідність глибокого та детального аналізу всієї

організації, тривогу, яку можуть викликати такі перевірки, а також важливість наголошення на тому, що висновки стосуються процесів і заходів безпеки, а не окремих осіб. Відверті коментарі співробітників дозволили скласти реєстр ризиків і практичний план дій, який перетворив дотримання вимог на інструмент планування. Щоб зменшити «сліпі зони», команда поєднує постійний моніторинг та зовнішню валідацію з високою видимістю залучення — округлення, комітети з робочих процесів та доступні ІТ — щоб зрозуміти клінічні та неклінічні процеси та вирішити проблему людського фактора, який все ще є головним джерелом ризику. Це поєднання зовнішньої експертизи, пріоритетних заходів з усунення недоліків та постійної комунікації допомагає невеликим лікарням підвищити рівень безпеки, незважаючи на обмежені ресурси…» ***(Andrea Fox. How to address 'cyber-uncertainty' and ensure your IT team's success // HIMSS Media (https://www.healthcareitnews.com/news/how-address-cyber-uncertainty-and-ensure-your-it-teams-success). 08.09.2025).***

***

«…Попри зростання бюджетів і усвідомлення кіберризиків, найуразливішим місцем у захисті медичних закладів залишається електронна пошта. Більшість атак — це фішинг: зловмисники проникають не через складні медичні системи, а через інбокси співробітників… Дослідження EasyDMARC показало, що понад половина з 2 000 провідних американських медичних організацій запровадили стандарт автентифікації DMARC, однак лише 15 % справді блокують підозрілі повідомлення, тоді як 40 % використовують найслабший режим, який лише фіксує, але не зупиняє загрозу. У медичному середовищі, де ІТ-команди зосереджені на безперебійному функціонуванні ЕМК та обладнання, пошта традиційно вважається другорядною інфраструктурою, хоча нею користується майже кожен працівник. Ситуацію загострюють нові вимоги Google, Yahoo та Microsoft: від 2024 р. вони вимагають суворого дотримання DMARC для масових відправників; невиконання ставитиме під загрозу доставлення листів, відповідність нормам і, зрештою, довіру пацієнтів. У секторі, де ціна помилки вимірюється не лише штрафами, а й якістю догляду, перехід від пасивного моніторингу до активного блокування та коректної конфігурації наявних інструментів має стати базовим стандартом кібербезпеки…» ***(Gerasim Hovhannisyan. Email: the weak link in healthcare cybersecurity // Future US, Inc. (https://www.techradar.com/pro/email-the-weak-link-in-healthcare-cybersecurity). 18.09.2025).***

***

«Сектор охорони здоров'я, який в основному базується на довірі та вразливості, стикається з ескалацією кризи кібербезпеки, причому порушення залишаються найпоширенішими та найдорожчими серед усіх галузей. У 2024 році американські компанії, що надають медичні послуги, повідомили про 588 порушень, в результаті яких було викрадено приблизно 180 мільйонів записів про пацієнтів — в середньому понад 750 000 записів щодня — що зробило людей вразливими до крадіжки особистих даних, фінансового шахрайства або затримки в

наданні медичної допомоги. Фінансові наслідки є жахливими: у 2025 році середня вартість порушення безпеки в секторі охорони здоров'я в США склала 7,42 мільйона доларів, що значно перевищує середній світовий показник і є найвищим показником за останні п'ятнадцять років поспіль. Більше того, виявлення та усунення цих порушень займає в середньому 279 днів, що подовжує крадіжку даних та перебої в роботі.

Недавні гучні інциденти підкреслюють системний вплив цих атак. Атака програм-вимагачів у 2024 році на Change Healthcare, велику американську компанію, що обробляє страхові виплати, торкнулася 190 мільйонів американців, паралізувавши обробку страхових виплат, зупинивши платежі та затримавши перевірку рецептів у лікарнях, клініках та аптеках. Аналогічно, спалах вірусу-вимагача Synnovis у Великій Британії коштував понад 32 мільйони фунтів стерлінгів на відновлення, оприлюднив сотні терабайтів даних про пацієнтів і змусив лондонські лікарні відкласти необхідну діагностику. Ці випадки демонструють, як одне порушення може паралізувати всю екосистему охорони здоров'я…

Згідно з доповіддю Verizon про розслідування випадків порушення безпеки даних, методи зловмисників постійно вдосконалюються, а майже 70% порушень у сфері охорони здоров'я відбуваються з вини інсайдерів через помилки, необізнаність або зловмисні наміри. Одночасно зовнішні зловмисники все частіше використовують незахищені вразливості, кількість яких як початковий вектор атак зросла на 180% у порівнянні з минулим роком, і запускають складні кампанії з використанням програм-вимагачів та фішингу, використовуючи вразливості старих систем та нестачу персоналу в IT-відділах.

Нові технології ще більше ускладнюють ситуацію. Генеративна штучна інтелігенція прискорила фішинг і соціальну інженерію, а автоматизовані засоби розвідки дозволяють зловмисникам швидко сканувати мережі на наявність вразливостей. IBM повідомляє, що атаки на основі штучного інтелекту коштують на мільйони дорожче, ніж традиційні порушення, а «тіньові» програми штучного інтелекту в підприємствах додають значних витрат. Однак штучний інтелект також пропонує захисникам потужні інструменти для швидшого виявлення та реагування, якщо ним керувати етично та ефективно.

Регулюючі органи, зокрема Міністерство охорони здоров'я та соціальних служб, реагують на це, вимагаючи не лише дотримання контрольних списків; тепер вони очікують від підприємств демонстрації комплексного управління ризиками в масштабах всієї організації, постійного нагляду за постачальниками та ретельно перевірених планів реагування на інциденти. Це означає, що кібербезпека більше не є лише проблемою IT, а є критично важливим питанням організаційного управління і, по суті, безпеки пацієнтів…

Вирішення цієї нагальної проблеми вимагає стратегічних змін. Кібербезпека повинна бути невід'ємною частиною клінічної безпеки. Організації охорони здоров'я повинні перейти від одноразових перевірок відповідності до постійного управління ризиками, створити надійні архітектури з сегментованими системами, впровадити автоматичне виявлення та реагування, а також проводити часті навчання з клінічним керівництвом. Операційна кібергігієна, включаючи

встановлення виправлень, багатофакторну автентифікацію, зашифровані резервні копії та перевірені плани відновлення, є обов'язковою. Інвестиції в персонал, що відповідає за безпеку, є не менш важливими, оскільки нестача кадрів призводить до мільйонних збитків від порушень, навіть у секторі з обмеженими ресурсами.

Зрештою, стійкість кібербезпеки в галузі охорони здоров'я вимагає спільних зусиль. Жодна лікарня, страхова компанія чи постачальник не може самостійно протистояти цим загрозам. Галузь потребує комплексних програм обміну інформацією, скоординованого планування на випадок надзвичайних ситуацій та надійної співпраці між державним і приватним секторами. Пацієнти також повинні бути залучені через прозору комунікацію після порушення, допомогу в захисті ідентичності та просування цифрової грамотності…» ***(Chuck Brooks. Healthcare Cybersecurity: The Urgency Of Now // Forbes Media LLC. (https://www.forbes.com/sites/chuckbrooks/2025/09/23/healthcare-cybersecurity-the-urgency-of-now/). 23.09.2025).***

***

Захист персональних даних та соціальні мережі

«У сучасному гіперпідключеному світі просторові дані — цифровий слід, що вказує географічне розташування — стали однією з найцінніших і найчутливіших форм інформації. На відміну від інших даних, вони не тільки повідомляють нам, де щось знаходиться, але й розкривають, коли, як, хто і чому, що дозволяє використовувати їх у критично важливих сферах, таких як логістика, містобудування, моніторинг клімату, точне землеробство, управління надзвичайними ситуаціями і навіть національна безпека. Завдяки сучасним датчикам, GPS, дронам, пристроям IoT та мережам 5G, постійно збираються величезні потоки просторових даних у реальному часі. За допомогою хмарних обчислень, аналізу великих даних та штучного інтелекту ця необроблена інформація перетворюється на інтелектуальні дані, що сприяють інноваціям, таким як цифрові двійники, та змінюють спосіб нашої взаємодії з фізичним світом.

Однак цей величезний потенціал супроводжується не менш величезними ризиками для кібербезпеки. Несанкціонований доступ до даних про місцезнаходження загрожує особистій конфіденційності — розкриттям домашніх адрес, конфіденційної інформації про повсякденний розпорядок дня або пересуваннях керівників — та корпоративній конфіденційності, наприклад, розкриттям критично важливих маршрутів ланцюгів постачання або місце Ще більшу небезпеку становлять підробка або зловмисні маніпуляції: наприклад, підробка GPS-сигналів може збити з курсу кораблі, літаки або автономні транспортні засоби, що може мати катастрофічні наслідки. Атаки на доступність, такі як глушіння GPS-сигналів або атаки типу «відмова в обслуговуванні», можуть паралізувати роботу, зупинити польоти, заблокувати роботу портів і вивести з ладу служби екстреної допомоги…

Для захисту цього життєво важливого ресурсу необхідні три основи кібербезпеки. По-перше, надійне управління даними забезпечує належну класифікацію, враховуючи, що координати критичної інфраструктури вимагають набагато більшого захисту, ніж місцезнаходження роздрібного магазину. По-друге, надійні практики управління даними захищають інформацію за допомогою шифрування, контролю доступу, перевірок цілісності та планів відновлення. По-третє, аналіз даних — з використанням систем аналізу загроз — переводить захист з реактивного на проактивний, виявляючи методи зловмисників, передбачаючи ризики та виявляючи ранні ознаки небезпеки…

Нові технології також формують майбутнє безпеки просторових даних. Штучний інтелект може аналізувати величезні масиви даних для швидшого виявлення аномалій, блокчейн може створювати незмінні записи, що захищають від фальсифікацій, а методи аналізу, що зберігають конфіденційність, дозволяють отримувати інформацію без розкриття чутливих деталей.

Оскільки суспільства все більше покладаються на інформацію про геолокацію для стимулювання інновацій та підвищення ефективності, її захист є не просто опцією, а необхідністю. Впроваджуючи надійну кібербезпеку в життєвий цикл просторових даних, уряди, організації та окремі особи можуть повністю розкрити її трансформаційний потенціал, одночасно забезпечуючи безпеку та стійкість основ нашого цифрового майбутнього…» ***(Louai Alarabi. Spatial data: What is it and why is cybersecurity so vital to it? // World Economic Forum (https://www.weforum.org/stories/2025/09/spatial-data-what-is-it-and-why-is-cybersecurity-so-vital-to-it/). 04.09.2025).***

***

«…Конфіденційність персональних даних та кібербезпека в арбітражі регулюються в першу чергу різноманітними національними імперативними законами, а не конкретними арбітражними статутами чи правилами. Хоча ці закони опосередковано впливають на обробку доказів, потенційно обмежуючи розкриття або подання певних документів, що містять персональні дані, їхня актуальність виходить за межі суто процедурних міркувань. Дотримання вимог законодавства про захист даних та кібербезпеку є обов'язковим для юридичних фірм, сторін та арбітрів, що робить необхідним управління арбітражем таким чином, щоб забезпечити дотримання цих вимог усіма учасниками…

Кібербезпека в арбітражі стосується автентичності та цілісності цифрових даних, які становлять основну частину сучасних документальних доказів та комунікацій. Легкість, з якою можна змінювати цифрові записи, та складність перевірки їх автентичності або ідентифікації «оригіналу», коли фізичного еквівалента не існує, становлять значну кіберзагрозу. Це вимагає вжиття захисних заходів для запобігання маніпуляціям, включаючи обмеження фізичного доступу до обладнання, впровадження надійного управління правами користувачів, визначення законних користувачів за допомогою багатофакторної автентифікації та забезпечення регулярного, зашифрованого та з позначкою часу резервного копіювання надійним ІТ-персоналом. Ці заходи збільшують ймовірність виявлення прихованих маніпуляцій з даними судовими експертами…

Окрім цілісності даних, кібербезпека також бореться із загрозою несанкціонованого проникнення в систему з метою отримання конфіденційної, привілейованої або секретної інформації, такої як рішення трибуналу. Такі вторгнення часто використовують вразливість системи або людську помилку (наприклад, фішинг). Контрзаходи включають миттєві оновлення програмного забезпечення, брандмауери, вкладені права доступу, надійне управління паролями з вторинною автентифікацією, примусове виходу з системи, складний моніторинг на основі штучного інтелекту, шифрування даних та обов'язкове навчання користувачів. Ці заходи, хоча і не забезпечують повного захисту, мають на меті зробити незаконний доступ економічно непривабливим. Вони також відповідають законам про захист персональних даних, які вимагають обмежень на використання даних. Іншим аспектом кібербезпеки є захист функціональності системи від саботажу, такого як атаки програм-вимагачів, шляхом впровадження надійних планів відновлення даних і систем.

Арбітраж ставить унікальні виклики в галузі кібербезпеки через свій тимчасовий, багатоюрисдикційний характер, що передбачає участь сторін, адвокатів та арбітрів, які утворюють тимчасову систему. Незважаючи на відсутність конкретних арбітражних правил щодо мінімальних технічних стандартів, усі учасники зобов'язані дотримуватися національних імперативних законів. З огляду на технічну складність та вимоги до ресурсів, прагматичним підходом є вирішення питань кібербезпеки на ранній стадії провадження, оцінка конкретних загроз та впровадження узгоджених процедурних розпоряджень. Ці розпорядження зазвичай охоплюють наскрізне шифрування, обмеження хмарного зберігання (шифрування з нульовим розкриттям інформації, розташування сервера), доступ за необхідністю (за винятком субпідрядників без конкретних угод), правила безпечного зберігання, збереження та знищення розкритих матеріалів та матеріалів справи, а також обов'язки щодо повідомлення у разі порушення…

Для окремих арбітрів або невеликих фірм, які не мають широкої IT-підтримки, мінімальні необхідні вимоги до кібербезпеки включають спеціальні комп'ютери, захищені паролем, з постійно оновлюваним програмним забезпеченням, шифруванням жорсткого диска, використанням облікових записів користувачів без прав адміністратора, безпечними налаштуваннями веб-браузера, необхідними програмами з надійних джерел з обмеженими правами доступу, постійно оновлюваними антивірусами та особистими брандмауерами, зашифрованими Wi-Fi-з'єднаннями та можливостями віддаленого видалення даних з мобільних пристроїв…

Людський фактор залишається найслабшою ланкою, що вимагає вжиття заходів безпеки, таких як уникнення використання ненадійного програмного забезпечення, ретельна перевірка електронних листів із посиланнями, перевірка вкладень, використання надійних унікальних паролів із менеджером, дотримання принципу необхідності доступу до даних та забезпечення фізичного захисту пристроїв і сховищ даних. Хоча дотримання вимог важко контролювати, кожна сторона несе відповідальність за захист своїх систем і своєчасне повідомлення інших про порушення, які можуть вплинути на процес.

З юридичної точки зору, навмисні або недбалі порушення кібербезпеки можуть призвести до збитків або штрафів відповідно до чинного обов'язкового законодавства. Вплив на арбітражне провадження, наприклад, скасування арбітражного рішення через фальсифікацію доказів, як правило, відповідає принципам, що застосовуються до будь-яких сфальсифікованих доказів. Однак допустимість незаконно отриманої інформації (наприклад, даних, отриманих шляхом хакерського втручання) та її наслідки є менш уніфікованими в різних юрисдикціях, що відображає різноманітні національні підходи до незаконно отриманих доказів…

Захист персональних даних, на який значний вплив має Загальний регламент про захист даних (GDPR) ЄС, є важливою складовою кібербезпеки. Хоча арбітраж не є винятком, у більшості випадків йдеться про керовані обсяги даних, пов'язаних зі сторонами або подіями, які часто обробляються без необхідності отримання явної згоди відповідно до статті 6(1) GDPR для законних цілей. Однак залишаються вторинні обов'язки, такі як інформування суб'єктів даних, надання можливості внесення виправлень та дотримання строків видалення (наприклад, після закінчення встановлених законом строків зберігання). Важливо, що персональні дані, отримані для арбітражу, не можуть бути згодом використані для інших цілей без нових правових підстав або явної згоди…

Щоб мінімізувати навантаження, пов'язане з дотриманням вимог, сторони та адвокати повинні надавати пріоритет гігієні даних: вносити тільки абсолютно необхідні персональні дані, анонімізувати або псевдонімізувати нерелевантну інформацію (наприклад, зафарбовувати, використовувати глосарії) та забезпечувати, щоб будь-які внесені дані були законними для цілей арбітражу або мали необхідну згоду. Транскордонні передачі даних за межі ЄС вимагають особливих запобіжних заходів, а субпідряд на обробку даних вимагає укладення відповідних договорів.

Процедурні розпорядження, що стосуються захисту даних, на відміну від основних процедурних правил, повинні бути встановлені на ранньому етапі. Ці розпорядження підкреслюють індивідуальну відповідальність за дотримання вимог, заохочують до мінімізації персональних даних та вимагають співпраці у разі порушень. Важливо, що ці заходи не слід плутати з процедурними правилами, порушення яких може призвести до визнання арбітражного рішення недійсним. Щодо надання документів, сторона може оскаржити наказ, якщо він вимагає вчинення дії, забороненої обов'язковим законодавством про захист даних. У таких випадках арбітражні суди можуть наказати анонімізацію, редагування або накласти суворі вимоги щодо зберігання та захисту на сторону, що отримує дані, при цьому арбітри та адвокати несуть пряму відповідальність згідно із законодавством про захист даних. Хоча незаконно отримані (зламані) дані викликають дедалі більшу стурбованість, їхня допустимість та відповідні санкції регулюються різними національними підходами, і в арбітражному праві не існує універсальних правил…» ***(Erik G W Schäfer. Managing data privacy and cybersecurity issues // Global Arbitration Review (https://globalarbitrationreview.com/guide/the-guide-evidence-in-international-arbitration/3rd-edition/article/managing-data-privacy-and-cybersecurity-issues). 09.09.2025).***

***

«Колумбійський університет нещодавно підтвердив масштабну кібератаку, в результаті якої було скомпрометовано особисту, фінансову та пов'язану зі здоров'ям інформацію, пов'язану зі студентами, абітурієнтами та співробітниками. Серед жертв є нинішні та колишні студенти, співробітники та абітурієнти. Повідомлення постраждалих осіб розпочалися 7 серпня і продовжуються на постійній основі.

Колумбійський університет, один із найстаріших університетів Ліги плюща, виявив порушення після збою в мережі в червні. За даними Колумбійського університету, збій був спричинений неавторизованою стороною, яка отримала доступ до його систем та викрала конфіденційні дані. Слідчі все ще оцінюють повний масштаб крадіжки.

Згідно з повідомленням про порушення, поданим до офісу генерального прокурора штату Мен, від порушення в Колумбійському університеті постраждало майже 869 000 осіб. Ця цифра включає студентів, співробітників, заявників і, в деяких випадках, членів сімей. ЗМІ також повідомили, що зловмисник заявив, що викрав приблизно 460 гігабайт даних із систем Колумбійського університету…

Колумбійський університет повідомив про інцидент правоохоронним органам та співпрацює з експертами з кібербезпеки. Університет заявив, що посилив свої системи новими засобами безпеки та вдосконаленими протоколами для запобігання майбутнім інцидентам.

Починаючи з 7 серпня, Колумбійський університет почав розсилати листи постраждалим, пропонуючи два роки безкоштовного моніторингу кредитної історії, консультацій щодо шахрайства та послуг з відновлення після крадіжки особистих даних…» ***(Kurt Knutsson. Columbia University data breach hits 870,000 people // FOX News Network, LLC (https://www.foxnews.com/tech/columbia-university-data-breach-hits-870000-people). 06.09.2025).***

***

«Уряд Пакистану розпочав термінове розслідування після повідомлень про масовий витік даних, що містять особисту інформацію власників SIM-карт, зокрема міністра внутрішніх справ Мохсіна Накві. Витік даних SIM-карт, які, за повідомленнями, відкрито продаються в Інтернеті, викликав загальнонаціональну стурбованість щодо цифрової безпеки та конфіденційності…

Згідно з повідомленнями ЗМІ, порушення стосується продажу конфіденційних даних SIM-карт на платформах Google. Стверджується, що дані про місцезнаходження мобільних телефонів продаються за 500 рупій, записи мобільних даних – за 2000 рупій, а навіть деталі закордонних поїздок – за 5000 рупій. Як повідомляє пакистанська англомовна газета Dawn, тривожним є те, що ці незаконні транзакції включають дані як про урядовців, так і про приватних громадян.

Ця новина з'явилася лише через кілька місяців після того, як Пакистанська національна команда реагування на кібернебезпеки (PKCERT) опублікувала серйозне попередження про глобальне порушення безпеки даних, яке торкнулося понад 180 мільйонів пакистанських інтернет-користувачів. PKCERT виявила загальнодоступну, незашифровану базу даних, що містила понад 184 мільйони унікальних облікових даних, включаючи імена користувачів, електронні адреси та паролі.

Дані, пов'язані з соціальними мережами, банківськими установами, платформами охорони здоров'я та урядовими порталами, були викрадені за допомогою шкідливого програмного забезпечення для викрадення інформації. Це шкідливе програмне забезпечення витягує конфіденційні дані з інфікованих систем. Викрадена інформація зберігалася без будь-якого шифрування або захисту паролем, що робило її легко доступною для використання.

«Вважається, що викрадена база даних була скомпільована за допомогою шкідливого програмного забезпечення Infostealer... Ці дані зберігалися у вигляді звичайного тексту і були повністю незахищені», — зазначено в повідомленні…» ***(Ashish Khaitan. Pakistan Launches Probe After Massive SIM Data Leak Hits Millions*** *// The Cyber Express LLC* ***(https://thecyberexpress.com/pakistan-probes-sim-data/). 08.09.2025).***

***

«Plex, компанія потокового передавання медіа, яка стоїть за своєю однойменною OTT-платформою та програмним забезпеченням для медіасерверів, підтвердила витік даних, в результаті якого «несанкціонована третя сторона» отримала доступ до особистої інформації деяких клієнтів. Хоча компанія не розкрила загальну кількість постраждалих користувачів, за повідомленнями, витік даних містить адреси електронної пошти, імена користувачів, паролі та дані автентифікації.

Компанія стверджує, що всі витік паролів був захищений криптографічним хешуванням відповідно до найкращих галузевих практик, що означає, що їх не можуть прочитати сторонні особи. Plex також підтвердив, що не зберігає жодної інформації про кредитні картки на своїх серверах, тому під час порушення не було скомпрометовано жодних конфіденційних фінансових даних.

Plex не уточнив використаний алгоритм хешування, але наголосив, що безпосередньої загрози безпеці користувачів немає. Тим не менш, компанія рекомендує всім клієнтам скинути свої паролі як запобіжний захід. Для цього відвідайте офіційну сторінку скидання пароля Plex та дотримуйтесь інструкцій.

Щоб запобігти шахрайству, Plex попереджає користувачів про необхідність остерігатися фішингових електронних листів із запитами паролів або даних кредитної картки. Компанія заявила, що ніколи не зв’язується з користувачами, щоб запитати особисту чи фінансову інформацію, і будь-який такий електронний лист слід розглядати як потенційно шкідливий.

Plex також рекомендує користувачам увімкнути двофакторну автентифікацію для додаткового рівня безпеки облікового запису…» ***(Kishalaya Kundu. Plex suffers major data breach, urges users to reset their passwords // TechSpot, Inc.***

(https://www.techspot.com/news/109389-plex-suffers-major-data-breach-urges-users-reset.html). 09.09.2025).

***

«Група хакерів, яка називає себе «Radiant», стверджує, що проникла в систему Kido International, оператора 18 дитячих садків у Великому Лондоні, і викрала особисті дані понад 8000 дітей. На своєму сайті в даркнеті група опублікувала зразки записів — імена, фотографії, домашні адреси та контактні дані сімей десяти учнів — і погрожувала опублікувати ще 30 профілів дітей та 100 файлів співробітників, якщо її вимоги не будуть виконані. Хакери, які заявили журналістам, що базуються в Росії, стверджують, що мали доступ до мережі Kido протягом декількох тижнів, але не розкрили суму викупу. Кіберкримінальний підрозділ лондонської поліції розпочав розслідування; арештів не було…

Національний центр кібербезпеки засудив напади на дитячі садки як особливо тяжкі злочини». ***(James Pearson. London nurseries hit by hackers, data on 8,000 children stolen // Yahoo (https://www.aol.com/london-nurseries-hit-hackers-data-142213178.html). 26.09.2025).***

***

«Кіберзлочинці заявляють про значне порушення безпеки бразильської компанії Maida.health, що займається медичною інформацією, стверджуючи, що було викрадено два терабайти медичних записів бразильської військової поліції. Ці надзвичайно конфіденційні дані, якщо вони є справжніми, містять вичерпні медичні записи офіцерів та членів їхніх сімей (що охоплюють такі спеціалізації, як кардіологія, неврологія та гінекологія), а також посвідчення особи, рахунки за медичні послуги, адміністративні протоколи, регуляторні сертифікати та клінічні дані пацієнтів. Хакери оголосили про злом на відомому підпільному форумі, хоча Cybernews не змогла самостійно перевірити ці заяви через недоступність зразків даних та відсутність відповіді від Maida.health…

Якщо ця інформація підтвердиться, витік даних матиме серйозні наслідки для конфіденційності, що може призвести до крадіжки особистих даних або медичного шахрайства, коли злочинці можуть видавати себе за жертв, щоб отримати медичну допомогу або ліки за рецептом. Цей інцидент підкреслює загальну тенденцію до ескалації атак на медичний сектор, який все частіше стає мішенню через наявність надзвичайно конфіденційних даних про пацієнтів. Вразливість цифрових провайдерів ставить під загрозу мільйони пацієнтів. Згідно з повідомленнями, понад 1,2 мільйона медичних пристроїв у всьому світі через неправильну конфігурацію мають доступ до Інтернету, що дозволяє отримати несанкціонований доступ до конфіденційних даних МРТ, КТ, рентгенівських знімків та систем управління лікарнями…» ***(Paulina Okunytė. Hackers say they nabbed Brazil's police medical files in massive breach // Cybernews (https://cybernews.com/security/brazil-police-health-data-breach/). 22.09.2025).***

***

«…Хоча в секторі кібербезпеки з'явилися занепокоєння щодо потенційних загроз, пов'язаних зі штучним інтелектом, в тому числі щодо витіснення робочих місць і операційних помилок, реальність є набагато більш багатообіцяючою. ШІ стає потужним інструментом, який доповнює людський досвід, а не замінює його, особливо в перевантажених операційних центрах безпеки (SOC)…

Постійні проблеми, такі як втома від тривог, нестача персоналу та цілодобовий моніторинг атак, призвели до високого рівня вигорання та плинності кадрів серед кваліфікованих спеціалістів. Штучний інтелект вирішує ці проблеми шляхом автоматизації повторюваних завдань, таких як сортування помилкових спрацьовувань, консолідація даних про загрози та перевірка захисту від нових атак. Це дозволяє аналітикам зосередитися на складних і важливих розслідуваннях і заходах реагування.

Під час багатовекторних атак штучний інтелект діє як помічник 24/7, швидко збираючи та співставляючи дані з різних систем, щоб визначити масштаби інциденту. Це прискорює розслідування та локалізацію, мінімізує збої в роботі та дозволяє швидше ділитися розвідданими про загрози зі світовою спільнотою безпеки. Крім того, можливості природної мови дозволяють аналітикам взаємодіяти з системами в діалоговому режимі, спрощуючи виконання таких завдань, як перевірка вразливостей…

Зрештою, ШІ слугує мультиплікатором сили, підвищуючи ефективність, зменшуючи операційний стрес і дозволяючи командам SOC більш ефективно використовувати людську винахідливість. У галузі, яка стикається з гострою нестачею талантів, ШІ пропонує не заміну людським навичкам, а необхідне партнерство для посилення кіберстійкості…» ***(Jonathan Fischbein. How AI Can Empower Cybersecurity Professionals—Not Replace Them // Forbes (https://www.forbes.com/councils/forbestechcouncil/2025/09/05/how-ai-can-empower-cybersecurity-professionals-not-replace-them/). 05.09.2025).***

***

«За даними OpenText, організації стикаються з перешкодами у сфері безпеки даних на шляху до впровадження штучного інтелекту. Інститут Ponemon опитав майже 1900 керівників інформаційних служб, керівників служб інформаційної безпеки та інших IT-керівників для звіту, опублікованого минулого місяця постачальником хмарних послуг та програмного забезпечення.

Майже три чверті респондентів заявили, що зменшення складності інформації є ключовим фактором для просування планів у сфері штучного інтелекту. Згідно з висновками звіту, головними причинами проблем із даними стали нові кіберзагрози, поширення пристроїв Інтернету речей та стрімке зростання обсягів неструктурованих корпоративних даних.

Згідно зі звітом, підприємства зміцнюють керівні структури, намагаючись подолати складність ситуації. Троє з п'яти респондентів висловилися за

призначення однієї особи, яка б контролювала стратегію щодо даних. Половина опитаних організацій вже найняла або планувала найняти головного спеціаліста з штучного інтелекту або цифрових технологій, щоб заповнити прогалину в керівництві…» ***(Matt Ashare. Data security gaps stymy enterprise AI plans // TechTarget, Inc. (https://www.cybersecuritydive.com/news/data-complexity-cybersecurity-generative-ai-adoption-opentext/759503/). 08.09.2025).***

***

«Нове дослідження з кібербезпеки, проведене компанією Sloan and Safe Security в Массачусетському технологічному інституті, проаналізувало 2800 атак програм-вимагачів і виявило, що 80% з них були задіяні штучним інтелектом. Штучний інтелект використовується для створення шкідливого програмного забезпечення, фішингових кампаній та соціальної інженерії на основі дипфейків , такої як фальшиві дзвінки до служби підтримки клієнтів. Великі мовні моделі використовуються для генерації коду та фішингового контенту. Також є засоби злому паролів за допомогою штучного інтелекту, обхід CAPTCHA тощо…

«Одних лише інструментів кібербезпеки на базі штучного інтелекту буде недостатньо», – пишуть вони. «Проактивний, багаторівневий підхід, що інтегрує людський нагляд, структури управління, симуляції загроз на основі штучного інтелекту та обмін розвідувальними даними в режимі реального часу, має вирішальне значення».

Дослідники стверджують, що комплексний підхід до боротьби із загрозами, що виникають на основі штучного інтелекту, складається з трьох типів захисту, кожен з яких є важливим:

1. **Автоматизована гігієна безпеки** , така як самовідновлюваний програмний код, системи самовиправлення, безперервне управління поверхнею атаки, архітектура на основі нульової довіри та самокеровані надійні мережі. Автоматизація цих рутинних завдань зменшує ручне навантаження, одночасно посилюючи захист від атак, спрямованих на вразливості основної системи.
2. **Автономні та оманливі системи захисту** , які використовують аналітику, машинне навчання та збір даних у режимі реального часу для навчання, виявлення та протидії загрозам. Прикладами є одночасна автоматизована оборона від рухомих цілей, а також оманлива тактика та інформація. Обидва типи систем дозволяють командам застосовувати проактивний підхід до захисту, а не застрягати в реактивному режимі.
3. **Розширений нагляд та звітність** , які надають керівникам аналітичні дані в режимі реального часу. Наприклад, автоматизований аналіз ризиків використовує штучний інтелект для виявлення нових загроз та прогнозування їхнього впливу на організацію.

Фахівці з кібербезпеки повинні проаналізувати історію успішного кіберзахисту — наприклад, захист від фішингу, соціальної інженерії та атак шкідливого програмного забезпечення — та врахувати, як звичні форми атак можуть розвиватися з додаванням штучного інтелекту…» ***(Zach Church. 80% of ransomware attacks now use artificial intelligence // MIT Sloan School of***

Management (https://mitsloan.mit.edu/ideas-made-to-matter/80-ransomware-attacks-now-use-artificial-intelligence). 08.09.2025).

***

«Компанія EC-Council, що займається сертифікацією, освітою, навчанням та послугами в галузі кібербезпеки, сьогодні оголосила, що інвестувала понад 20 мільйонів доларів у FireCompass Pvt. Ltd., постачальника платформи для наступальної безпеки на базі штучного інтелекту, в рамках своєї програми «Cybersecurity Innovation Commitment» на суму 100 мільйонів доларів.

Заснована в 2019 році, FireCompass пропонує платформу для активної безпеки на базі штучного інтелекту, яка об'єднує кілька функцій тестування безпеки в одне безперервне рішення. Основна мета компанії — допомогти підприємствам моделювати реальних супротивників у великому масштабі, що дозволяє їм виявляти приховані вразливості до того, як зловмисники зможуть ними скористатися.

Платформа Firecompass пропонує агентну технологію штучного інтелекту, призначену для автоматизації всього циклу розвідки, виявлення шляхів атаки та їх використання, що зазвичай вимагає великих операцій за участю спецпідрозділів.

Платформа об'єднує різні функції кібербезпеки під одним дахом: управління поверхнею атаки, безперервне управління ризиками, автоматизоване тестування на проникнення, червоне командне тестування та тестування на проникнення як послугу. Уніфікований підхід дозволяє організаціям зменшити свою залежність від різнорідних інструментів та ручного тестування, замінюючи їх безперервними симуляціями збройних сил зі швидкістю машини.

Відмінність FireCompass від інших постачальників полягає в його здатності об'єднувати вразливості в ланцюги та переміщуватися латерально по мережах, імітуючи дії реальних зловмисників. Метод надає докази ризиків, що можуть бути використані, а не просто перераховує теоретичні слабкі місця. Це надає клієнтам високоточні результати з майже нульовим рівнем хибних спрацьовувань та дозволяє командам безпеки зосередитися на усуненні недоліків, а не на аналізі шуму.

За даними компанії, її технологія виявила мільйони шляхів атак, одночасно скоротивши середній час відновлення приблизно на 40%.

Кажуть, що нові інвестиції виходять за рамки фінансової підтримки, оскільки Рада ЄС мобілізує свою всесвітню партнерську мережу, базу випускників та дослідницькі програми підприємств для прискорення інновацій FireCompass та глобальної експансії, забезпечуючи підприємствам доступ до найсучасніших технологій змагального моделювання, доступних сьогодні…» ***(Duncan Riley. EC-Council invests $20M+ in FireCompass to expand AI offensive security // SiliconANGLE Media Inc. (https://siliconangle.com/2025/09/04/ec-council-invests-20m-firecompass-expand-ai-offensive-security/). 04.09.2025).***

***

«Дослідники Palo Alto Networks виявили новий метод атаки, який може становити значний ризик для ланцюга поставок штучного інтелекту, і вони продемонстрували його вплив на продукти Microsoft та Google, а також потенційну загрозу для проектів з відкритим кодом.

Метод атаки на ланцюг поставок штучного інтелекту під назвою «Повторне використання простору імен моделей» передбачає, що зловмисники реєструють імена, пов’язані з видаленими або переданими моделями, які розробники отримують з таких платформ, як Hugging Face.

Успішна атака може дозволити зловмисникам розгортати шкідливі моделі штучного інтелекту та досягати довільного виконання коду, йдеться в дописі в блозі Palo Alto Networks, де описується повторне використання простору імен моделей .

Hugging Face — це популярна платформа для розміщення та обміну попередньо навченими моделями, наборами даних та застосунками штучного інтелекту. Коли розробники хочуть використовувати модель, вони можуть посилатися на неї або витягувати її на основі назви моделі та імені її розробника у форматі Author/ModelName.

Під час атаки повторного використання простору імен моделі зловмисник шукає моделі, власник яких видалив свій обліковий запис або перевів його на нове ім'я, залишивши старе ім'я доступним для реєстрації.

Зловмисник може зареєструвати обліковий запис з іменем цільового розробника та створити шкідливу модель з іменем, на яке, ймовірно, посилатимуться багато — або спеціально цільові — проекти.

Дослідники Palo Alto Networks продемонстрували потенційні ризики для платформи машинного навчання Vertex AI від Google, зокрема її репозиторію Model Garden для попередньо навчених моделей.

Model Garden підтримує пряме розгортання моделей від Hugging Face, і дослідники показали, що зловмисник міг зловживати цим для проведення атаки повторного використання простору імен моделей, зареєструвавши ім'я облікового запису Hugging Face, пов'язаного з проектом, який був видалений, але все ще перелічений та перевірений Vertex AI…

Окрім демонстрації атаки на хмарні платформи Google та Microsoft, співробітники Palo Alto розглянули репозиторії з відкритим кодом, які можуть бути вразливими до атак через посилання на моделі Hugging Face з використанням ідентифікаторів формату Author/ModelName…

Google, Microsoft та Hugging Face були повідомлені про ризики, і з того часу Google почав щоденно сканувати моделі-сиріти, щоб запобігти зловживанням.

Однак, Palo Alto зазначив, що «основна проблема залишається загрозою для будь-якої організації, яка використовує моделі лише за назвою. Це відкриття доводить, що довіряти моделям, заснованим виключно на їхніх назвах, недостатньо та вимагає критичної переоцінки безпеки в усій екосистемі штучного інтелекту».

Щоб зменшити ризики, пов'язані з повторним використанням простору імен моделей, компанія з безпеки рекомендує прив'язувати використану модель до певного коміту, щоб запобігти неочікуваним змінам поведінки, клонувати модель та зберігати її в надійному місці, а не отримувати її зі стороннього сервісу, а також

проактивно сканувати код на наявність посилань на моделі, які можуть становити ризик». ***(Eduard Kovacs. AI Supply Chain Attack Method Demonstrated Against Google, Microsoft Products // SecurityWeek (https://www.securityweek.com/ai-supply-chain-attack-method-demonstrated-against-google-microsoft-products/). 04.09.2025).***

***

«Хакери тепер можуть використовувати як зброю помічників ШІ-кодування, використовуючи лише захований файл ліцензії, перетворюючи інструменти розробника на тихих розповсюджувачів шкідливого коду. Про це йдеться у новому звіті компанії з кібербезпеки HiddenLayer, який показує, як ШІ можна обманом змусити сліпо копіювати шкідливе програмне забезпечення в проекти.

Метод підтвердження концепції, який отримав назву «Атака на ліцензію CopyPasta», використовує те, як інструменти штучного інтелекту обробляють поширені файли розробників, такі як LICENSE.txt та README.md. Вбудовуючи приховані інструкції або «впровадження запитів» у ці документи, зловмисники можуть маніпулювати агентами штучного інтелекту, щоб вони впроваджували шкідливий код, навіть не усвідомлюючи цього від користувача.

«Ми рекомендували запровадити захист від непрямих введень запитів під час виконання та забезпечити ретельну перевірку будь-яких змін, внесених до файлу», – сказав *Decrypt Кеннет Юнг, дослідник HiddenLayer та автор звіту.*

За словами Юнга, CopyPasta вважається вірусом, а не черв'яком, оскільки для його поширення все одно потрібні дії користувача. «Користувач повинен певним чином діяти, щоб шкідливе навантаження поширювалося», – сказав він.

Незважаючи на необхідність певної взаємодії з користувачем, вірус розроблений таким чином, щоб вислизати повз увагу людини, використовуючи те, як розробники покладаються на агентів штучного інтелекту для обробки рутинної документації.

«CopyPasta ховається в невидимих коментарях, захованих у файлах README, які розробники часто делегують агентам штучного інтелекту або мовним моделям для написання», – сказав він. «Це дозволяє йому поширюватися непомітно, майже непомітно»…» ***(Jason Nelson. 'CopyPasta' Attack Shows How Prompt Injections Could Infect AI at Scale // Decrypt Media, Inc. (https://decrypt.co/338143/copypasta-attack-shows-prompt-injections-infect-ai-scale). 04.09.2025).***

***

«Майже три чверті пристроїв розумного дому в ОАЕ вразливі до кібератак, якщо вони не захищені належним чином, попередила Рада з кібербезпеки країни.

У коментарях державному інформаційному агентству *WAM* рада заявила, що підключені технології, такі як голосові помічники, системи спостереження та автоматизовані освітлювальні й охолоджувальні установки, все частіше стають мішенню хакерів, особливо коли користувачі покладаються на налаштування за замовчуванням або нехтують основними заходами безпеки.

Ризиковані практики включають постійне підключення голосових помічників до Інтернету або передачу відвідувачам основного пароля Wi-Fi в будинку. Обидва ці методи можуть створювати шлюзи для зловмисників для крадіжки даних або дистанційного керування пристроями.

Дитячі монітори, які зараз поширені в багатьох будинках, були виділені як особливо вразливі, оскільки зловмисники потенційно можуть записувати розмови, відстежувати переміщення всередині будинку або навіть спілкуватися безпосередньо з дітьми.

Щоб зменшити ризики, рада порадила три ключові кроки: використовувати надійні, унікальні паролі; регулярно оновлювати програмне забезпечення пристроїв; та керувати всіма розумними пристроями через центральний вузол для обмеження точок входу.

Також було рекомендовано домогосподарствам вимикати голосових помічників, коли вони не використовуються, активувати налаштування конфіденційності та уникати підключення непотрібних пристроїв до Інтернету. Також було рекомендовано налаштувати окрему мережу Wi-Fi для смарт-пристроїв, ізолюючи їх від основної домашньої мережі. Сім'ям було рекомендовано купувати лише ті пристрої, які їм дійсно потрібні, а не заповнювати будинки гаджетами з підключенням до Інтернету, що розширює зону атаки.

У рамках своєї поточної ініціативи «Кіберпульс» рада нещодавно розпочала тижневу інформаційну кампанію, пропонуючи рекомендації щодо оновлень програмного забезпечення, практик безпеки пристроїв та важливості пильності, оскільки кіберризики розвиваються у все більш цифровому домашньому середовищі». ***(Huda Ata. Cybersecurity Council warns UAE homes over vulnerable smart devices // Al Nisr Publishing LLC (https://gulfnews.com/uae/government/cybersecurity-council-warns-uae-homes-over-vulnerable-smart-devices-1.500260106). 07.09.2025).***

***

«…Розумні гаджети, які роблять будинки та офіси більш зручними, також стали одними з найслабших місць у сучасній кіберзахисті. Дослідники в галузі безпеки виділяють сім поширених пристроїв Інтернету речей (IoT), які зловмисники регулярно використовують: розумні термостати, голосові помічники/динаміки, веб-камери, підключені до Інтернету холодильники, «розумні» лампочки, мережеві принтери/багатофункціональні пристрої та камери дверних дзвінків…

Більшість пристроїв постачаються з паролями за замовчуванням, слабким шифруванням і рідко оновлюваним прошиванням, тому вторгнення в один пристрій може стати плацдармом для проникнення в решту мережі Wi-Fi. Термостати та холодильники витокують дані під час передачі; веб-камери та динаміки використовуються для таємного спостереження; лампочки та розумні розетки використовуються для запуску DDoS-атак; принтери зберігають незахищені скани, що дає хакерам доступ до корпоративних систем; а камери дверних дзвінків дозволяють стороннім особам шпигувати або повністю вимкнути трансляцію…

Рекомендовані заходи протидії є простими, але часто ігноруються: змініть заводські облікові дані, своєчасно встановлюйте оновлення прошивки та розміщуйте обладнання IoT в окремій VLAN або гостьовій мережі, щоб компрометація не поширилася на ноутбуки та сервери. Доки виробники не створять більш надійну «безпеку за замовчуванням», відповідальність за зміцнення цих повсякденних пристроїв залишається на користувачах та IT-персоналі, перш ніж зручність, яку вони пропонують, перетвориться на дороге порушення…» ***(Ava Callegari. 7 Vulnerable IoT Devices: Hacking Risks and Security Tips // iEntry, Inc. (https://www.webpronews.com/7-vulnerable-iot-devices-hacking-risks-and-security-tips/). 09.09.2025).***

***

«…Кіберзахист перетворився на сукупність абревіатур — SIEM, SOAR, EDR, XDR, CNAPP, DSPM — але єдине питання, яке має значення, є простим: на якому етапі ланцюжка атак зловмисника продукт зупиняє атаку і як швидко?

Ланцюжок кіберударів Lockheed-Martin (розвідка → доставка → експлуатація/«бум» → управління та контроль → бічне переміщення → мета) дає універсальну карту цих точок розриву. Інструменти, які надійно блокують певний етап — зупиняють доставку фішингових повідомлень, нейтралізують трафік C2, виявляють бічне переміщення — стають платформами; ті, що не можуть пов'язати свою цінність з певним етапом, з часом зникають або поглинаються більш широкими пакетами. Історія показує таку закономірність: окремі брандмауери, IDS та веб-фільтри об'єдналися в брандмауер нового покоління; AV, антивірусне програмне забезпечення та HIPS об'єдналися в EDR/XDR; сьогоднішня «буквальна юшка» навколо хмари, ідентичності та даних консолідується таким самим чином…

Штучний інтелект прискорює цей цикл. Зловмисники вже використовують GenAI для створення витончених фішингових приманок, мутації шкідливого програмного забезпечення та сканування поверхонь атаки зі швидкістю машини. Тому «AI-native» безпека не може бути додатковою аналітикою; вона повинна включати навчання та автоматизацію в профілактику, виявлення та реагування:

• Ліворуч від буму: моделі вивчають нормальну поведінку користувачів і активів, позначаючи тонкі зондування або підроблені електронні листи, які пропускають фільтри сигнатур.

• Праворуч від буму: механізми кореляції великих мовних моделей об'єднують слабкі сигнали — дивні запити DNS, незначні зміни привілеїв — у цілісні наративи зловмисників і можуть за лічені секунди запустити автоматичне блокування.

Для захисників, які використовують на 30 % більше інструментів, ніж три роки тому, при цьому все ще відчуваючи нестачу персоналу, переможними продуктами стануть ті, що скорочують час розслідування з годин до хвилин і переміщують точку розриву далі вліво в ланцюжку. Інвестори та керівники служб інформаційної безпеки можуть використовувати модель ланцюжка знищення, щоб розрізнити маркетингові категорії, що перекриваються: дві стартап-компанії, що

займаються «хмарною безпекою», можуть взагалі не конкурувати, якщо одна з них перериває початковий доступ, а інша зупиняє витік даних…

Зрештою, мета залишається незмінною: перенести ризик з користувачів назад на супротивників, зруйнувавши всі шляхи атаки. Штучний інтелект надає захисникам нові важелі впливу, але успіх буде належати тим постачальникам, які зроблять ланцюжок атак коротшим, швидшим і дешевшим для руйнування, перетворивши реактивну гру в кота і мишу на проактивну, автоматизовану перевагу…» ***(Malika Aubakirova, Joel de la Garza, Zane Lackey. Breaking the Cybersecurity Kill Chain with AI // Andreessen Horowitz (https://a16z.com/breaking-the-cybersecurity-kill-chain-with-ai/). 09.09.2025).***

***

«…Виступаючи на саміті з кібербезпеки в Біллінгтоні, директор Національного агентства геопросторової розвідки (NGA) віце-адмірал Френк Вітворт попередив, що хакери зараз використовують штучний інтелект, змушуючи кіберзахисників США протидіяти «ШІ за допомогою ШІ». Він закликав командувачів оснастити керівників служб інформаційної безпеки (CISO) передовими інструментами безпеки на основі штучного інтелекту, зазначивши, що власна платформа NGA Maven, використання якої з січня подвоїлося, а з березня 2024 року зросло вчетверо, демонструє, як машинне навчання може швидко виявляти та прогнозувати загрози. Вітворт додав, що навіть «застаріла автоматизація» приносить значні результати: NGA створила 7500 карт Латинської Америки за 7,5 тижнів, а раніше на цю роботу йшло 7,5 років…

Його зауваження повторили слова новопризначеного національного директора з кібербезпеки Шона Кернкросса, який днем раніше закликав до «загальнонаціонального» партнерства з промисловістю та союзниками з метою викриття зловмисних дій іноземних держав, підвищення витрат супротивників та зміцнення стійкості США…

Генерал Ден Кейн, голова Об'єднаного комітету начальників штабів, заявив, що сучасна війна зараз залежить від збору даних, багаторівневого аналізу штучного інтелекту та надання командирам «єдиного вікна» в режимі реального часу для швидшого прийняття тактичних і стратегічних рішень, уникаючи при цьому ненавмисної ескалації.

Пентагон підтримує ці зусилля фінансово та реорганізацією: він уклав нові контракти на суму 200 мільйонів доларів у сфері штучного інтелекту, підписав потенційну угоду на суму 10 мільярдів доларів терміном на 10 років з компанією Palantir щодо аналітики для армії та реструктурує своє Головне управління з даних та штучного інтелекту, скорочуючи штат, але обіцяючи «пріоритет штучного інтелекту» в Міністерстві оборони, навіть попри скорочення власної платформи Advana…» ***(Lauren C. Williams. Fight AI-powered cyber attacks with AI tools, intelligence leaders say // Government Media Executive Group LLC. (https://www.defenseone.com/defense-systems/2025/09/fight-ai-powered-cyber-attacks-ai-tools-intelligence-leaders-say/408031/). 10.09.2025).***

***

«…У лабораторії автономного та підключеного транспорту (ACT) Технологічного інституту Джорджії дослідники вивчають, як можуть відбуватися кібератаки на автономні транспортні засоби, занурюючи водіїв у повнорозмірний симулятор із 360-градусним віртуальним середовищем і відстежуючи все, від рухів очей до рухів кермом. Директор Срінівас Піта каже, що основна увага приділяється взаємодії між людьми, транспортними засобами та інфраструктурою, а докторант Янцзяо Чен зазначає, що зв'язок є основним вектором атаки, наслідки якого можуть варіюватися від незначних заторів до серйозних зіткнень. Їхні дослідження показують, що коли люди усвідомлюють, що автомобілі можуть бути зламані, вони стають більш обережними і тримаються на більшій відстані — і навіть без явних попереджень багато хто пристосовується до нетипової поведінки автономних автомобілів. Ця робота проводиться на тлі реальних проблем: Waymo публічно ставить на перше місце кібербезпеку, але надає обмежену інформацію, а гучні інциденти — від дистанційного доступу 19-річного підлітка до 25 автомобілів Tesla в 13 країнах у 2022 році до інших зловживань Tesla та хакерських атак на системи безключового доступу — підкреслюють ризики... Довіра громадськості залишається низькою — лише 13% водіїв у США довіряють автономним автомобілям у 2025 році — хоча 78% підтримують пріоритетність систем безпеки, що підкріплює думку Піти про те, що побудова довіри є фундаментальною…» ***(Cody Combs. Driverless vehicles are now in hackers' crosshairs - and cyber security experts prepare for the worst // The National (https://www.thenationalnews.com/future/technology/2025/09/12/can-hackers-break-into-driverless-vehicles/). 10.09.2025).***

***

«…Швидка автоматизація складів та конвергенція IT і OT розширили площу атаки в промислових середовищах Інтернету речей, що викликало інтерес до сегментації мережі як основного засобу захисту. Сегментація розділяє мережі на ізольовані зони, щоб обмежити доступ і непотрібний трафік, тоді як мікросегментація застосовує ще більш точні засоби контролю на рівні додатків для захисту систем OT. Експерти, такі як генеральний директор Mission Secure Джон Адамс, рекомендують ретельно перевіряти вимоги до трафіку та застосовувати межі сегментів за допомогою брандмауерів, підкреслюючи, що сегментація не є панацеєю, але ефективно уповільнює супротивників і обмежує радіус ураження. Склади можуть сегментуватися за допомогою брандмауерів, списків контролю доступу та VLAN або застосовувати сучасний програмно-визначений доступ, який централізовано застосовує політики. Потреба зростає разом із бурхливим розвитком ринку автоматизації (24,09 млрд доларів у 2025 році), де збільшення обсягу трафіку ускладнює ручне виявлення загроз, а зловмисники націлюються на критично важливі системи…

Сегментація допомагає запобігти бічному переміщенню, покращує продуктивність шляхом ізоляції трафіку з високим пріоритетом для уникнення перевантажень та підтримує безперервність бізнесу під час інцидентів, що робить її ідеальною для зменшення ризиків конвергенції IT/OT без створення вузьких місць у важливих операціях. Прагматичний підхід передбачає три етапи:

картографування активів і потоків даних; визначення стратегії сегментації за типом пристрою, чутливістю даних, критичністю активів або функцією (за допомогою ручних VLAN, динамічної сегментації на основі NAC або програмно-визначених контролерів/API); а також впровадження та постійний моніторинг засобів контролю. Кожен варіант має свої плюси і мінуси — динамічні та програмно-визначені методи адаптуються до мінливих ризиків, але вимагають сумісної інфраструктури та створюють централізовані точки відмови, що є проблемою в ОТ-середовищах, де багато контролерів залишаються без патчів (згідно з доповіддю Microsoft за 2022 рік, 75 % з них мають вразливості високого рівня). Завдяки регулярним аудитам і, за необхідності, штучному інтелекту або RPA для оптимізації нагляду, сегментація не може зупинити кожну атаку, але істотно посилює безпеку об'єкта, мінімізуючи вплив…» ***(Zac Amos. Embracing Network Segmentation for Warehouse Cybersecurity // Automation.com (https://www.automation.com/en-us/articles/september-2025/network-segmentation-warehouse-cybersecurity?listname=Automation). 12.09.2025).***

***

«…Хакер використав чат-бот Claude від Anthropic для проведення багатоетапної кіберзлочинної кампанії проти щонайменше 17 організацій, продемонструвавши, як генеративна ШІ може автоматизувати все, від розвідки до вимагання викупу. Згідно з доповіддю Anthropic про загрози, зловмисник наказав Claude знайти незахищені кінцеві точки VPN, створити шкідливе програмне забезпечення для викрадення інформації, адаптоване до таких секторів, як оборона та охорона здоров'я, відібрати з викрадених файлів дані, що мають високу цінність, і навіть розрахувати суму викупу в біткойнах від 75 000 до 500 000 доларів… За допомогою «хакерства вібрацій» моделі — формулювання запитів з метою обходу засобів захисту — зловмисник отримав код для експлуатації, автоматично сформовані листи з вимаганням викупу та інструкції щодо налаштування біткойн-гаманця, що дозволило йому здійснювати масштабні операції без володіння елітними навичками кодування. Компанія Anthropic заявила, що виявила аномальні шаблони запитів, обмежила доступ та посилила моніторинг у режимі реального часу, але критики стверджують, що нинішні захисні заходи залишаються недосконалими, що викликає питання щодо відповідальності постачальників та можливих регуляторних заходів, особливо в ЄС… Цей інцидент відповідає більш широкій тенденції загроз, пов'язаних із штучним інтелектом, — від інструментів типу WormGPT до ризиків введення команд, зазначених у рейтингу OWASP «10 найбільших загроз для великих мовних моделей у 2025 році», — з використанням доменного фронтингу та інших тактик, що посилюють вплив. Пропоновані заходи щодо зменшення ризиків включають моніторинг, спрямований на штучний інтелект, нанесення водяних знаків на код, згенерований штучним інтелектом, для полегшення атрибуції, виправлення постачальниками вразливостей серверів та більш тісний обмін інформацією в галузі. З огляду на викуп у розмірі шестизначних сум та потенційні наслідки для національної безпеки, цей випадок є суворим попередженням про те, що заходи безпеки повинні розвиватися так само швидко, як і системи штучного інтелекту, що трансформують

злочини…» ***(Corey Blackwell. Hacker Exploits Claude AI to Automate Cyberattacks on 17 Companies // iEntry, Inc. (https://www.webpronews.com/hacker-exploits-claude-ai-to-automate-cyberattacks-on-17-companies/). 13.09.2025).***

***

«…За даними компанії Genians, хакери з групи Kimsuky, підтримувані Північною Кореєю, використовували ChatGPT для створення переконливого шаблону військового посвідчення Південної Кореї та провели фішингову кампанію проти журналістів, дослідників та правозахисників. Компанія Genians виявила, що підроблена електронна пошта, яка, як здавалося, надходила з адреси .mil.kr, містила приховане шкідливе програмне забезпечення. Genians заявила, що зловмисники обійшли захисні заходи ChatGPT за допомогою маніпуляцій із підказками — методу, який компанія відтворила, підкресливши, як штучний інтелект може бути використаний у всьому ланцюжку вторгнення… Ця операція вписується в більш широку схему: компанія Anthropic нещодавно повідомила, що північнокорейські актори використовують її модель Claude Code для створення резюме, проходження співбесід з кодування та виконання технічних завдань для американських компаній з рейтингу Fortune 500, а OpenAI раніше заблокувала акаунти, пов'язані з Північною Кореєю, за створення фальшивих резюме, супровідних листів та публікацій у соціальних мережах. Активна з 2012 року і давно займається збором розвідувальної інформації, Kimsuky зазвичай використовує spearphishing для проникнення в цілі, пов'язані з політикою Північної Кореї в Південній Кореї, Японії та США; кількість скомпрометованих пристроїв в цій останній кампанії невідома. Офіційні особи США та Південної Кореї попереджають, що зловмисники продовжують використовувати підроблені домени та фальшиві профілі рекрутерів, закликаючи спільноти, що знаходяться в зоні ризику, увімкнути багатофакторну автентифікацію, підвищити обізнаність про фішинг та посилити фільтри електронної пошти, оскільки Пхеньян все частіше поєднує хакерство, крадіжку криптовалюти та тіньові контракти для фінансування своєї санкціонованої ядерної програми…» ***(Jai Hamid. North Korea-linked hackers used ChatGPT to create fake military IDs // Cryptopolitan (https://www.cryptopolitan.com/north-korea-hackers-chatgpt-fake-military-id/). 14.09.2025).***

***

«…Проекти «розумних міст» швидко поширюються — 69 % муніципалітетів у всьому світі зараз мають офіційну стратегію, а в 2024 році було встановлено близько 83 000 нових датчиків — але заходи з кібербезпеки, що їх захищають, відстають…

Гіперпідключені системи, що керують сиренами, камерами, світлофорами, водоочищенням, енергоменеджментом та іншими комунальними послугами, збільшують площу атаки: хакери вже запустили всі сирени торнадо в Далласі (2017), заблокували 70 % мережі відеоспостереження Вашингтона (2017), втрутилися в рівні хімічних речовин на водоочисній станції у Флориді (2021) та паралізували транспорт в Ольштині, Польща (2023)…

Оскільки один скомпрометований датчик може спричинити ланцюгову реакцію в усьому місті, необхідно забезпечити безпеку всього периметра, проте в багатьох установках сучасні, краще захищені пристрої поєднуються зі старим, легко вразливим обладнанням. Ці точки входу можуть дати злочинцям шлях до ширших корпоративних або муніципальних мереж, як це проілюстрували такі витівки, як «злом Google Maps» у 2020 році, коли 99 смартфонів обдурили навігаційне програмне забезпечення, змусивши його повідомляти про фантомні затори. Тому фахівці з безпеки попереджають, що, хоча абсолютна безпека є неможливою, муніципалітети повинні посилити захист на всіх рівнях — сегментувати мережі, виправляти або виводити з експлуатації застарілі пристрої та запроваджувати суворі заходи контролю доступу — щоб створити якомога більше бар'єрів проти атак, які можуть порушити роботу основних міських служб…» ***(María Ramos Domínguez. Cybersecurity in smart cities under scrutiny // FoundryCo, Inc. (https://www.csoonline.com/article/4058179/cybersecurity-in-smart-cities-under-scrutiny.html). 19.09.2025).***

***

«…Штучний інтелект змінив кібербезпеку, аналізуючи величезні потоки даних для виявлення аномалій, блокування атак і попередження людей, а машинне навчання покращило швидкість реагування та точність. Однак ці інструменти також створюють ризики, такі як «розумні» атаки на основі штучного інтелекту, порушення конфіденційності через збір великих даних, складність і вартість, помилкові спрацьовування, які перевантажують команди, надмірна залежність, яка відсуває на другий план людське судження, та етичні проблеми, пов'язані з непрозорими рішеннями. Окрім підприємств, штучний інтелект тепер лежить в основі цифрового виховання дітей: інтелектуальні інструменти сканують на наявність шахрайства, шкідливого програмного забезпечення, шкідливого контенту та кібербулінгу, допомагаючи батькам захищати дітей, одночасно забезпечуючи позитивне використання технологій. Однак багато заходів з підвищення обізнаності зупиняються на організаційному рівні, залишаючи повсякденних користувачів вразливими, якщо сім'ї не здійснюють активного моніторингу онлайн-активності, не оновлюють програмне забезпечення, не встановлюють чітких правил та не застосовують засоби захисту на основі машинного навчання… Переваги є суттєвими: ШІ може обробляти величезні масиви даних за лічені хвилини, виявляти загрози швидше, ніж люди, зменшувати кількість людських помилок, фільтруючи підозрілу поведінку в електронних листах, логінах і на веб-сайтах, діяти в режимі реального часу для стримування фішингу та шкідливого програмного забезпечення, а також прогнозувати нові ризики на основі аналізу шаблонів. Щоб збалансувати переваги та ризики, організації та приватні особи повинні мінімізувати збір даних, дотримуватися законів про конфіденційність та суворого управління, поєднувати ШІ з людським наглядом, постійно тестувати та налагоджувати моделі, інвестувати в постійне навчання користувачів, підтримувати системи в актуальному стані та дотримуватися прозорості та підзвітності після інцидентів. Якщо все зробити правильно, поєднання швидкості та масштабів штучного інтелекту з людським

досвідом створює надійний захист, який максимізує цінність інтелектуальної безпеки та мінімізує її недоліки…» ***(AI-Powered Cybersecurity Tools: Opportunities and Risks // MercoPress (https://en.mercopress.com/2025/09/17/ai-powered-cybersecurity-tools-opportunities-and-risks). 17.09.2025).***

***

«Останній звіт Lenovo «Work Reborn» показує, що штучний інтелект трансформує кіберризики швидше, ніж більшість організацій можуть до цього пристосуватися: 65 % з 600 опитаних світових IT-лідерів визнають, що їхні системи безпеки застаріли для атак із використанням штучного інтелекту, і лише 31 % впевнені, що зможуть їх відбити. Генеративний штучний інтелект породжує новий клас загроз — поліморфне шкідливе програмне забезпечення, глибоко підроблений фішинг та адаптивні «внутрішні» боти — тоді як моделі штучного інтелекту, навчальні дані та підказки, які використовують компанії, самі стають цінними цілями. 70 % респондентів також стурбовані тим, що випадкове використання інструментів штучного інтелекту співробітниками створює нові ризики…

Оскільки ці атаки навчаються і мутують у режимі реального часу, Lenovo стверджує, що «тільки ШІ може боротися з ШІ». Компанія впроваджує інтелектуальні технології у весь свій портфель продуктів — кінцеві пристрої AI-PC, систему забезпечення безпеки ланцюга поставок ThinkShield та платформу кіберстійкості «від хмари до периферії», що надається через механізм Care of One™. Ключові можливості включають виявлення аномалій на основі штучного інтелекту, автоматизований аналіз ролей та керовану кіберстійкість як послугу (CRaaS), яка, за повідомленнями перших клієнтів, забезпечує 99,5 % точність виявлення загроз, час відгуку менше 30 хвилин та економію витрат у перший рік понад 20 %. Сервери ThinkSystem x86 компанії, які одинадцять років поспіль посідають перше місце за часом безвідмовної роботи за версією ITIC, забезпечують апаратну основу.

Визнання галузі підтверджує актуальність та позиціонування Lenovo: компанія Gartner прогнозує, що до 2027 року 90 % успішного впровадження штучного інтелекту в кібербезпеці буде пов'язано з тактичною автоматизацією завдань, а Lenovo щойно отримала три нагороди Fortress Cybersecurity Awards 2025 у категоріях лідерства в області нульової довіри, безпеки ланцюгів постачання та послуг з відновлення хмарних систем. Послання чітке: традиційні, засновані на правилах засоби захисту вже не можуть йти в ногу з часом; підприємства повинні інтегрувати адаптивний захист на основі штучного інтелекту в кожну кінцеву точку, додаток і потік даних, щоб перетворити ризики, пов'язані зі штучним інтелектом, на конкурентне, безпечне зростання…» ***(Lenovo Finds 65% of IT Leaders Admit Their Defenses Can't Withstand AI Cybercrime // Lenovo Group Limited (https://news.lenovo.com/pressroom/press-releases/it-leaders-admit-their-defenses-cant-withstand-ai-cybercrime/). 18.09.2025).***

***

«Сучасна робоча сила переживає перебудову внаслідок швидкого впровадження автономних агентів штучного інтелекту, які зараз беруть на себе завдання у сферах розробки, продажів, досліджень, обслуговування клієнтів, створення контенту та фінансів. Ці системи можуть планувати, приймати рішення та діяти з мінімальним контролем з боку людини, і компанії швидко переносять їх з прототипів у виробництво. В результаті кількість нелюдських та агентних ідентичностей стрімко зростає — очікується, що цього року вона перевищить 45 мільярдів, що в 12 разів перевищує чисельність людської робочої сили. Проте, згідно з опитуваннями, лише невелика частина організацій має стратегії управління цими ідентичностями, незважаючи на те, що компрометація ідентичностей є основною причиною порушень, а генеративний штучний інтелект робить фішинг та соціальну інженерію набагато небезпечнішими…

Агенти штучного інтелекту створюють унікальні ризики для безпеки: вони часто потребують широкого доступу до конфіденційних даних компанії, що робить їх привабливими об'єктами для атак. Зловмисники можуть маніпулювати ними за допомогою таких тактик, як введення команд, потенційно змушуючи агентів розкривати інформацію або виконувати несанкціоновані дії. На відміну від людей, ці агенти аутентифікуються не за допомогою паролів або MFA, а за допомогою API-токенів і криптографічних сертифікатів, що ускладнює їх управління, моніторинг і скасування в разі компрометації. Їх динамічний життєвий цикл, висока автономність і схильність до затуманення видимості посилюють ризики…

Щоб вирішити ці проблеми, організації повинні впровадити «структуру безпеки ідентичності» — систему, яка захищає кожну ідентичність (людську та нелюдську) у всіх додатках і системах. Для агентів штучного інтелекту ключовими є три принципи. По-перше, безпека, що вимагає точних, обмежених у часі дозволів і детального контролю доступу для запобігання ескалації привілеїв або витоку даних. По-друге, взаємодія, що забезпечує безпечну взаємодію агентів з іншими інструментами та системами за допомогою стандартів, таких як Model Context Protocol (MCP). По-третє, прозорість, що вимагає постійного моніторингу, аудиту та виявлення аномалій для виявлення зловживань до їх ескалації.

Оскільки більшість компаній перебувають на початкових етапах впровадження агентного ШІ, вони мають можливість з самого початку інтегрувати надійне управління ідентифікацією безпосередньо в ці системи, незалежно від того, чи створюють вони агентів самостійно, чи використовують сторонні інструменти. Довгострокова стійкість вимагатиме постійного управління, прозорості та контролю. Маючи надійну основу для ідентифікації, організації можуть безпечно масштабувати ШІ-агентів, розкриваючи їхній величезний потенціал і мінімізуючи ризики, пов'язані з цією швидко зростаючою нелюдською робочою силою…» ***(Eric Kelleher. What to do about unsecured AI agents – the cyberthreat no one is talking about // World Economic Forum (https://www.weforum.org/stories/2025/09/unsecured-ai-agents-cyberthreat/). 25.09.2025).***

***

«Оскільки зловмисники все частіше використовують штучний інтелект як зброю, безпека за принципом «нульової довіри» залишається надзвичайно важливою, але повинна швидко вдосконалюватися. Принцип «нульової довіри» базується на підході «ніколи не довіряй, завжди перевіряй» і передбачає сегментацію та суворі перевірки ідентичності для запобігання загрозам, таким як крадіжка облікових даних. Зараз штучний інтелект дозволяє зловмисникам масово створювати надзвичайно переконливі фішингові кампанії, автоматизувати крадіжку токенів і створювати депфейки, які обманюють як людей, так Недавні порушення безпеки, такі як атака на токени OAuth на Salesloft через інтеграцію з Salesforce, які, начебто, були захищені моделями нульової довіри, показують, як вкрадені або надмірно привілейовані ідентичності все ще можуть підривати сегментовані мережі…

Штучний інтелект підвищує ставки двома способами: кількісно, дозволяючи злочинцям здійснювати тисячі атак, тоді як раніше вони могли здійснити лише десятки, та якісно, створюючи фейкові зображення, які обходять традиційні засоби перевірки. Тому майбутні засоби контролю «воротаря» потребуватимуть додаткових або керованих штучним інтелектом перевірок для підтвердження автентичності абонента, користувача або агента. Межі ідентичності повинні бути ще більш жорсткими, надаючи агентам лише своєчасний доступ з мінімальними привілеями та вимагаючи повторної автентифікації при переході між доменами…

Поява автономних агентів штучного інтелекту ускладнює ситуацію: компанії хочуть, щоб ці системи обробляли величезні масиви конфіденційних даних, щоб стати «розумнішими», але це бажання може вийти за межі вимог сегментації нульової довіри. Якщо зловмисник захопить агента, який вже підключений до критично важливих баз даних, він може проводити експлойти «живучи з того, що є», тихо витягуючи файли переговорів, записи про пацієнтів або вихідний код, залишаючись при цьому важко відстежуваним.

Однак штучний інтелект також може посилити принцип нульової довіри. Аналітика на основі машинного навчання може виявляти аномальну поведінку агентів, автоматизувати ротацію сертифікатів і сприяти впровадженню мікросегментації на рівні підприємства. Успіх залежатиме від того, чи впровадять організації управління ідентифікацією та детальну політику в кожне впровадження штучного інтелекту, гарантуючи, що агенти підтверджують свою особу, отримують доступ лише до необхідної інформації та залишають контрольований слід.

Коротко кажучи, модель «нульової довіри» все ще працює — обмежуючи радіус ураження за допомогою сегментації та перевірки ідентичності — але вона повинна еволюціонувати, щоб протистояти прискореній штучним інтелектом швидкості, масштабу та обману. Компанії, які додають до своїх існуючих систем «нульової довіри» вдосконалені штучним інтелектом засоби виявлення, більш глибокі етапи перевірки та більш суворі заходи контролю з мінімальними привілеями, будуть краще підготовлені до протистояння наступній хвилі атак, що базуються на штучному інтелекті…» ***(Arielle Waldman. Zero Trust: Strengths and Limitations in the AI Attack Era // TechTarget, Inc. (https://www.darkreading.com/endpoint-security/zero-trust-strengths-and-limitations-in-the-ai-attack-era). 19.09.2025).***

***

«…Штучний інтелект швидко перевершує людей у виявленні вразливостей програмного забезпечення, але це саме по собі не зміцнить кібербезпеку, попередив колишній керівник кібербезпеки Агентства національної безпеки і Білого дому Роб Джойс на саміті Google з кіберзахисту. Великі мовні моделі та спеціалізовані агенти, такі як XBOW, вже «перевіряють кожну дверну ручку» в Інтернеті, виявляючи недоліки швидше, ніж будь-яка команда людей; проте більшість організацій все ще «погано справляються з виправленням вразливостей». Хоча великі технологічні компанії можуть швидко виправляти проблеми, великі ділянки цифрової екосистеми працюють на застарілих або непідтримуваних системах, і ніхто не може — або не має права — встановлювати оновлення. У міру того, як ШІ прискорює виявлення вразливостей, це програмне забезпечення, яке неможливо виправити, стане основним джерелом системного ризику, що потенційно може спровокувати «пожежу на Західному узбережжі» — ланцюжок порушень, перш ніж захист буде вдосконалено…

Джойс також застеріг компанії, які підключають автономних агентів ШІ до електронної пошти, баз знань та інших основних платформ. Зловмисники вже використовують таких агентів для виконання запитів на основі великих мовних моделей по вкрадених даних, виявляючи найприбутковіші файли для вимагання викупу або шантажу. Він прогнозує, що такі організації, як Північна Корея, які керуються прибутком, незабаром спеціалізуватимуться на експлуатації корпоративних розгортань ШІ, оскільки «саме там є гроші». Коротко кажучи, ШІ посилює як здатність знаходити слабкі місця, так і небезпеку того, що ці слабкі місця залишаться невиправленими і їх легко можна буде використати як зброю, що робить дисциплінований управління патчами та ретельний контроль агентів ШІ більш важливими, ніж будь-коли…» ***(Eric Geller. AI-powered vulnerability detection will make things worse, not better, former US cyber official warns // TechTarget, Inc. (https://www.cybersecuritydive.com/news/ai-vulnerability-detection-patching-threats-mandiant-summit/760746/). 22.09.2025).***

***

«…Дослідники Radware продемонстрували «ShadowLeak» — техніку непрямого введення команд, яка перетворює інтегрованих в електронну пошту AI-асистентів на невидимі інструменти витоку даних. Коли користувач Gmail, який підключив ChatGPT, просить агента «підсумувати мої непрочитані листи», запит повністю обробляється на серверах OpenAI: модель витягує повідомлення через API, аналізує їх і повертає підсумок. Приховуючи HTML-інструкції в, на перший погляд, нешкідливому електронному листі — використовуючи білий на білому або мініатюрний текст — зловмисник може змусити агента виконувати додаткові команди під час аналізу вхідних повідомлень жертви, наприклад, надсилати повний вміст вибраних повідомлень, облікові дані або інші пов'язані сховища даних на URL-адресу, контрольовану зловмисником. Оскільки дія відбувається в хмарі OpenAI і не генерує вихідного трафіку, типового для шкідливого програмного забезпечення, мережа та засоби безпеки жертви не

бачать нічого підозрілого; користувач просто отримує запитуваний підсумок, не підозрюючи, що дані були викрадені…

Під час тестування ChatGPT виконував основні зловмисні команди приблизно в половині випадків, а рівень успішності різко зростав, коли приховані інструкції формулювалися як термінові запити відділу кадрів або відділу з дотримання нормативних вимог. Хоча концептуальне підтвердження Radware було зосереджено на Gmail і ChatGPT, така сама сліпа пляма, ймовірно, існує скрізь, де плагіни агентного ШІ мають доступ рівня OAuth до поштових скриньок або корпоративних додатків. Radware повідомила про цю проблему OpenAI в червні; до серпня атака вже не працювала, а Bugcrowd пізніше підтвердила, що OpenAI застосувала виправлення, хоча компанія не надала детальної інформації про свої контрзаходи. Повна, надійна захист майже напевно вимагатиме багаторівневих заходів безпеки — очищення вхідних даних, надійного логування, перевірки відповідності намірам та фільтрів на основі штучного інтелекту, здатних виявляти зловмисні комбінації природної мови, — оскільки традиційні регулярні вирази або статичні правила не в змозі впоратися з цим завданням. Коротко кажучи, підключення потужних агентів LLM до електронної пошти або інших чутливих систем створює нову, практично невиявну поверхню атаки, і для її усунення може знадобитися додаткове впровадження штучного інтелекту для контролю над штучним інтелектом…» ***(Nate Nelson. 'ShadowLeak' ChatGPT Attack Allows Hackers to Invisibly Steal Emails // TechTarget, Inc. (https://www.darkreading.com/vulnerabilities-threats/shadowleak-chatgpt-invisibly-steal-emails). 19.09.2025).***

***

«На конференції Proofpoint Protect 2025 лідери у сфері безпеки попередили, що фішинг через електронну пошту, який зараз переважно здійснюється за допомогою інструментів штучного інтелекту, залишається найбільшим вектором порушення безпеки у світі. Proofpoint, яка щодня сканує третину світового електронного трафіку (3,5 млрд повідомлень, 49 млрд URL-адрес, 3 млрд вкладень), оцінює, що шахрайство є причиною 85% з 50 млрд доларів США, втрачених нещодавно внаслідок кіберзлочинів, і що фішинг лежить в основі більшості успішних атак. Поведінка користувачів є важливим фактором: 71% співробітників визнають, що роблять «ризиковані» кліки, 58% потрапляють у класичні пастки соціальної інженерії, а понад мільйон атак щомісяця спрямовані на обхід багатофакторної автентифікації, хоча 89% захисників все ще вважають MFA майже надійним захистом…

Генеративна штучна інтелігенція (AI) значно посилює загрозу. Дослідження Proofpoint показує, що AI скорочує навантаження на зловмисника приблизно на 95%, а посилання, створені за допомогою великих мовних моделей, приваблюють на 46% більше кліків, ніж традиційні приманки. Ця технологія настільки знизила планку, що програмісти більше не потрібні: 54% керівників служб інформаційної безпеки вважають генеративну AI серйозною загрозою. Результатом цього є зростання кількості фішингу в поєднанні з програмним забезпеченням для віддаленого доступу (34% кампаній із використанням шкідливого програмного

забезпечення на основі URL-адрес), вибухове зростання кількості QR-кодів-приманок (4,2 млн у першому півріччі 2025 року) та повністю автоматизовані «агенти» спірфішингу, які повторюють і масштабують власні кампанії в режимі реального часу.

Захисники також звертаються до штучного інтелекту. Стратегія Proofpoint базується на легких, спеціалізованих моделях, які оновлюються приблизно 2,5 рази на тиждень, попередньо перевіряють пошту, перш ніж вона потрапляє до користувачів, додають попереджувальні банери та повністю блокують шкідливий трафік. Проте керівники визнали, що штучний інтелект сам по собі є «лисицею в курнику»: необхідні захисні бар'єри, журнали аудиту, відкат і аварійні вимикачі, оскільки агенти штучного інтелекту ще більш вразливі до соціальних інженерних хитрощів, ніж люди. Висновок: багаторівневий захист електронної пошти, перевірені джерела завантаження, постійне налаштування моделей штучного інтелекту та постійне навчання користувачів тепер є обов'язковими, оскільки і злочинці, і захисники змагаються за використання однієї і тієї ж потужної технології…» ***(Drew Robb. Proofpoint Exec: 'Phishing is the Leading Cause of Breaches Globally' // TechnologyAdvice (https://www.techrepublic.com/article/news-proofpoint-conference-ai-email-security-phishing/). 26.09.2025).***

***

«На саміті Financial Review Cyber Summit колишній радник уряду Австралії з питань кібербезпеки Аластер Макгіббон попередив, що електромобілі та інші розумні пристрої, пов'язані з Китаєм, становлять все більшу загрозу безпеці та національній безпеці, і заявив, що державним службовцям слід заборонити користуватися китайськими електромобілями…

Посилаючись на рішення Австралії від 2018 року про виключення «високоризикових» постачальників з 5G, він зазначив, що мільйони пристроїв Інтернету речей, «контрольованих Китаєм», зараз вбудовані в критично важливі системи, а автомобілі з підключенням до Інтернету функціонують як платформи для прослуховування та спостереження. Він описав найгірші сценарії, за яких виробники можуть дистанційно вимкнути функції безпеки побутових акумуляторів та електромобілів, що призведе до перезарядження, вимкнення, а навіть вибухів, або погіршити характеристики транспортних засобів у години пік у вибраних містах. Ризики для конфіденційності вже спонукали до вжиття запобіжних заходів, зокрема заходів, спрямованих на запобігання збору даних з електромобіля китайського виробництва, що належить міністру внутрішніх справ Тоні Берку, з огляду на занепокоєння щодо телефонних даних, прослуховування дзвінків та відстеження географічного положення. Попередження Макгіббона збігаються з діями США: адміністрація Байдена запропонувала правила щодо заборони автомобілів китайського виробництва через побоювання щодо безпеки, а австралійські законодавці, такі як Барнабі Джойс, закликали до аналогічного перегляду, поширивши перевірку на побутову техніку, таку як сонячні нагрівачі на дахах…

Зростають заклики до перегляду урядової політики, подібного до рішення щодо телекомунікацій 2018 року, навіть незважаючи на те, що китайські бренди

зараз становлять близько 80% електромобілів, що продаються в Австралії. Тільки в серпні австралійці придбали понад 20 000 автомобілів китайського виробництва, чотири китайські компанії вперше увійшли до десятки лідерів продажів, а BYD піднялася на шосте місце в загальному рейтингу, оскільки її продажі зросли майже в чотири рази в порівнянні з минулим роком». ***(NICHOLAS WILSON. Australian cyber warfare expert makes a chilling claim about Chinese EVs that every driver should read // Associated Newspapers Ltd (https://www.dailymail.co.uk/news/article-15103231/Australia-EV-China.html). 17.09.2025).***

***

«…Злочинне угруповання RevengeHotels (TA558), яке діє з 2015 року, розпочало нову фішингову кампанію, в якій використовує код, згенерований за допомогою великої мовної моделі (LLM), для доставки VenomRAT, трояна віддаленого доступу, написаного за допомогою штучного інтелекту, співробітникам готелів. Під виглядом запитів на бронювання електронні листи містять шкідливі документи, які встановлюють RAT, що дозволяє викрадати облікові дані та викрадати дані платіжних карток гостей.

Маянк Кумар, інженер-засновник DeepTempo, що спеціалізується на штучному інтелекті, каже, що цей інцидент ілюструє «як швидко штучний інтелект індустріалізує кіберзлочинність». Завдяки автоматизації виявлення вразливостей, маскування та створення поліморфного шкідливого програмного забезпечення, штучний інтелект дозволяє невеликим командам здійснювати масштабовані, високоухильні операції, що перевершують традиційні, створені вручну атаки. Іспаномовні приманки вже вразили цілі в Латинській Америці та Європі, продемонструвавши здатність штучного інтелекту долати мовні бар'єри…

Кумар попереджає, що генеративна ШІ також використовується державними організаціями для вдосконалення шкідливого програмного забезпечення, дезінформації та фішингу з використанням глибоких підробок, що значно знижує вартість складних кампаній. Він закликає захисників відмовитися від статичних інструментів на основі сигнатур і впровадити виявлення аномалій у поведінці, яке моделює нормальну активність системи та позначає відхилення. Це єдиний надійний спосіб виявити атаки, породжені ШІ, перш ніж вони знову змішаються з легітимним трафіком». ***(Tim Sandle. RevengeHotels: AI weakens cybersecurity for holidaymakers // DIGITAL JOURNAL INC. (https://www.digitaljournal.com/tech-science/revengehotels-ai-weakens-cybersecurity-for-holidaymakers/article). 17.09.2025).***

***

«Дослідники в галузі безпеки попереджають, що кіберзлочинці вже не просто експериментують з генеративним штучним інтелектом — вони інтегрують можливості великих мовних моделей (LLM) безпосередньо у свої інструменти та ланцюги атак. Компанія SentinelOne виявила, мабуть, найперший відомий зразок шкідливого програмного забезпечення з вбудованою LLM — бінарний файл Windows під назвою MalTerminal. Написана до листопада 2023 року, програма викликає GPT-4 від OpenAI під час виконання і дозволяє оператору

вибрати, чи повинна модель видавати логіку програм-вимагачів або скрипт зворотної оболонки; супутні варіанти Python роблять те саме, а супутня утиліта під назвою FalconShield просить GPT проаналізувати підозрілий код і скласти звіт про аналіз шкідливого програмного забезпечення. Хоча MalTerminal більше схожий на доказ концепції, ніж на зброю, яку можна побачити в реальному житті, він сигналізує про якісну зміну: майбутнє шкідливе програмне забезпечення може генерувати або модифікувати власні корисні навантаження на вимогу, ускладнюючи статичне виявлення та захист на основі сигнатур…

Зловмисники також використовують LLM проти самих засобів безпеки на основі штучного інтелекту. Компанія StrongestLayer нещодавно задокументувала фішингові електронні листи, які приховують рядки «prompt-injection» всередині HTML (оформлені за допомогою display:none і 1-піксельних білих шрифтів), які повідомляють сканеру штучного інтелекту, що повідомлення є звичайною інвойсом «без ознак зловмисності». Ця хитрість дозволяє електронному листу пройти через автоматичні фільтри; як тільки жертва відкриває прикріплений HTML-файл, експлойт Follina (CVE-2022-30190) завантажує корисний вантаж HTA, отримує додаткове шкідливе програмне забезпечення, вимикає Microsoft Defender і встановлює стійкість. Як HTML-, так і HTA-файли містять додаткові коментарі «отруєння LLM», щоб обдурити подальший аналіз…

Тим часом Trend Micro повідомляє про різке збільшення кількості фішингових наборів, які використовують конструктори сайтів на базі штучного інтелекту, такі як Lovable, Netlify і Vercel, для масового створення підроблених сторінок CAPTCHA, що перенаправляють на сайти для збору облікових даних. Безкоштовний хостинг, надійний брендинг і розгортання в один клік, які пропонують ці платформи, дозволяють зловмисникам швидко і дешево запускати масштабні кампанії, тоді як сканери безпеки часто зупиняються на нешкідливому на вигляд етапі CAPTCHA.

В цілому, результати дослідження показують, що інструменти генеративного штучного інтелекту стають мультиплікатором сили для зловмисників, допомагаючи їм створювати переконливі приманки, обходити захист на основі штучного інтелекту і навіть генерувати живий шкідливий код, відкриваючи нову еру адаптивних, недорогих і масових кібератак…» ***(Ravie Lakshmanan. Researchers Uncover GPT-4-Powered MalTerminal Malware Creating Ransomware, Reverse Shell // The Hacker News (https://thehackernews.com/2025/09/researchers-uncover-gpt-4-powered.html). 20.09.2025).***

***

Кіберзлочинність та кібертероризм

«У середу компанія Jaguar Land Rover підтвердила, що дані були скомпрометовані в результаті кібератаки, яка змусила її зупинити діяльність минулого тижня, а виробництво на заводах у Великій Британії та за кордоном, як очікується, буде призупинено щонайменше до понеділка.

Найбільший британський виробник автомобілів заявив у середу, що його криміналістичне розслідування, проведене за підтримки зовнішніх фахівців з кібербезпеки, встановило, що «деякі дані були порушені», і що про це було повідомлено регуляторні органи…

Ця атака, вперше виявлена минулого вівторка, змусила JLR зупинити виробництво і відправити працівників додому.

Заводи в Мідлендсі, Мерсісайді та за кордоном залишаються закритими, а також постраждали постачальники, деякі з яких не мають доступу до систем, що використовуються для постачання запасних частин або реєстрації транспортних засобів.

Однак роздрібна торгівля та сфера послуг продовжують працювати у звичайному режимі…

Хакерська група під назвою Scattered Spider взяла на себе відповідальність за інцидент, опублікувавши скріншоти, на яких нібито видно внутрішні IT-системи JLR…

Це порушення стало одним із найсерйозніших кіберінцидентів, з якими зіткнувся виробник, що належить Tata, за останні роки, і аналітики попереджають, що фінансові та операційні витрати можуть бути значними, якщо системи залишатимуться поза мережею протягом тижнів…» ***(Josh White. JLR confirms some data compromised in cyberattack // VORTEX MEDIA NETWORK SL (https://www.sharecast.com/news/news-and-announcements/jlr-confirms-some-data-compromised-in-cyberattack--20870149.html). 10.09.2025).***

***

«Jaguar Land Rover (JLR) почав відновлювати частину своїх цифрових операцій після того, як 2 вересня через масштабну кібератаку компанія була змушена зупинити виробництво, що призвело до порушення ланцюга поставок і залишення тисяч працівників вдома. У нещодавньому повідомленні компанія зазначила, що тривають роботи з відновлення, зокрема повернення до нормального функціонування Глобального центру логістики запчастин, ліквідація заборгованості перед постачальниками та відновлення фінансових систем для оптового продажу та реєстрації автомобілів. Компанія JLR, що належить Tata, співпрацює з правоохоронними органами, судовими експертами та Національним центром кібербезпеки Великобританії, щоб забезпечити безпечний повторний запуск, хоча відновлення виробництва було відкладено до 1 жовтня. Інцидент, який приписують кіберзлочинній групі Scattered Spider, також супроводжувався крадіжкою даних клієнтів — що спочатку заперечувалося автовиробником, але згодом було підтверджено — що додало серйозності порушенню роботи…» ***(David Jones. Jaguar Land Rover begins phased restoration of services following cyberattack // TechTarget, Inc. (https://www.cybersecuritydive.com/news/jaguar-land-rover-restoration-cyberattack/761251/). 26.09.2025).***

***

«Фінансові установи стикаються з дедалі більшим мінним полем кібербезпеки, де кількість витоків даних подвоїлася з 2023 року, що дедалі більше впливає на довіру компанії до ринку або її регуляторний статус.

Згідно зі звітом AInvest, кількість порушень безпеки з боку третіх сторін у фінансовому секторі подвоїлася з 2023 року. У звіті також зазначається, що середні збитки від порушення безпеки сягають 4,8 мільйона доларів, а інциденти, пов'язані з інсайдерами, коштують 17,4 мільйона доларів на організацію.

Зі зростанням кількості кібератак від сторонніх постачальників та інсайдерів, інвестори починають ретельно перевіряти акції фінтех- та банківських компаній на предмет кіберстійкості так само пильно, як і прибуток на акцію.

На стримування хакерських атак такого типу часто потрібно близько 80 днів, що ілюструє, як експерти досі намагаються протидіяти ризикам у реальному часі.

Наслідки виходять за рамки балансових звітів: наприклад, транскордонний витік даних Santander у 2025 році підірвав його ринкові позиції ще до того, як було стягнуто штрафи регуляторів.

Під час цієї атаки було викрадено дані 30 мільйонів клієнтів з Іспанії, Уругваю та Чилі, а також деяких співробітників Santander, зокрема їхні персональні дані, такі як номери соціального страхування. У жовтні 2024 року банк був оштрафований на 50 000 євро іспанським агентством із захисту даних (AEPD) за неповідомлення про порушення та порушення Загального регламенту про захист даних (GDPR).

«Після розслідування ми підтвердили, що було отримано доступ до певної інформації, що стосується клієнтів Santander у Чилі, Іспанії та Уругваї, а також до всіх нинішніх та деяких колишніх співробітників групи Santander», – йдеться у заяві, опублікованій тоді.

«У базі даних немає жодних транзакційних даних, а також жодних облікових даних, які б дозволили здійснювати транзакції за рахунками, включаючи реквізити онлайн-банкінгу та паролі».

Ці тенденції узгоджуються з дослідженням Міжнародного валютного фонду, яке показало, що зростаючі масштаби та складність кібератак на фінансову інфраструктуру зараз достатньо великі, щоб загрожувати економічній стабільності.

Зростання вартості кібервтрат після того, як порушення було виявлено, розкрито клієнтам та оштрафовано регуляторами, зросло до 2,5 мільярда доларів, враховуючи вплив на репутацію, регулювання та коригувальні заходи…

Для інвесторів ключовий висновок очевидний: зрілість кібербезпеки має враховуватися при оцінці та виборі акцій, особливо у фінтех- та банківському секторах.

Компанії, що інвестують в архітектуру нульової довіри, що означає вимогу суворої перевірки кожного користувача, пристрою та програми перед наданням доступу до ресурсів, а також виявлення аномалій на основі штучного інтелекту, ймовірно, будуть краще захищеними та безпечнішими для інвесторів, які хочуть уникнути хакерських атак.

Крім того, компанії, які проводять ретельні щоквартальні аудити своїх планів кібербезпеки від сторонніх організацій, отримують набагато більше довіри з боку ринків капіталу.

Операційна стійкість є ще одним критичним фактором, оскільки установи, що беруть участь у кібервійськових іграх та навчаннях з реагування на інциденти, організованих такими організаціями, як Федеральна резервна система та FS-ISAC, сприймаються більш схвально.

Ще одна ознака того, що банки серйозно ставляться до безпеки? Керівники фінансових установ, які надають пріоритет навчанню співробітників кібербезпеці, визнані тим, що ефективно усувають найнебезпечніші прогалини в ланцюжку захисту, покращуючи загальне управління ризиками для людей.

Поєднання регуляторного тиску, зростання фінансових наслідків та геополітичних кіберзагроз означає, що інвестори більше не можуть дозволити собі ігнорувати показники кібербезпеки. Фірми, які ставляться до оборони як до центру витрат, зрештою можуть мати гірші результати, ніж ті, хто розглядає її як стратегічний актив.

Фінансові установи, які дотримуються надійної кібергігієни, передбачають нові загрози, включаючи ризики, пов'язані зі штучним інтелектом та квантовими системами, та відповідають регуляторним очікуванням, цілком можуть виділитися як перевірені лідери, а не як потенційні пасивні ресурси. Безпека завтрашнього балансу цілком може залежати від сили сьогоднішнього захисту». ***(Riley Gutiérrez McDermid. Bank Hacking Has Doubled Since 2023 And Investors Are Getting Spooked // GIZMODO USA LLC. (https://gizmodo.com/bank-hacking-cybersecurity-investors-spooked-2000653618). 06.09.2025).***

***

«…У рамках, ймовірно, найбільшої на сьогоднішній день атаки на ланцюжок поставок, хакери проникли в пакети програмного забезпечення з відкритим кодом, які щотижня оновлюються понад 2 мільярди разів, і скомпрометували майже два десятки пакетів, розміщених у репозиторії npm. Про атаку стало відомо в понеділок після того, як у соціальних мережах з'явилися повідомлення про те, що Джош Джунон (псевдонім Qix), адміністратор уражених пакетів, став жертвою фішингового листа. У листі, надісланому з підробленого домену (support.npmjs.help), стверджувалося, що його обліковий запис npm буде закрито, якщо він не оновить свої дані для двофакторної автентифікації (2FA). Джунон зізнався, що попався на цю аферу, заявивши: «Вибачте всім, я мав бути більш уважним»…

Протягом години після захоплення облікового запису зловмисники відправили шкідливі оновлення до 20 пакетів npm, ввівши код, призначений для перехоплення транзакцій з криптовалютою. Шкідливе програмне забезпечення, що складалося з 280 рядків, відстежувало заражені системи на предмет переказів, пов'язаних з Ethereum, Bitcoin, Solana, Tron, Litecoin і Bitcoin Cash, замінюючи адреси гаманців одержувачів на ті, що контролювалися хакерами. Скомпрометовані пакети, включаючи широко використовувані залежності, такі як chalk, debug та ansi-styles, є основою екосистеми JavaScript, що посилює масштаби атаки. Компанія з безпеки Socket попередила, що масштаби порушення вказують на цілеспрямовані зусилля з метою максимізації збитків у всій спільноті відкритого програмного забезпечення…

Цей інцидент збігся з двома іншими атаками на ланцюжок поставок:

1. GitGuardians розкрив порушення, яке торкнулося 3325 секретів аутентифікації в PyPI, npm, Docker Hub, GitHub, Cloudflare та AWS, при цьому 327 користувачів GitHub були скомпрометовані через зловмисні оновлення пакетів…

2. Wiz повідомив про атаку на Nx, систему побудови, під час якої хакери викрали токени GitHub і npm, зловживали інструментами командного рядка AI для пошуку конфіденційних файлів і оприлюднили приватні репозиторії, зробивши їх загальнодоступними. Викрадені облікові дані були завантажені до репозиторіїв під назвою s1ngularity-repository, що спонукало Wiz назвати цю кампанію «s1ngularity»…

Атака npm підкреслює зростаючу загрозу компрометації ланцюгів постачання, що використовують доступ адміністраторів та фішинг-тактики. Експерти закликають до підвищеної пильності, особливо щодо запитів 2FA та неперевірених доменних комунікацій…» ***(Dan Goodin. Software packages with more than 2 billion weekly downloads hit in supply-chain attack // Condé Nast (https://arstechnica.com/security/2025/09/software-packages-with-more-than-2-billion-weekly-downloads-hit-in-supply-chain-attack/). 09.09.2025).***

***

«У вихідні на День праці 2025 року Cloudflare успішно нейтралізувала рекордну розподілену атаку на відмову в обслуговуванні (DDoS), яка досягла піку в 11,5 терабіт на секунду (Тбіт/с), що майже на 60% перевищило попередній рекорд у 7,3 Тбіт/с, встановлений лише кількома місяцями раніше. Атака, яка тривала приблизно 35 секунд, наводнила ціль понад 5,1 мільярда пакетів на секунду гіпер-об'ємним потоком протоколу користувацьких дейтаграм (UDP), призначеним для насичення пропускної здатності та виснаження серверних ресурсів…

Атака була спричинена комбінацією скомпрометованих пристроїв Інтернету речей та хмарних провайдерів, серед яких Google Cloud був одним з найпомітніших джерел, хоча більшість атак були здійснені з інших інфраструктур. Автономна, глобально розподілена мережа Cloudflare виявила та нейтралізувала атаку в режимі реального часу без ручного втручання, не допустивши перебоїв в обслуговуванні клієнтів.

Цей інцидент підкреслює тривожну тенденцію: DDoS-атаки зростають як за масштабами, так і за частотою. Лише у другому кварталі 2025 року Cloudflare заблокував понад 6 500 гіпер-об'ємних атак - в середньому 71 на день - і вже запобіг 27,8 мільйонам DDoS-атак у 2025 році, що на 30% перевищує показник 2024 року. Зловмисники все частіше використовують хмарні ресурси та ботнети Інтернету речей для проведення коротких, але потужних атак…» ***(Steven Vaughan-Nichols. Cloudflare stops new world's largest DDoS attack over Labor Day weekend // ZDNET (https://www.zdnet.com/article/cloudflare-stops-new-worlds-largest-ddos-attack-over-labor-day-weekend/). 02.09.2025).***

***

«…Виборча комісія Великобританії витратила три роки і понад 250 000 фунтів стерлінгів на відновлення після масштабної кібератаки, в результаті якої особисті дані 40 мільйонів виборців потрапили до рук хакерів, які, як підозрюється, підтримуються китайською державою. Порушення, вперше виявлене в жовтні 2022 року, залишалося непоміченим протягом більше року після того, як зловмисники скористалися незакритою вразливістю в Microsoft Exchange в серпні 2021 року, незважаючи на поширені попередження про цю вразливість…

У своєму першому інтерв'ю про злом новий генеральний директор комісії Віжай Рангараджан визнав, що організація допустила серйозні помилки в системі безпеки, зокрема не оновила програмне забезпечення, використовувала слабкі паролі та проігнорувала поради Національного центру кібербезпеки (NCSC). Хакери отримали доступ до повного реєстру виборців (імен та адрес усіх виборців Великої Британії) та всіх внутрішніх електронних листів, що викликало побоювання, що вони могли зірвати вибори, хоча доказів втручання виявлено не було…

Управління комісара з питань інформації (ICO) винесло офіційне зауваження, не наклавши штраф, але законодавці та зацікавлені сторони були «шоковані самозаспокоєністю». Рангараджан визнав, що співробітники недооцінили ризик, незважаючи на гучні випадки, такі як хакерська атака на вибори в США у 2016 році.

Після порушення комісії було проведено реорганізацію системи кібербезпеки, отримано найвищий рівень сертифікації NCSC (Cyber Essentials Plus) та збільшено бюджет на забезпечення безпеки. Однак повний масштаб дій хакерів залишається невідомим, що викликає тривогу щодо можливого зловживання даними або майбутніх загроз виборам…» ***(Joe Tidy. It's taken three years to recover from China hack, election watchdog says // BBC (https://www.bbc.com/news/articles/c80gl8yvj9go). 09.09.2025).***

***

«…На початку 2025 року кількість кібератак на навчальні заклади різко зросла. За даними Check Point Research, з січня по липень, коли школи та коледжі повернулися до навчання, їх кількість зросла на 41% порівняно з аналогічним періодом минулого року. У середньому на кожну організацію щотижня припадало 4356 атак, і цей сектор залишався найбільш уразливим у світі, випереджаючи урядові установи (2716), телекомунікації (2636) та охорону здоров'я (2468). Найбільше постраждав регіон Азіатсько-Тихоокеанського регіону, де в середньому за тиждень на одну організацію припадало 7869 атак, тоді як Північна Америка зазнала найрізкішого річного зростання на 67%, а найбільший стрибок на рівні країни зафіксували установи США… Використовуючи свою платформу ThreatCloud AI, Check Point пов'язує вразливість освіти з великою залежністю від онлайн-платформ і публічних мереж, поширеним розкриттям облікових даних, обмеженими бюджетами та недостатньою обізнаністю студентів і співробітників у питаннях кібербезпеки. Ці висновки відображають більш широкі тенденції в бізнесі — 78% компаній стикалися з програмним забезпеченням-вимагачем протягом останнього року, оскільки атаки на основі штучного інтелекту стають все

складнішими для виявлення, що підкреслює необхідність збільшення бюджетів на безпеку, залучення нових талантів та підвищення кваліфікації персоналу. Однак, оскільки 98% керівників не в змозі виявити всі ознаки фішингу, перспективи залишаються тривожними без рішучих дій…» ***(Gus Mallett. Study: Cyberattacks Against US Education Sector Are on the Rise // Marketing VF Ltd. (https://tech.co/news/cyberattacks-us-education-sector-rise). 08.09.2025).***

***

«…Група кіберзлочинців ShinyHunters привернула увагу всього світу після того, як Google закликав 2,5 мільярда користувачів посилити безпеку після злом Salesforce, підкресливши зростання популярності голосової соціальної інженерії («вішингу»), в якій зловмисники видають себе за співробітників служби технічної підтримки, щоб виманити паролі та багатофакторні коди. Ця тактика все частіше використовується завдяки глибоким підробкам та генеративному клонуванню голосу за допомогою штучного інтелекту і застосовується проти таких компаній, як Qantas, Pandora, Adidas, Chanel, Tiffany & Co. та Cisco… Активна з 2020 року і відома спробами продати дані 73 мільйонів клієнтів AT&T, ShinyHunters перейшла від експлуатації вразливостей хмарних і веб-додатків до атак на постачальників послуг з управління клієнтами, таких як Salesforce, щоб отримати доступ до багатих наборів даних про багатьох клієнтів; в середині серпня вона заявила про співпрацю з Scattered Spider і Lapsus$, опублікувала 2,8 мільйона записів Allianz Life Salesforce, перш ніж її канал Telegram був видалений, перейменований в Scattered Lapsus$ Hunters і почав пропонувати програмне забезпечення для вимагання викупу з перевагою для публічного вимагання… Членство та псевдоніми часто перетинаються між цими міжнародними угрупованнями (наприклад, Scattered Spider також називають UNC3944, Oktapus, Octo Tempest, Storm-0875, Muddled Libra). Хоча окремі користувачі можуть в основному залишатися пильними, організації можуть зменшити ризик вішингу за допомогою інформування та навчання на основі сценаріїв, посиленої верифікації (перевірка посвідчення особи на камеру та складніші контрольні питання) та багатофакторної автентифікації, стійкої до фішингу, такої як збіг номерів та геоверифікація…» ***(Jennifer Medbury. Who are ShinyHunters? The hacking group that targeted Google // Independent (https://www.independent.co.uk/tech/google-data-breach-shinyhunters-cyber-attack-b2821097.html). 05.09.2025).***

***

«Eclypsium, компанія з безпеки ланцюгів поставок, спостерігає сплеск сканування шкідливих програм. Сканування впливає як на споживче, так і на корпоративне обладнання та пов'язане зі скомпрометованими маршрутизаторами Cisco, Linksys та Araknis.

Фонд Shadowserver раніше попереджав про понад 2200 нових скомпрометованих маршрутизаторів.

«Для зловмисників це не має значення, головне, щоб це працювало», – йдеться у звіті Eclypsium.

«Інструменти та методи атаки, спрямовані на мережеві пристрої та Інтернет речей, можуть варіюватися від найновіших експлойтів нульового дня до тих, яким 15 років і більше».

У спостережуваних атаках зловмисники були спеціально спрямовані на:

- Маршрутизатори Cisco Small Business серії RV, більшість з яких мають термін служби до кінця (EOL) і не отримують оновлень прошивки чи підтримки.
- Моделі серії Linksys LRT, які досягли кінця терміну служби, але можуть отримувати деяку розширену підтримку.
- Araknis Networks AN-300-RT-4L2W, який є кінцевим продуктом, і оновлення прошивки не розповсюджуватимуться.

Окремо, ФБР раніше попереджало про хакерів, які націлені на застаріле мережеве обладнання, що приймає застарілі, незашифровані протоколи, такі як Cisco Smart Install (SMI) та Simple Network Management Protocol (SNMP).

Незважаючи на те, що вразливості, яка відстежується як CVE-2018-017, сім років, російські зловмисники все ще успішно її використовують.

Дослідники попереджають, що для вразливих маршрутизаторів, що використовуються приватними особами або малим бізнесом, доступно мало засобів виявлення та запобігання – навіть якщо патч доступний, багато хто його не встановлює. Тим часом зловмисники можуть легко сканувати Інтернет на наявність вразливих пристроїв…

Дослідники наполягають на вимкненні та заміні застарілих незашифрованих протоколів, включаючи TELNET та SNMP або SMI для пристроїв Cisco, а також на гарантії того, що системи оновлені…» ***(Ernestas Naprys. Surge in malicious scans for outdated routers: hackers hunting for old Cisco, Linksys gear // Cybernews (https://cybernews.com/security/surge-in-malicious-scans-for-outdated-routers/). 04.09.2025).***

***

«…Керівники служб безпеки часто вважають даркнет лише кримінальним середовищем, але насправді це важливе джерело раннього попередження: групи хакерів, що використовують програми-вимагачі, та посередники, що надають початковий доступ, рекламують там викрадені дані, облікові дані та точки доступу до мережі, сигналізуючи про те, що ви стали жертвою зломів або є їхньою ціллю. Ефективні програми постійно відстежують журнали крадіжок, згадки про бренди та домени, а також пропозиції доступу до RDP/VPN/адміністратора, перевіряють будь-які виявлені дані, визначають масштаб і стримують активні вторгнення, зберігають докази, повідомляють про необхідність та готуються до вимагання… Інформація з даркнету також допомагає формувати стратегію, розкриваючи, які групи, сектори та вразливості є актуальними; команди повинні поєднувати це з каналами ISAC/CERT, відстежувати експлуатовані CVE у своєму технологічному стеку та стежити за оголошеннями про набір учасників загроз, які вказують на фокус галузі. Моніторинг варіюється від інструментів для початківців, таких як Have I Been Pwned, до інформаційних платформ (наприклад, Flashpoint, Recorded Future) та комерційних послуг, таких як SpyCloud (оперативні сповіщення про витоки/повноваження з інтеграцією SOC) та DarkOwl

(пошук/аналітика), але закриті форуми, канали Telegram та сайти для зливу даних вимагають досвідчених аналітиків або надійних партнерів… Обман (медові банки, канарські токени) може виявити внутрішні та зовнішні загрози, якщо його правильно інтегрувати з SIEM/XDR, а фахівці повинні використовувати надійні засоби OPSEC (Tor, VPN, спеціальні пристрої, блокування скриптів). Дивіться за межі власного периметра на ризики, пов'язані з третіми сторонами, відстежуючи згадки про ключових постачальників, MSP, SaaS, SSO/CRM або хмарних провайдерів, які можуть бути використані для латерального переміщення… Найголовніше — підключіть зовнішні сигнали до систем виявлення та реагування: співвіднесіть витоки індикаторів з телеметрією автентифікації та ідентифікації в AWS, Azure, Okta, M365; у разі виявлення витоку скасуйте доступ, перереєструйте MFA, ізолюйте служби та виконайте сценарії дій. Відстежуючи розмови в даркнеті та порівнюючи їх із внутрішніми аномаліями, команди можуть виявляти та запобігати атакам на етапі планування, а не лише після їхнього впливу…» ***(Josh Fruhlinger. A CISO's guide to monitoring the dark web // IDG Communications, Inc. (https://www.csoonline.com/article/4046242/a-cisos-guide-to-monitoring-the-dark-web.html). 03.09.2025).***

***

«Chess.com, найбільша і найпопулярніша онлайн-платформа для гри в шахи, підтвердила, що стала жертвою кібератаки, в результаті якої втратила конфіденційну інформацію про невелику частину своїх користувачів.

У повідомленні про витік даних, поданому до Генеральної прокуратури штату Мен, компанія зазначила, що інцидент стався 5 червня і був виявлений приблизно через два тижні, 19 червня.

Загалом було викрадено дані 4541 особи з понад 200 мільйонів зареєстрованих користувачів Chess.com.

Хакери, імена яких не були названі в звіті, змогли викрасти дані за допомогою стороннього інструменту для передачі файлів, який використовував Chess.com.

Компанія не захотіла назвати, який саме інструмент це був, але Recorded Future News знайшла два популярних бренди інструментів для передачі файлів — Wing FTP і CrushFTP, які в липні 2025 року повідомили про «серйозні вразливості» і закликали клієнтів встановити виправлення.

Компанія також підкреслила, що її код та інфраструктура залишилися неушкодженими і що на даний момент немає доказів того, що викрадені файли були використані зловмисниками.

Невідомо, яку саме інформацію вони викрали, окрім імен людей, оскільки Chess.com підтвердила лише те, що банківська інформація та дані для входу не були скомпрометовані.

Наразі ніхто не взяв на себе відповідальність за цей напад…» ***(Sead Fadilpašić. Not quite checkmate yet - thousands of Chess.com fans may have had details stolen in cyberattack, here's what we know // Future US, Inc. (https://www.techradar.com/pro/security/thousands-of-chess-com-fans-may-have-had-details-stolen-in-cyberattack). 05.09.2025).***

***

«…Wiz повідомляє, що атака на ланцюжок постачання «s1ngularity» використовувала скомпрометований токен NPM для платформи Nx build, щоб опублікувати вісім шкідливих випусків, які в Linux і macOS запускали після інсталяції telemetry.js для пошуку секретів (API-ключі, токени GitHub/NPM, SSH-ключі, криптогаманці) та інші конфіденційні файли, а потім кодували їх у base64 і викрадали, автоматично створюючи публічні репозиторії GitHub з назвами, що містили варіації «s1ngularity-repository»; корисне навантаження також втручалося в файли запуску оболонки, щоб вивести з ладу нові термінали, і намагалося використовувати CLI-інтерфейси штучного інтелекту (наприклад, Claude, Gemini) для розвідки та викрадення даних, при цьому було виявлено три різних корисних навантаження. Викриті журнали серверів та подальший аналіз пов'язали понад 20 000 викрадених файлів із 225 користувачами, понад 2300 витоками секретної інформації та щонайменше 1700 користувачами, чиї секрети були викриті (кожен із них мав токен GitHub), хоча справжня кількість жертв, ймовірно, є вищою; приблизно половина жертв мали встановлені AI CLI, але витік даних за допомогою AI відбувся менш ніж у 25% випадків, і менше ніж 100 унікальних дійсних секретів було підтверджено у 20 000 файлів — переважно для AI-сервісів (Langsmith, Anthropic, OpenAI) та хмарних платформ (AWS, Azure, Vercel), без підтвердженого викрадення криптовалюти. Після початкових заходів з вилучення (скасування токена Nx, видалення пакетів і репозиторіїв) зловмисники використовували скомпрометовані облікові дані для доступу до 480 облікових записів (близько 300 організаційних) і публічного розкриття понад 6700 приватних репозиторіїв (одна організація втратила понад 700), а згодом використовували два облікові записи користувачів для публікації понад 500 репозиторіїв із суфіксом _bak для однієї організації; GitHub згодом видалив їх. Для OPSEC зловмисники спочатку використовували webhook.site (що допомогло скомпрометувати токен Nx, але обмежує анонімні записи), а потім перейшли до витоку даних тільки тоді, коли був присутній gh CLI і можна було створити публічне репозиторій, уникаючи власної інфраструктури. Wiz закликає шукати IoC, змінювати всі секретні дані та перевіряти журнали аудиту GitHub на наявність подій org_credential_authorization.deauthorize; близько 100 унікальних токенів NPM (понад 40% тих, що були викрадені раніше) залишаються дійсними, тоді як лише ~5% скомпрометованих токенів GitHub все ще активні…» ***(Ionut Arghire. Over 6,700 Private Repositories Made Public in Nx Supply Chain Attack // SecurityWeek (https://www.securityweek.com/over-6700-private-repositories-made-public-in-nx-supply-chain-attack/). 08.09. 2025).***

***

«Літня перерва в роботі телекомунікаційних мереж Люксембургу була спричинена реакцією внутрішніх систем Пошти на кібератаку, а не самою атакою, заявив міністр економіки Лекс Деллес. Хоча стаціонарні (VoIP) та мобільні мережі не залежать безпосередньо від Інтернету і технічно залишалися працездатними, 23 липня багато користувачів втратили доступ до послуг на близько чотири години, через що тисячі людей не могли зателефонувати за

номером 112, оскільки деякі клієнти не могли підключитися до DNS-серверів, а мобільна мережа перейшла в аварійний режим, що погіршило якість зв'язку. Спочатку Пошта звинуватила програмне забезпечення, а потім підтвердила кібератаку; Деллес підкреслив, що заходи, які вплинули на VoIP, відображали реакцію систем управління мережею Пошти на раптові зміни трафіку, а не саму загрозу. Після спільного аналізу з GovCERT, технологічний провайдер Пошти надав технічні рекомендації щодо протидії подібним атакам, а влада оцінила потенційний вплив на критичну інфраструктуру та залучила операторів. Уряд не планує вводити нові правила кібербезпеки для телекомунікаційних провайдерів та їхніх постачальників…» ***(Aaron Grunwald. Cyberattack hit Post servers, not phone network itself, says economy minister // The Luxembourg Times (https://www.luxtimes.lu/luxembourg/cyberattack-hit-post-servers-not-phone-network-itself-says-economy-minister/88853555.html). 08.09.2025).***

***

«…У звіті Nova Scotia Power, поданому до провінційної Енергетичної комісії Нової Шотландії, про кібератаку в березні 2025 року детально описано «складне та скоординоване» вторгнення, яке, ймовірно, зачепило набагато більше ніж приблизно 277 000 клієнтів, про яких вже було повідомлено, — потенційно всіх клієнтів — і підтверджує, що деякі викрадені дані були опубліковані в даркнеті. Компанія заявляє, що атака сталася приблизно 19 березня, але була виявлена лише 25 квітня, коли програми перестали працювати; негайне розслідування виявило несанкціонований доступ до частин її IT-мережі, і до 1 травня було встановлено, що інформація про клієнтів була порушена, і клієнтів попередили про необхідність бути пильними. Порушення призвело до збою в білінгу: після паузи з 25 квітня по 4 червня компанія виставила рахунки на основі попереднього року використання, через що деякі рахунки здавалися завищеними через необроблені платежі, коротші інтервали білінгу або оцінки, що не відображали останні зміни; NS Power скасувала штрафи за прострочення платежів і пообіцяла коригування, щоб клієнти не платили за електроенергію, яку вони не використовували. Компанія видалить усі номери соціального страхування клієнтів зі своїх файлів, а 28 травня Управління комісара з питань конфіденційності Канади розпочало розслідування. Щоб зменшити ризик, NS Power пропонує п'ять років безкоштовного моніторингу кредитної історії TransUnion з моніторингом даркнету та відшкодуванням витрат до 1 мільйона доларів; після деяких труднощів із реєстрацією компанія додала онлайн-поради та провела понад 30 очних сесій і заявляє, що тепер більшість користувачів можуть зареєструватися за лічені хвилини. Запити на інформацію від Енергетичної комісії відображають занепокоєння клієнтів щодо зловживання особистими даними та проблем із моніторингом кредитної історії; оцінка масштабів NS Power триває, і планується надсилання подальших повідомлень у міру виявлення додаткових постраждалих клієнтів…» ***(Sean Mott. All customers potentially impacted by NS Power cyberattack: report // BellMedia (https://www.ctvnews.ca/atlantic/nova-scotia/article/all-customers-potentially-impacted-by-ns-power-cyberattack-report/). 08.09.2025).***

***

«…Недавні кіберінциденти в ланцюжку поставок, спрямовані проти британських роздрібних торговців і виробників, підкреслюють просту істину: середні та великі організації повинні бути готові не тільки відбивати атаки, але й працювати та відновлюватися, коли системи пошкоджені. Національний центр кібербезпеки (NCSC) радить почати з основ: впровадити п'ять основних заходів контролю в рамках схеми Cyber Essentials — своєчасне встановлення виправлень, суворе управління доступом, безпечна конфігурація, захист від шкідливого програмного забезпечення та захист меж — щоб блокувати більшість загроз. Більші або більш складні підприємства повинні розширити цю основу за допомогою Cyber Assessment Framework (CAF), яка допомагає їм ідентифікувати критично важливі послуги, оцінити ризики, яким піддаються ці послуги (чи то від випадкових злочинців, чи то від досвідчених зловмисників), та забезпечити їх підтримку або відновлення під час збою…

Планування без репетицій не має сенсу. Організації, які найкраще справляються з ситуацією, вже склали карту своїх IT-ресурсів, провели аналіз впливу на бізнес, щоб визначити, що має залишатися в робочому стані, призначили чіткі ролі та канали комунікації на випадок кризових ситуацій і відпрацювали процес прийняття рішень за допомогою настільних вправ. Такі навчання дозволяють продовжувати роботу для клієнтів і партнерів навіть під час відновлення технологій.

Стійкість також є колективним зусиллям: галузеві групи довіри та форуми для обміну інформацією, що підтримуються NCSC, процвітають завдяки відвертому повідомленню про інциденти та отриманому досвіду, підвищуючи стандарти в цілих галузях. Правління та генеральні директори повинні контролювати цю роботу; керівництво NCSC «Кіберуправління для правлінь» показує лідерам, як інтегрувати кіберризики в стратегічні рішення…

NCSC закликає організації використовувати його рекомендації щодо реагування та відновлення, впроваджувати Cyber Essentials та застосовувати CAF — практичні кроки, що сприяють зміцненню впевненості у здатності протистояти збуренням, швидко відновлюватися та залишатися працездатними.» ***(Jonathon Ellison. Cyber resilience matters as much as cyber defence // National Cyber Security Centre (https://www.ncsc.gov.uk/blog-post/why-resilience-matters-as-much-as-defence). 09.09.2025).***

***

«…Нове опитування SecurityScorecard, в якому взяли участь 546 IT-керівників, показує, що кіберризики в ланцюгах постачання стрімко зростають: 71% організацій за останній рік зазнали принаймні одного істотного інциденту, пов'язаного з третіми сторонами, а 5% — десяти або більше, тоді як дані Verizon показують, що частка порушень, пов'язаних із третіми сторонами, майже подвоїлася і становить 30%. Оскільки сучасні підприємства покладаються на розгалужену мережу постачальників, провайдерів SaaS та відкритого коду, зловмисники тепер віддають перевагу найслабшій ланці — підрядникам, хмарним платформам або CI/CD-конвеєрам — замість «головних

воріт»… Недавні компрометації, пов'язані з Salesforce, Workday, Colt Technology і Farmers Insurance, а також кампанії таких груп, як «Murky Panda», ілюструють, як викрадені токени OAuth, інтеграції з надмірними правами доступу та шкідливі пакети в репозиторіях, таких як npm або PyPI, дозволяють злочинцям «увійти, а не зламати», успадковуючи довіру та доступ, вже надані вище за течією. Через п'ять років після катастрофи SolarWinds багато конвеєрів розробки залишаються неправильно налаштованими, SBOM розглядаються як статична паперова робота, і лише 21 % компаній заявляють, що навіть половина їх розширеного ланцюжка поставок підпадає під дію активної програми кібербезпеки; лише 26 % включають планування реагування на інциденти в управління ризиками третіх сторін. Тому експерти закликають перейти від анкет до твердих доказів — багатофакторної автентифікації, реєстрації, розгортання EDR, пен-тестів, симуляцій фішингу, настільних вправ та обов'язкових положень про повідомлення про порушення — одночасно отримуючи можливість відстежувати в режимі реального часу кожен компонент програмного забезпечення, залежність та зв'язок з постачальниками…» ***(John Leyden. 71% of CISOs hit with third-party security incident this year // IDG Communications, Inc. (https://www.csoonline.com/article/4051668/71-of-cisos-hit-with-third-party-security-incident-this-year.html). 09.09.2025).***

***

«…Кібербезпека зараз є невід'ємною частиною безперебійної роботи бізнесу, оскільки сучасні загрози можуть паралізувати організації будь-якого розміру. Основні небезпеки можна розділити на сім категорій: (1) шкідливе програмне забезпечення — програми-вимагачі, шпигунські програми або віруси, приховані в переконливих електронних листах і на веб-сайтах, — руйнують системи або викрадають дані; (2) фішинг використовує все більш реалістичні повідомлення, створені за допомогою штучного інтелекту, для збору облікових даних, як це було в разі злом Twitter у 2020 році; (3) відмова в обслуговуванні (DoS) і розподілені DoS-атаки паралізують послуги та завдають значних фінансових збитків; (4) атаки типу «людина посередині», поширені в незахищених мережах Wi-Fi, непомітно перехоплюють дані для входу та фінансові дані; (5) SQL-ін'єкції використовують слабкі веб-форми для доступу до баз даних і викрадення записів про клієнтів; (6) експлойти нульового дня використовують невідомі програмні недоліки, такі як баг Chrome 2022 року, до того, як з'явиться виправлення; та (7) DNS-тунелювання приховує шкідливий трафік у звичайних запитах доменних імен, щоб обійти брандмауери. Розуміння цих векторів є першим кроком до захисту особистої інформації та безпеки підприємства…» ***(Mardi McNaughton. Cybersecurity 101: Common types of cyber attacks // DIGITAL JOURNAL INC. (https://www.digitaljournal.com/business/cybersecurity-101-common-types-of-cyber-attacks/article). 11.09.2025).***

***

«…Radio World повідомляє про серію очевидних хакерських атак на радіостанції, що використовують обладнання Barix AoIP, які відбулися в період з 29 серпня до Дня праці. В результаті атак з уражених пристроїв

транслювалися нецензурні матеріали та підроблені повідомлення EAS. Флетчер Прайд з Family First Radio Network підкреслив, що 600–650 пристроїв Barix є загальнодоступними в усьому світі (близько 300 у США), стверджуючи, що пристрої, які рекламують свою присутність перед входом у систему, полегшують їх виявлення. Серед постраждалих станцій – KRLL(AM) у Каліфорнії, штат Міссурі, та KPOG(LP) у Де-Мойні; захищений паролем Exstreamer KPOG з переадресацією портів був захоплений, а його пароль змінено, що змусило виконати заводське скидання налаштувань, після чого станція змінила облікові дані та планує додати VPN. Подібні випадки захоплення Barix були зафіксовані в 2016 році, коли компанія закликала використовувати надійні, довгі паролі, захист брандмауером і не підключати пристрої до відкритого Інтернету — рекомендації, які, за її словами, все ще актуальні. Barix тепер зазначає, що новіші моделі, такі як Exstreamer M400, постачаються з унікальними паролями за замовчуванням, і просуває свою послугу StreamGuys «Reflector» для безпечних AoIP-з'єднань, заохочуючи клієнтів звертатися до служби підтримки. Інженери в цілому рекомендують уникати прямих публічних IP-адрес і переадресації портів, використовуючи VPN-тунелі та списки контролю доступу, або, якщо VPN неможливі, тимчасово відкривати порти тільки за необхідності або ізолювати пристрої на приватних IP-адресах за допомогою ретрансляторів віддаленого доступу (наприклад, DWService, AnyDesk). Коментатори додають, що хоча виробники повинні розробляти продукти з урахуванням безпеки, більша частина провини лежить на мовниках, які продовжують ігнорувати основні найкращі практики…» ***(Elle Kehres. Apparent Barix Hacks Highlight Gaps in Cybersecurity // Future Publishing Limited (https://www.radioworld.com/news-and-business/apparent-barix-hacks-highlight-poor-cybersecurity-practices). 10.09.2025).***

***

«…Британське Управління з питань інформації (ICO) попереджає, що студенти, які діють зловмисно — часто заради виклику або слави — все частіше стають винуватцями кіберінцидентів у школах і коледжах, ризикуючи стати кіберзлочинцями. Проаналізувавши понад 200 повідомлень про порушення з боку інсайдерів за період з січня 2022 року по серпень 2024 року, ICO виявило, що 57% з них були спричинені студентами, а майже третина — викраденими логінами, за що студенти несуть відповідальність у 97% випадків… Попередження з'явилося на тлі загального занепокоєння щодо підліткових хакерських угруповань (наприклад, Scattered Spider/ShinyHunters/Lapsus$) та даних NCA, які показують, що кожен п'ятий підліток віком 10–16 років бере участь у незаконній діяльності в Інтернеті, а 5% 14-річних займаються хакерством, причому навіть семирічна дитина була направлена до програми Cyber Choices. Серед прикладів – учні 11 класу, які використовували інструменти для злому паролів, щоб отримати доступ до даних учнів, та студент, який використовував вкрадені облікові дані співробітників для перегляду, зміни або видалення конфіденційних записів (академічних, медичних, захисних та контактних даних). Основні причини виходять за межі дій учнів: близько чверті випадків були пов'язані з неналежними практиками персоналу (неприглянуті або спільні пристрої), п'ята частина — з

надсиланням даних на особисті пристрої, а близько 17 % — з технічними несправностями; лише 5 % випадків були пов'язані зі складними обхідними шляхами, що підкреслює необхідність дотримання основних правил гігієни. ICO закликає школи покращити безпеку та оновити навчання з питань GDPR і повідомлення про інциденти, а також радить батькам підтримувати відкритий діалог і розглянути ресурси NCA Cyber Choices для легального використання навичок…» ***(Alex Scroxton. Students an increasing source of cyber threat in UK schools // TechTarget, Inc. (https://www.computerweekly.com/news/366630564/Students-an-increasing-source-of-cyber-threat-in-UK-schools). 11.09.2025).***

***

«…Постачальник послуг з очищення DDoS-атак у Західній Європі зазнав масованої UDP-атаки з інтенсивністю 1,5 мільярда пакетів на секунду — однієї з найбільших зафіксованих атак за інтенсивністю пакетів — яка на короткий час загрожувала вивести його з ладу, але була заблокована автоматичною системою виявлення FastNetMon за лічені секунди. Ботнет використовував тисячі зламаних маршрутизаторів та пристроїв Інтернету речей у понад 11 000 мережах; FastNetMon підтвердив, що багато з викрадених маршрутизаторів були MikroTik… Компанія також зафіксувала майже ідентичну атаку потужністю 1,49 Гбіт/с на провайдера послуг очищення даних у Східній Європі, супроводжувану запискою з вимогою викупу, надісланою через веб-сайт жертви, що вказує на ту саму бот-мережу. На відміну від гучних атак із пропускною здатністю в терабіти на секунду, ця атака була зосереджена на швидкості передачі пакетів, яка може перевантажити обладнання для захисту ще до насичення каналів зв'язку… Засновник FastNetMon закликав інтернет-провайдерів фільтрувати шкідливий трафік ближче до джерела, щоб уникнути перетворення пристроїв їхніх клієнтів на «безкоштовну артилерію». Інцидент стався лише через кілька днів після того, як Cloudflare заявила, що відбила атаку потужністю 11,5 Тбіт/с, що свідчить про те, що зловмисники перевіряють як пропускну здатність, так і обмеження обробки пакетів…» ***(Carly Page. Anti-DDoS outfit walloped by record packet flood // The Register (https://www.theregister.com/2025/09/11/fastnetmon_ddos_attack/). 11.09.2025).***

***

«…ФБР опублікувало термінове попередження, в якому перелічено ознаки компрометації, пов'язані з двома фінансово мотивованими групами загроз, UNC6395 та UNC6040, після того, як обидві групи були викриті у викраденні даних з середовищ Salesforce компаній, а потім вимагали виплатити викуп за збереження їх конфіденційності…

UNC6395 використовував викрадені токени OAuth для інтеграції Salesloft Drift, порушення, яке було пов'язане з багатомісячним доступом зловмисників до репозиторіїв GitHub компанії Salesloft (березень–червень 2025 року). З того часу Salesloft ізолював інфраструктуру Drift, відключив чат-бота з штучним інтелектом, змінив облікові дані та попередив клієнтів, що будь-які дані або інтеграції,

пов'язані з Drift, можуть бути скомпрометовані, поки компанія впроваджує більш суворі заходи багатофакторної аутентифікації та захисту репозиторіїв…

UNC6040, активна з кінця 2024 року, віддає перевагу кампаніям голосового фішингу (vishing), щоб обдурити співробітників і змусити їх видати свої облікові дані, а потім використовує підроблений Salesforce Data Loader і спеціальні скрипти Python для виконання масових API-запитів і викрадення великих обсягів інформації. Подальші електронні листи та дзвінки з вимаганням викупу, часто підписані «ShinyHunters», здається, надходять від пов'язаної групи під назвою UNC6240. Google заявляє, що ці зловмисники можуть незабаром посилити тиск, запустивши публічний сайт з витоком даних…

Тим часом ShinyHunters, Scattered Spider і LAPSUS$ коротко оголосили про створення спільного бренду («scattered LAPSUS$ hunters 4.0»), але 12 вересня 2025 року заявили, що «заходять у тінь», що, на думку експертів, є тимчасовим кроком, спрямованим на уникнення уваги правоохоронних органів, а не справжнім виходом з бізнесу.

У своєму повідомленні ФБР закликає організації, особливо ті, що використовують Salesforce, переглянути опубліковані IoC, провести аудит OAuth-додатків, запровадити багатофакторну автентифікацію та ретельно контролювати використання API, наголошуючи, що зникнення групи зловмисників рідко означає, що небезпека зникла…» ***(Ravie Lakshmanan. FBI Warns of UNC6040 and UNC6395 Targeting Salesforce Platforms in Data Theft Attacks // The Hacker News (https://thehackernews.com/2025/09/fbi-warns-of-unc6040-and-unc6395.html). 13.09.2025).***

***

«…Атаки на основі доменів набувають все більшого поширення, оскільки зловмисники використовують системи доменних імен (DNS) та пов'язану інфраструктуру — шляхом викрадення доменів, типосквоттингу, гомографічних хитрощів, атаки на основі домену (DGA) та доменного фронтингу — для маскування під легітимний трафік, уникнення контролю та викрадення даних, а штучний інтелект зараз значно підвищує масштаб і точність таких атак, генеруючи та реєструючи тисячі схожих доменів за лічені хвилини… Недавні інциденти показують, що домени, створені за допомогою штучного інтелекту, сприяють поширенню фішингу та програм-вимагачів, що імітують бренди, у сферах фінансів, охорони здоров'я, виробництва та критичної інфраструктури, тоді як зловмисники поєднують маніпулювання доменами з методами грубої сили, відкритим RDP та векторами ланцюга постачання; неконтрольовані пристрої та системи управління, приховані за авторитетними доменами, погіршують прогалини у виявленні та збільшують витрати. Керівники служб інформаційної безпеки переглядають бюджети та стратегії щодо ризиків, пов'язаних зі штучним інтелектом, оскільки регуляторні органи впроваджують більш жорсткі заходи управління, такі як рекомендації США та режими у стилі ЄС, хоча їх виконання відстає від загрози, що спонукає до закликів перевищити мінімальні вимоги до відповідності розширення безпеки DNS (DNSSEC) С, оперативної інформації про загрози, партнерства з надійними реєстраторами та

підходів нульової довіри, які ретельно перевіряють усі доменні домени. Приклади з практики 2025 року підкреслюють операційні наслідки (наприклад, зупинка виробництва у виробника через типографічну помилку) та нові техніки, такі як клікджекінг розширень на основі DOM, тоді як галузеві звіти відносять доменні тактики до найпоширеніших типів атак і закликають до багаторівневого захисту, поведінкового аналізу та моніторингу за допомогою штучного інтелекту… У всьому світі державні суб'єкти використовують доменний фронтинг для атак на критично важливі сектори, а експерти попереджають, що штучний інтелект і майбутні квантові можливості, які сприяють кампаніям «збирай зараз, розшифровуй пізніше», ще більше ускладнять захист. Загальний консенсус: захист доменів повинен розглядатися як стратегічний міжгалузевий пріоритет; тільки поєднуючи передові інструменти, проактивне управління та спільну розвідку, організації можуть створити стійкість до цієї швидкозмінної загрози…» ***(Dorene Billings. Rising DNS Cyber Attacks: AI-Driven Threats Demand Zero-Trust Defenses // iEntry, Inc. (https://www.webpronews.com/rising-dns-cyber-attacks-ai-driven-threats-demand-zero-trust-defenses/). 13.09.2025).***

***

«…Лондонська юридична фірма HFW стверджує, що нігерійські організовані злочинні угруповання є найчастішими контрагентами у справах про кіберзлочини у сфері судноплавства, якими вона займається. Вони часто здійснюють високодохідні шахрайські операції типу «людина посередині», перехоплюючи електронні листи, викрадаючи облікові дані або фінансову інформацію та запускаючи програми-вимагачі, щоб захопити контроль над системами. HFW іноді веде переговори з ними за допомогою лаконічних щоденних повідомлень… Вразливість сектору швидко зростає: HFW повідомляє, що середня вартість усунення наслідків атаки подвоїлася до 550 000 доларів між 2022 і 2023 роками, а середній розмір викупу становить 3,2 мільйона доларів, коли усунення наслідків є складним. Згідно з даними Міжнародної палати судноплавства, близько 80% світової торгівлі здійснюється морським транспортом, тому судноплавство входить до топ-10 цілей для атак. Кількість інцидентів, зафіксованих університетом NHL Stenden, зросла з 10 у 2021 році до щонайменше 64 у 2023 році, причому багато з них пов'язані з державними структурами Росії, Китаю, Північної Кореї та Ірану. Зростаюча цифровізація та підключення до мережі — від поступової модернізації 22-річних суден до поширення супутникових зв'язків, таких як Starlink, — розширили площу атаки як для суден, так і для портів; з'явилися навіть несанкціоновані бортові інтернет-установки, а нові датчики викидів створюють додаткові точки входу. Окрім вимагання, глушіння та підробка GPS можуть фізично загрожувати суднам, як підозрюється у випадку з посадкою на мілину MSC Antonia в Червоному морі, а також повідомляється про інші випадки втручання в навігацію в Балтійському морі… Хоча технології протидії перешкодам існують, вони є дорогими, а застарілі системи обмежують можливість частих оновлень. Галузь посилює захист: з 2021 року Міжнародна морська організація вимагає управління кіберризиками в рамках систем управління безпекою суден, включаючи як IT-контроль, так і оперативний контроль. Експерти стверджують, що за останні

шість-сім років обізнаність і готовність значно покращилися, але поєднання кримінальних і підтримуваних державою загроз, а також оперативні та фінансові ризики, як і раніше, тримають судноплавство в центрі уваги кіберзлочинців…» ***(Emma Woollacott. Why hackers are targeting the world's shipping // BBC (https://www.bbc.com/news/articles/c36k01513l4o). 12.09.2025).***

***

«…Дослідники з Black Lotus Labs компанії Lumen попереджають, що кіберзлочинці переходять від викрадених домашніх пристроїв до скомпрометованих віртуальних приватних серверів (VPS) для створення великомасштабних проксі-ботнетів, прикладом чого є мережа «SystemBC», що існує вже давно. SystemBC, що діє з 2019 року, контролює понад 80 серверів управління та близько 1500 ботів щодня, з яких майже 80 % — це VPS-інстанції, що містять незахищені вразливості (кожен хост має в середньому 20 CVE, часто включаючи критичні)… Після зараження ці сервери з високою пропускною здатністю діють як ретрансляційні вузли, які направляють величезні обсяги фішингового, брут-форс, викрадацького та іншого шкідливого трафіку від імені злочинних проксі-сервісів, таких як REM Proxy або VN5Socks, які, в свою чергу, постачають такі угруповання, як AvosLocker і Morpheus. Підхід VPS пропонує зловмисникам більшу пропускну здатність, довшу стійкість (40 % вузлів залишаються скомпрометованими більше місяця) і мінімальні перебої в роботі користувачів, тому оператори навіть не турбуються про приховування: окремі боти щодня викачують гігабайти даних і швидко потрапляють до чорного списку, але залишаються корисними всередині проксі-мережі. Lumen заблокував трафік SystemBC на своїй магістралі та опублікував індикатори компрометації, щоб допомогти захисникам розірвати зв'язки з цією розширюваною інфраструктурою загроз, що працює на VPS…» ***(Sead Fadilpašić. VPS servers hijacked into malware proxies - here's how to stay safe // Future US, Inc. (https://www.techradar.com/pro/security/vps-servers-hijacked-into-malware-proxies-heres-how-to-stay-safe). 19.09.2025).***

***

«…Кібератаки, які колись здавалися притаманними лише великим підприємствам, тепер з однаковою жорстокістю вражають малі та середні підприємства і навіть місцеві органи влади. Guardz повідомляє, що щотижневі атаки на малі та середні підприємства майже подвоїлися в першій половині 2025 року, причому понад 80 % з них були спрямовані на викрадення облікових даних; легкодоступні набори «атака як послуга» в даркнеті дозволяють навіть початківцям-хакерам проводити ефективні кампанії з використанням програм-вимагачів та фішингу. Муніципалітети також наражаються на небезпеку: у липні місто Сент-Пол, штат Міннесота, зазнало скоординованої атаки типу «вимагання викупу», відповідальність за яку взяла на себе нова банда Interlock, змусивши чиновників відключити мережі, скинути облікові дані 3500 співробітників і викликати підрозділ кіберзахисту Національної гвардії. Незважаючи на витік 43 ГБ даних, місто відмовилося платити і відновлює послуги з незаражених резервних

копій, одночасно впроваджуючи більш широкі засоби безпеки. Неподалік, Академія політики Аспена все ще розслідує витік даних, спричинений фішингом, який підкреслює вразливість сектору — обмежені бюджети, застарілі системи, нечисленний персонал з кібербезпеки та величезні масиви даних громадян…

З огляду на те, що в першому кварталі кількість випадків використання програм-вимагачів для «хакерських атак і витоку інформації» зросла на 28 %, експерти попереджають, що жодна організація не є занадто малою, щоб стати мішенню. Вони закликають малі та середні підприємства та муніципалітети впроваджувати керовані платформи виявлення та реагування (часто через постачальників керованих послуг), проводити аудит інфраструктури, оновлювати системи, сегментувати мережі та розробляти чіткі плани реагування на інциденти. Довгострокова стійкість залежатиме від партнерства між державним і приватним секторами, більш гнучких закупівель, стипендій для залучення талановитих фахівців та участі в спільнотах з обміну інформацією, таких як Центри обміну та аналізу інформації (ISAC)…» ***(Jack M.*** *Germain.* ***Ransomware Wave Hits SMBs and Cities // ECT News Network, Inc. (https://www.technewsworld.com/story/ransomware-wave-hits-smbs-and-cities-179920.html). 19.09.2025).***

***

«Cloudflare оголосила, що самостійно нейтралізувала найбільшу розподілену атаку типу «відмова в обслуговуванні» (DDoS), яка коли-небудь фіксувалася.

Гіпероб'ємна атака досягла безпрецедентного піку в 22,2 терабіти на секунду (Tbps) і 10,6 мільярда пакетів на секунду (Bpps), встановивши новий і тривожний рекорд за масштабами кіберзагроз.

Ця атака більш ніж удвічі перевищує за розміром будь-яку раніше спостережувану DDoS-атаку, що свідчить про значне посилення можливостей зловмисників та ботнетів, якими вони керують…

Рекордна атака була примітна не тільки своїм масштабом, але й короткотривалістю. Вся подія тривала лише близько 40 секунд, що було тактикою, спрямованою на те, щоб перевантажити захист, не давши йому можливості повністю відреагувати…» ***(Guru Baran. 22.2 Tbps DDoS Attack Breaks Internet With New World Record // Cyber Security News (https://cybersecuritynews.com/ddos-attack-world-record/). 23.09.2025).***

***

«…Процес найму став новим критичним вектором атак, коли кіберзлочинці використовують генеративну штучну інтелігенцію та викрадені дані для створення синтетичних ідентичностей і проникнення в організації, навіть у команди безпеки. Уявіть, що ви наймаєте на роботу, здавалося б, кваліфікованого аналітика з безпеки, який має переконливе резюме, відповідні сертифікати, пройшов успішні відеоспівбесіди та перевірку анкетних даних. За кілька днів цей «працівник» отримує доступ до конфіденційних систем, таких як SIEM, привілейованих облікових даних та посібників з реагування на інциденти. Однак ця особа є фейком, а людина, яка за нею стоїть, — це зловмисник, який

незабаром починає викрадати конфіденційні дані журналів, вимикати сповіщення кінцевих точок та змінювати правила брандмауера, забезпечивши собі місце в першому ряду в центрі операцій з безпеки.

Цей сценарій далеко не гіпотетичний; компанія CrowdStrike нещодавно повідомила про понад 320 випадків шахрайства з дистанційною роботою з боку північнокорейських зловмисників, які використовують ШІ для проникнення в організації. На відміну від традиційного шахрайства при наймі на роботу, пов'язаного з підробкою резюме, ШІ тепер дозволяє шахраям легко створювати переконливі резюме, генерувати синтетичні особисті дані та використовувати відео з глибокою підробкою, щоб успішно пройти співбесіди. Для спеціалізованих посад, таких як кібербезпека, штучний інтелект може навіть допомогти підготувати та відпрацювати технічні відповіді, що дозволяє зловмисникам обійти технічні засоби захисту та діяти з таким самим законним доступом, як і довірений співробітник…

Вирішення цієї проблеми є складним через низку факторів. Практика найму персоналу в першу чергу дистанційно означає, що особиста перевірка особи є рідкістю. Зловмисники поєднують викрадені дані, такі як номери соціального страхування, з штучним інтелектом, щоб створити переконливі цифрові образи. Сучасні технології deepfake можуть імітувати міміку та голос, обманюючи навіть досвідчених інтерв'юерів. Крім того, статичні методи перевірки, такі як сканування документів, не можуть протистояти динамічному підробленню особи…

Щоб захиститися від цієї зростаючої загрози, організації повинні інтегрувати процес найму в цикл забезпечення безпеки ідентичності, поширюючи принципи нульової довіри на кожну взаємодію з кандидатами. Найкращі практики включають перевірку ідентичності при першому контакті за допомогою високонадійних перевірок та перевірок наживності під час співбесід, а також масштабування інтенсивності цих перевірок залежно від чутливості посади, особливо для привілейованих посад. Дуже важливо інтегрувати ці перевірки безпеки в робочі процеси відділу кадрів, щоб виявляти аномалії та постійно контролювати поведінку співробітників після першого дня роботи, виявляючи будь-які підозрілі моделі доступу після прийняття на роботу…» ***(Mike Engle. How hiring fraud has become a cybersecurity threat vector // Biometrics Research Group, Inc. (https://www.biometricupdate.com/202509/how-hiring-fraud-has-become-a-cybersecurity-threat-vector). 22.09.2025).***

***

«Генеральний прокурор Пенсільванії Дейв Сандей оголосив про кібератаку 18 серпня, детально описавши, як було зламано комп'ютерну мережу та сервери відомства, що призвело до відключення його веб-сайту, електронної пошти та телефонних послуг. Хоча багато послуг було поступово відновлено протягом наступних тижнів, атака спричинила значні затримки в роботі. Генеральна прокуратура, в якій працює близько 1200 осіб у 17 офісах, запросила початкову 30-денну паузу в усіх цивільних і кримінальних судових процесах у всьому штаті, посилаючись на неможливість співробітників отримати доступ до даних судових процесів, зв'язатися зі свідками або відповісти на судові

документи. Ця пауза була згодом продовжена в державному суді Філадельфії та у федеральному суді Східного округу Пенсільванії…

17 вересня офіс Сандея підтвердив, що не здійснював жодних виплат викупу і повідомив «декілька осіб», інформація про яких могла бути скомпрометована, хоча конкретні деталі про дані не були оприлюднені. Як офіс генерального прокурора, так і філадельфійське відділення ФБР відмовилися коментувати триваюче розслідування або конкретну участь Inc. Незважаючи на значні перебої в роботі, в тому числі вимушене використання деякими співробітниками «альтернативних каналів» для роботи, Сандей підтвердив відданість свого офісу місії захисту жителів Пенсільванії та висловив впевненість у їхніх зусиллях з відновлення роботи, пообіцявши надавати постійні оновлення щодо розслідування…» ***(Michael Tanenbaum. Global ransomware group claims responsibility for cyberattack on Pa. Attorney General's Office // WWB Holdings, LLC. (https://www.phillyvoice.com/pennsylvania-attorney-general-data-breach-ransomware-inc/). 23.09.2025).***

***

«…У квітні 2025 року британський роздрібний гігант Co-operative Group виявив спробу вторгнення в свою IT-мережу і, щоб її стримати, навмисно вимкнув значну частину своєї інфраструктури бек-офісу та кол-центру. Хоча магазини та служби доставки додому продовжували працювати в режимі онлайн, відключення поширилося на ланцюжок поставок та платіжні системи: полиці були порожніми протягом тижнів, і група в кінцевому підсумку попередила, що річний прибуток знизиться приблизно на 120 мільйонів фунтів стерлінгів, а дохід буде на 200 мільйонів фунтів стерлінгів нижчим за очікуваний. Цей епізод також викрив дорогу прогалину в стратегії управління ризиками Co-op. Компанія інвестувала значні кошти в превентивні заходи кібербезпеки та застрахувала себе на випадок необхідності негайного технічного реагування, але не мала спеціальної кіберполітики, що покривала б переривання бізнесу або операційні збитки. Як наслідок, більша частина фінансових збитків не буде відшкодована, що різко контрастує з такими компаніями, як Marks & Spencer, які розраховують відшкодувати значну частину своїх нещодавніх кіберзбитків за допомогою страхування…

Для американських компаній цей інцидент дає три чіткі уроки. По-перше, швидка ізоляція скомпрометованих систем і надійне планування безперебійної роботи можуть захистити послуги, що надаються клієнтам, та репутацію компанії. По-друге, кіберстрахування повинно доповнювати, а не замінювати, надійні засоби контролю безпеки і повинно охоплювати ризики переривання бізнесу та ланцюга поставок. По-третє, ради директорів та керівництво вищої ланки повинні розглядати кіберстійкість як питання балансу, зважуючи профілактичні витрати, готовність персоналу та комплексне страхування. У міру зростання масштабів та складності атак досвід Co-op нагадує, що залишення компонента кіберризику, пов'язаного з втратою доходів, фактично без страхування може обійтися набагато дорожче, ніж передбачають багато організацій…» ***(Steven Byerley. Major UK retailer's cyber breach offers lessons for US businesses // KM Business Information***

US, Inc (https://www.insurancebusinessmag.com/us/news/cyber/major-uk-retailers-cyber-breach-offers-lessons-for-us-businesses-551161.aspx). 26.09.2025).

***

«Кіберзлочинці використовують складні тактики, дешеві гаджети та психологічний тиск, щоб організувати шахрайство під виглядом «цифрового арешту», обманюючи жертв і змушуючи їх розлучитися зі своїми заощадженнями під приводом розслідування правоохоронних органів. Ці складні схеми зазвичай починаються з автоматизованих дзвінків з інтерактивною голосовою відповіддю (IVR), часто з робочим голосом, які видають себе за представників уряду або банків і неправдиво стверджують, що мобільний номер або банківський рахунок жертви пов'язані з відмиванням грошей. Ці дзвінки генеруються SIM-боксами — невеликими пристроями, що містять десятки SIM-карт, які маршрутизують інтернет-дзвінки VoIP через місцеві мобільні номери, надаючи миттєву достовірність іноземним абонентам. Ці SIM-карти часто активуються шахрайським шляхом за допомогою викрадених або дубльованих посвідчень особи, що забезпечує постійне постачання для злочинців…

Як тільки жертва відповідає, залякування посилюється. Шахраї переносять розмову на WhatsApp або Skype, де вони видають себе за «слідчих», часто одягнених у офіційну форму, і показують підроблені документи, такі як фальшиві ордери на арешт, повідомлення RBI або поліцейські посвідчення. Мета полягає в тому, щоб викликати паніку, погрожуючи негайним арештом, якщо жертва не погодиться переказати гроші для «перевірки» або «збереження». Вся ця операція, що нагадує невеликий call-центр, здійснюється за допомогою простих пристроїв, таких як маршрутизатори, модеми, ноутбуки та мобільні телефони, що дозволяє бандам щодня бомбардувати тисячі телефонів.

За цими шахрайськими схемами стоїть добре організована мережа: оператори в Південно-Східній Азії розробляють сценарії операцій і контролюють грошові потоки, місцеві рекрути управляють SIM-боксами, посередники постачають SIM-карти з підробленими даними KYC, а «грошові мули» переказують вкрадені кошти через кілька банківських рахунків або конвертують їх у криптовалюту, таку як USDT, щоб швидко затерти сліди. Ці шахрайські схеми процвітають завдяки використанню людської психології, поєднуючи авторитет правоохоронних органів із терміновістю загрози арешту, що переважає логіку жертв. Хоча особливо вразливими є люди похилого віку, поліція повідомляє, що жертвами стають також професіонали, студенти і навіть банківські працівники…

Зазвичай жертв просять переказати гроші на рахунки, які нібито «контролюються судом», звідки кошти швидко перекладаються, переказуються між різними банківськими рахунками, знімаються готівкою або конвертуються в криптовалюту, щоб уникнути заморожування.

П'ять основних ознак цифрової афери з арештом включають: автоматичні дзвінки, в яких стверджується про зв'язок з відмиванням грошей; дзвінки від осіб, які видають себе за чиновників (поліція, CBI, TRAI, банк) і вимагають «негайної співпраці»; перехід на відеодзвінки через WhatsApp/Skype з підробленими ордерами або посвідченнями; тиск з метою негайного переказу грошей для

«безпечного зберігання» або «перевірки»; а також погрози арештом або блокуванням рахунку в разі невиконання інструкцій. Влада наголошує, що жодна справжня влада ніколи не вимагатиме грошей по телефону або під час відеодзвінка…

Окрім цифрових арештів, кіберзлочинність проникла в повсякденне життя через різні інші хитрі способи дії, зокрема: «грошові пастки», які обманом змушують літніх громадян активувати переадресацію дзвінків для перехоплення одноразових паролів (OTP); «пастки зображень WhatsApp», які вбудовують шкідливий код за допомогою стеганографії для викрадення банківських реквізитів; «шахрайство з OLX та QR-кодами», коли шахраї обманом змушують жертв сканувати QR-коди, які вираховують гроші замість того, щоб їх отримувати; «шахрайство з використанням чужого імені», коли зловмисники зловживають назвами агентств, таких як CBI, щоб вимагати гроші за «вирішення справ»; «фальшиві пропозиції роботи», які спонукають шукачів роботи сплачувати реєстраційні внески; «шахрайство з акціями/інвестиціями», яке просуває фальшиві схеми з «гарантованою прибутковістю»; та «шахрайство з побаченнями та шлюбом», яке використовує емоції для отримання фінансових вимог.

Щоб убезпечити себе, люди ніколи не повинні ділитися одноразовими паролями (OTP) або банківськими реквізитами, уникати завантаження файлів або зображень від невідомих контактів, перевіряти QR-коди та облікові дані перед транзакціями, скептично ставитися до пропозицій, які здаються занадто хорошими, щоб бути правдою…» ***(Jagpreet Singh Sandhu. From SIM boxes to fake warrants: the hidden machinery of cybercrime rackets // The Indian Express [P] Ltd. (https://indianexpress.com/article/cities/chandigarh/sim-boxes-fake-warrants-cybercrime-rackets-10274449/). 27.09.2025).***

***

Діяльність хакерів та хакерські угруповування

«…Злочинне угруповання LunaLock скомпрометувало платформу для замовлення творів мистецтва Artists&Clients, відкрито погрожуючи продати вкрадений творчий контент компаніям зі штучного інтелекту для навчання моделей, якщо не буде сплачено викуп. Атака, що сталася близько 30 серпня, зашифрувала файли сайту і зробила доступними конфіденційні дані користувачів, включно з ілюстраціями, комунікаціями з клієнтами та платіжними реквізитами.

LunaLock вимагала викуп від $50 000 у біткоїнах або монетах Monero, обіцяючи розшифрувати файли та видалити дані після оплати. У разі відмови вони пообіцяли публічно оприлюднити дані - потенційно порушуючи правила GDPR в ЄС - і особливо підкреслили свій намір передати викрадені твори мистецтва фірмам, що займаються розробкою штучного інтелекту, для тренувальних наборів даних. Хоча спосіб передачі залишається незрозумілим, дослідниця безпеки Теммі Харпер зазначила, що це перший відомий випадок, коли зловмисники використовують навчання ШІ як важіль для вимагання…

Платформа, яка пропагує мистецтво, створене людиною, і прямо забороняє використання ШІ, наразі не працює в режимі офлайн. Її користувачі наразі стикаються зі значними ризиками для приватності, тоді як ширша творча спільнота, яка вже занепокоєна безоплатним використанням ШІ їхніх творів, може все частіше ставати мішенню таких загроз. Artists&Clients ще не зробила офіційної заяви щодо цього порушення…» ***(*Alfonso Maruccia.** Ransomware hackers threaten to feed stolen art to AI companies // TechSpot, Inc. (https://www.techspot.com/news/109337-ransomware-hackers-threaten-feed-stolen-art-ai-companies.html). 04.09.2025).***

***

«…Salesloft повідомила, що група UNC6395 протягом кількох місяців (березень–червень) таємно отримувала доступ до її облікового запису GitHub, а потім влітку провела кампанію, яка зачепила сотні компаній, зокрема Google, Zscaler, Cloudflare та Palo Alto Networks. Під час вторгнення зловмисники завантажили кілька репозиторіїв, додали гостьового користувача та налагодили робочі процеси, проводячи розвідку в середовищах додатків Salesloft та Drift… Пізніше вони отримали доступ до середовища AWS компанії Drift, отримали токени OAuth для інтеграції клієнтів і використовували їх для вилучення даних через ці інтеграції; серед розкритих секретів були ключі AWS, паролі, токени, пов'язані з Snowflake, та дані про продажі. Компанія Mandiant була залучена для розслідування першопричини, масштабів та локалізації інциденту, а також для перевірки сегментації між Salesloft і Drift; зараз вона заявляє, що інцидент локалізовано і переведено до етапу криміналістичної перевірки якості. Salesloft повідомляє, що вжито заходів для усунення наслідків, а інтеграція з Salesforce відновлена…» ***(Emma Woollacott. Salesloft Drift hackers had access to company GitHub account for months before attacks // Future US, Inc. (https://www.itpro.com/security/cyber-attacks/salesloft-drift-hackers-had-access-to-company-github-account-for-months-before-attacks). 09.09.2025).***

***

«Нещодавно виявлена хакерська група, яку дослідники кібербезпеки назвали «GhostRedirector», скомпрометувала щонайменше 65 серверів Windows по всьому світу, розгорнувши спеціальне шкідливе програмне забезпечення, призначене для маніпулювання результатами пошукових систем з метою отримання фінансової вигоди.

Згідно з новим звітом ESET, зловмисник використовує шкідливий модуль для служб Інтернет-інформації (IIS) компанії Microsoft для реалізації складної схеми SEO-шахрайства, що в першу чергу приносить користь веб-сайтам азартних ігор.

Атаки, які тривають щонайменше з серпня 2024 року, використовують два раніше недокументовані спеціальні інструменти: пасивний бекдор на C++ під назвою «Rungan» та шкідливий вбудований модуль IIS під назвою «Gamshen».

Хоча Rungan надає зловмисникам можливість виконувати команди на скомпрометованому сервері, Gamshen є ядром операції, розробленої для надання послуг з «SEO-шахрайства як послуги».

Дослідники пояснюють, що Gamshen функціонує, перехоплюючи веб-трафік на зараженому сервері. Модуль спеціально налаштований на активацію лише тоді, коли він виявляє запит від веб-сканера Google, Googlebot.

Для звичайних відвідувачів веб-сайт функціонує нормально. Однак, коли Googlebot сканує сайт, Gamshen змінює відповідь сервера, вводячи дані з власного сервера керування та контролю.

Ця техніка дозволяє зловмисникам створювати штучні зворотні посилання та використовувати інші маніпулятивні SEO-тактики, ефективно захоплюючи репутацію скомпрометованого веб-сайту для підвищення рейтингу сторінки цільового веб-сайту.

ESET вважає, що основними бенефіціарами цієї схеми є різні веб-сайти азартних ігор, орієнтовані на португаломовних користувачів. Дослідники ESET із середньою впевненістю пов'язують кампанію з раніше невідомим кітайським хакером…» ***(Guru Baran. GhostRedirector Hackers Compromise Windows Servers With Malicious IIS Module To Manipulate Search Results // Cyber Security News (https://cybersecuritynews.com/ghostredirector-hacks-windows-servers/). 04.09.2025).***

***

«З березня по червень 2025 року північнокорейська група Lazarus провела глобальну кампанію «Contagious Interview», в результаті якої щонайменше 230 (а ймовірно, і набагато більше) фахівців у галузі блокчейну були обмануті і заразили свої комп'ютери шкідливим програмним забезпеченням, замаскованим під матеріали для пошуку роботи. Видаючи себе за рекрутерів, хакери заманювали жертв (переважно фахівців з маркетингу та фінансів у криптографічних компаніях) на сайти для перевірки навичок, які відображали фальшиві помилки CAPTCHA; на цих сторінках жертвам пропонувалося скопіювати та вставити команди PowerShell «ClickFix», які встановлювали програми, призначені для викрадення облікових даних цифрових активів…

Неправильна конфігурація сервера розкрила журнали зловмисників і показала, наскільки професійно проводиться ця кампанія. Команди Lazarus співпрацюють у режимі реального часу через Slack, а потім відстежують вразливість власної інфраструктури за допомогою західних інструментів аналізу загроз, таких як Validin, VirusTotal і чорний список Maltrail, фактично перетворюючи ці сервіси на радари раннього попередження. Коли домен або файл позначається як небезпечний, оперативники відмовляються від нього і запускають нові сервери, замість того щоб переглядати систему безпеки — це цикл, що визначається квотами на доходи Пхеньяна. Незважаючи на цю недбалість OPSEC, тактика залишається ефективною: SentinelLabs відзначає 29-відсотковий рівень зараження серед користувачів, які перейшли за шкідливими посиланнями. Висновки компанії призвели до закриття фальшивих сайтів з працевлаштування, електронних поштових акаунтів, IP-адрес та хостів шкідливого програмного забезпечення, але аналітики попереджають, що Lazarus, ймовірно, вже відновлює свою інфраструктуру, щоб продовжувати збирати незаконну криптовалюту для санкціонованих програм озброєння Північної Кореї…» ***(Ernestas Naprys. Fake***

recruiters from North Korea plot attacks on Slack, abuse Western cyber intelligence // Cybernews (https://cybernews.com/security/fake-recruiters-from-north-korea-plot-attacks-on-slack/). 06.09.2025).

***

«…Іранська група кібершпигунів UNC1549 (відома також як Nimbus Manticore/Smoke Sandstorm) поширює нові бекдори та інфостілери, які мають цифровий підпис із законними сертифікатами SSL.com, що дозволяє шкідливому програмному забезпеченню обходити більшість антивірусних движків. Дослідники з Check Point і Prodaft виявили, що сертифікати були видані сумнівним голландським і шведським компаніям (Insight Digital B.V., RGC Digital AB, Sevenfeet Software AB), які, судячи з усього, є шахрайськими або підробленими; на мінімалістичних веб-сайтах цих компаній, які знаходяться «в стадії розробки», відсутні контактні дані — це тривожні ознаки, на які повинен звернути увагу сертифікаційний орган (CA). Оскільки код містить дійсні підписи, рівень виявлення був «значно» нижчим, і багато зразків залишаються невиявленими. SSL.com, сертифікаційний орган із Х'юстона, який брав участь у цьому процесі, не пояснив, як були видані сертифікати та чи були вони скасовані, незважаючи на правила CA/Browser Forum, які вимагають скасування протягом 24 годин після підтвердження зловживання…

Дослідники стверджують, що інші групи зловмисників також зловживають сертифікатами SSL.com; три з чотирьох сертифікатів, використаних у поточній кампанії, все ще є дійсними. Для захисту від підписаного шкідливого програмного забезпечення підприємствам слід враховувати індикатори компрометації, опубліковані Check Point, ретельно перевіряти метадані сертифікатів на наявність незвичайних пар «підписувач-ім'я файлу» та позначати бінарні файли з недавніми датами компіляції та підписання, які маскуються під відоме програмне забезпечення…» ***(Rob Wright. Iranian State Hackers Use SSL.com Certificates to Sign Malware // TechTarget, Inc. (https://www.darkreading.com/vulnerabilities-threats/iranian-hackers-ssl-certificates-sign-malware). 26.09.2025).***

***

«…компанія з кібербезпеки Recorded Future виявила зловмисника в липні 2024 року, відстежуючи його під назвою TAG100. На основі аналізу останніх дій і тактики групи, Recorded Future стверджує, що група, яку вона зараз відстежує під назвою RedNovember, «з великою ймовірністю є групою, що займається зловмисною діяльністю, спонсорованою китайською державою»…

У квітні, під час візиту міністра оборони США Піта Хегсета до Панами, RedNovember здійснила атаки на 30 панамських організацій. Аналогічно, хакерська діяльність групи була виявлена в грудні 2024 року, коли Китай проводив несподівані військові навчання навколо Тайваню.

Група використовує інфраструктуру шкідливого програмного забезпечення, пов'язану з іншою китайською групою, яку Google Mandiant відстежує під назвою UNC5266, що вказує на перетин інфраструктур шкідливого програмного

забезпечення. Китайські хакери зазвичай обмінюються тактиками та інструментами.

RedNovember також зосередився на компрометації периферійних пристроїв, які є поширеною ціллю для китайських та інших хакерів. Китайські хакерські угруповання, які Google Mandiant відстежує як UNC3886 та UNC4841, також віддають перевагу периферійним пристроям як шлюзу до корпоративних мереж.

З минулого року RedNovember зламала кілька периферійних пристроїв, зокрема Cisco Adaptive Security Appliance, F5 BIG-IP, Palo Alto Networks, Sophos SSL VPN і Fortinet. Крім того, вона націлилася на програмні платформи для комунікації та співпраці 3CX, Zimbra і Outlook Web Access.

Ця тактика також дозволила групі розширити свою діяльність на урядові та приватні організації, включаючи оборонні та аерокосмічні організації, космічні організації та юридичні фірми в США, Панамі, Азії та Європі…

Потрапивши в мережу, що була піддана злому, група поєднує експлойти для перевірки концепції з фреймворками Pantegana з відкритим кодом, що використовуються для пост-експлоатації та мають можливості обфускації. Група також використовує корисне навантаження Go під назвою Leslieloader, яке завантажує бекдор під назвою SparkRAT.

Варіанти Go сумісні з Windows, Linux та OSX. Вони підтримують завантаження та вивантаження файлів, зчитування системних відбитків та пряму взаємодію командного рядка із зараженими хостами.

Використання групою інструментів з відкритим кодом є яскравим прикладом того, як китайські державні хакери використовують «недорогі, масштабовані інструменти для досягнення високоцінного шпигунства»…» ***(Akshaya Asokan. New Chinese Espionage Hacking Group Uncovered // Information Security Media Group, Corp. (https://www.databreachtoday.com/new-chinese-espionage-hacking-group-uncovered-a-29569). 25.09.2025).***

***

«Дослідники з безпеки Group-IB повідомляють, що іранська група MuddyWater (також відома як Earth Vetala/Static Kitten/Mango Sandstorm) оновила свою стратегію. Група, пов'язана з Міністерством розвідки та безпеки Ірану, як і раніше, починає з фішингу, але відновила стару улюблену тактику — документи Microsoft Office з макросами Visual Basic — незважаючи на блокування за замовчуванням Microsoft у 2022 році. Коли одержувачі ігнорують попередження, макрос запускає бекдор Phoenix…

Ця зміна відбувається в той час, коли MuddyWater відмовляється від інсталяторів для віддаленого моніторингу та управління (Atera, ScreenConnect тощо), які масово використовувалися в 2023-24 роках. Натомість хакери покладаються на більш багатий арсенал власних інструментів: BugSleep (бекдор для передачі файлів), Phoenix injector, Fooder loader, Stealth Cache та безліч раніше розроблених інструментів, таких як PowerStats і MuddyC2Go.

Інфраструктура також була модернізована. Зараз група приховує вузли управління та контролю за Cloudflare, запускає їх лише на кілька днів і розміщує корисні дані на Amazon AWS або основних VPS-хостах (DigitalOcean, OVH, M247),

а також у «куленепробивних» постачальників, таких як Stark Industries, які ігнорують вимоги про видалення. Понад 300 пов'язаних доменів свідчать про значні ресурси…

Відродження макросів нагадує захисникам, що користувачі все ще можуть обійти засоби захисту Office; Group-IB радить повністю вимкнути непідписані макроси. Уряд США нещодавно повторно наголосив, що іранські зловмисники становлять дедалі більшу загрозу для критичної інфраструктури — про це свідчить оновлений, більш прихований набір інструментів MuddyWater та тактика маскування глобальної інфраструктури». ***(Mathew J. Schwartz. What's Old Is New Again as Iranian Hackers Exploit Macros // Information Security Media Group, Corp. (https://www.inforisktoday.com/whats-old-new-again-as-iranian-hackers-exploit-macros-a-29465). 17.06.2025).***

***

Вірусне та інше шкідливе програмне забезпечення

«…Хакери перетворили X Grok на мимовільний підсилювач у великій кампанії з розповсюдження шкідливого програмного забезпечення, використовуючи рекламну систему платформи за схемою, що отримала назву "Grokking". Дослідники з Guardio Labs (на чолі з Наті Тал) виявили 4 вересня, що зловмисники купують розкручену рекламу відеокарт і ховають шкідливі URL-адреси в неперевірених метаданих "From:", часто використовуючи сенсаційні або обмежені за віком приманки, щоб обійти модерацію; потім вони відповідають на власні оголошення і позначають Grok питаннями на кшталт "What’s the link?", спонукаючи довірений системний обліковий запис прочитати приховані метадані і опублікувати URL-адресу у відкритому доступі. Це поєднує платне охоплення з довірою до ШІ, що призводить до сотень тисяч і мільйонів показів і вразливості величезної кількості користувачів до сайтів зі шкідливим програмним забезпеченням. Ця тактика є частиною більш широкої хвилі кіберзлочинності з використанням ШІ: зловмисники відроджують інструменти в стилі WormGPT, обертаючи основні моделі, такі як Grok і Mixtral від Mistral, у зламані, "нецензуровані" інтерфейси, що продаються на таких форумах, як BreachForums, за кілька сотень євро, дозволяючи здійснювати фішинг, генерувати шкідливе програмне забезпечення і корисне навантаження, а також надаючи покрокові інструкції. Аналітики (наприклад, Cato Networks) підкреслюють, що основний ризик полягає в здатності зловмисників обійти засоби захисту за допомогою системних підказок і контексту розгортання, перетворюючи легітимні в інших випадках LLM на "помічників кіберзлочинців".» ***(Matt Gonzales. Cybercriminals ‘Grok’ Their Way Past X’s Defenses to Spread Malware // TechnologyAdvice (https://www.techrepublic.com/article/news-grok-ai-malware-grokking/). 05.09.2025).***

***

«…Дослідники з Інженерної школи Тандон при Нью-Йоркському університеті визнали, що створили шкідливе програмне забезпечення, відоме

під назвою "PromptLock", яке компанія ESET, що спеціалізується на кібербезпеці, раніше назвала першим відомим прикладом програм-вимагачів на основі штучного інтелекту в дикій природі. Код, написаний на мові Golang, використовує підказки для маніпулювання великою мовною моделлю (LLM) для автономного виконання етапів атаки зловмисників, включаючи розвідку, викрадення даних, шифрування та написання записок з вимогою викупу…

Минулого місяця шкідливе програмне забезпечення, завантажене до VirusTotal під час фінального тестування, виявила компанія ESET, яка спочатку вважала його незавершеним злочинним проектом. Пізніше дослідники з Нью-Йоркського університету підтвердили, що це була академічна перевірка концепції, розроблена для ілюстрації ризиків, що виникають на перетині ШІ та кібербезпеки. Проект під назвою "Ransomware 3.0" демонструє, як LLM можуть динамічно генерувати поліморфний шкідливий код, створюючи унікальні варіанти з кожним виконанням, що значно ускладнює його виявлення.

Фінансоване грантами Міністерства енергетики, Національного наукового фонду та нью-йоркської компанії Empire State Development, дослідження спрямоване на проактивне виявлення вразливостей у кіберзагрозах, що створюються за допомогою штучного інтелекту. Команда під керівництвом професора Рамеша Каррі та аспіранта Мд Раза навмисно приховала певні технічні артефакти (наприклад, специфічні підказки та поведінкові сценарії), щоб запобігти зловживанню з боку зловмисників.

Хоча ESET оновила свій аналіз, щоб відобразити академічне походження PromptLock, обидві організації погоджуються, що відкриття залишається важливим: це перший публічно задокументований випадок повністю замкнутого циклу, організованого LLM-шпигунським програмним забезпеченням з вимогою викупу. Цей інцидент прискорив ширший діалог про кіберзагрози, підсилені штучним інтелектом, і необхідність адаптивного захисту в умовах мінливого ландшафту загроз…» ***(Derek B. Johnson. NYU team behind AI-powered malware dubbed 'PromptLock' // CyberScoop (https://cyberscoop.com/ai-ransomware-promptlock-nyu-behind-code-discovered-by-security-researchers/). 05.09.2025).***

***

«Хакери поширюють шкідливі SVG-файли, які підробляють реальні веб-сайти, щоб обманом змусити жертв завантажувати шкідливі програми.

Дослідники з кібербезпеки VirusTotal виявили шкідливе програмне забезпечення після додавання підтримки SVG до своєї платформи Code Insight на базі штучного інтелекту.

Файли масштабованої векторної графіки (SVG) використовуються для відображення зображень, які залишаються чіткими за будь-якого розміру. Оскільки вони базуються на XML, вони можуть містити не лише фігури, а й скрипти та вбудований код, і зловмисники можуть скористатися цим, приховуючи шкідливий JavaScript або посилання всередині SVG. Файл може потім запускати завантаження з ходу, фішингові перенаправлення або виконання скриптів під час відкриття у браузері .

У цій кампанії файли SVG, відкриті в браузері, відображали веб-сайт судової системи Колумбії, що виглядав достовірно, а також фальшивий індикатор виконання завантаження. Після завершення «завантаження» користувачам пропонується зберегти на свої комп'ютери захищений паролем ZIP-архів.

Файли SVG, найімовірніше, поширюються через фішингові повідомлення, підробку електронного листа з судовим наказом або щось подібне.

«Фальшивий портал відображається точно так, як описано, імітуючи процес завантаження офіційного урядового документа», – йдеться у звіті VirusTotal. «Фішинговий сайт містить номери справ, токени безпеки та візуальні підказки для зміцнення довіри, і все це створено у файлі SVG».

Завантажений ZIP-архів нібито містив легітимний виконуваний файл з веб-браузера Comodo Dragon, перейменований, щоб виглядати як офіційний судовий документ, шкідливу DLL-бібліотеку та два зашифровані файли. Якщо жертва запускає браузер, вона активує DLL-бібліотеку, встановлюючи додаткове шкідливе програмне забезпечення в систему.

VirusTotal повідомив, що наразі виявила понад 500 SVG-файлів, які були частиною тієї ж кампанії, але залишилися поза увагою антивірусних рішень та інших платформ захисту кінцевих точок.

Нам небагато відомо про жертв, окрім того, що вони, найімовірніше, колумбійці…»
(Sead Fadilpašić. Hackers are sneaking malware into SVG images to bypass antivirus - here's what we know // Future US, Inc. (https://www.techradar.com/pro/security/hackers-are-sneaking-malware-into-svg-images-to-bypass-antivirus-heres-what-we-know). 08.09.2025).

***

«…Компанія Trend Micro повідомляє про нову кампанію Atomic macOS Stealer (AMOS), яка маскує шкідливе програмне забезпечення під «зламані» програми, щоб обійти останні вдосконалення безпеки Apple. Це знаменує собою значну тактичну зміну від традиційних інфекцій .dmg, які зараз в основному блокуються вдосконаленим Gatekeeper macOS Sequoia, до методів інсталяції на основі терміналу, що реалізуються за допомогою соціальної інженерії. Користувачі, які шукають піратське програмне забезпечення (зокрема «CleanMyMac») на таких сайтах, як haxmac[.]cc, перенаправляються на цільові сторінки AMOS, які визначають операційну систему і або подають шкідливий .dmg, або дають жертвам вказівку скопіювати і вставити команди в термінал (підроблена приманка у стилі CAPTCHA). Інфраструктура використовує обертові домени, URL-адреси та перенаправлення, щоб уникнути статичного виявлення, зберігаючи при цьому узгодженість інструкцій. Виконання запускає скрипт, який завантажує «оновлення» AppleScript у тимчасовий каталог і встановлює LaunchDaemon (com.finder.helper.plist) для безперервного виконання прихованого процесу .agent, забезпечуючи стійкість шляхом ідентифікації поточного користувача, що не є root, а потім викрадаючи конфіденційні дані, включаючи облікові дані, дані браузера, криптогаманці, чати Telegram, профілі VPN, елементи ключової ланцюжка, Apple Notes та файли із загальних папок…

Опубліковане 4 вересня дослідження попереджає, що викрадені дані можуть призвести до крадіжки облікових даних, фінансових збитків та більш серйозних вторгнень у підприємства, закликаючи до застосування комплексних стратегій захисту, які не покладаються виключно на вбудовані засоби захисту macOS…» ***(James Coker. macOS Stealer Campaign Uses "Cracked" App Lures to Bypass Apple Security // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news/macos-stealer-cracked-apps-bypass/). 05.09.2025).***

***

«У новому звіті, опублікованому сьогодні провайдером послуг безпечного доступу Aryaka Networks Inc., міститься попередження про зростаючу загрозу від Vidar, шкідливого програмного забезпечення як послуги для викрадення інформації, яке набуло популярності після першої появи в 2018 році.

Vidar з'явився на сцені шкідливого програмного забезпечення як похідний продукт від сімейства шкідливого програмного забезпечення Arkei, а сьогодні перетворився на більш потужну, самостійну платформу з модульною архітектурою та підтримкою плагінів. У звіті зазначається, що його зростаюча популярність у кіберзлочинному співтоваристві в 2025 році пояснюється простотою розгортання, що дозволяє навіть малокваліфікованим зловмисникам здійснювати крадіжки облікових даних та викрадення даних як у приватних осіб, так і в підприємств.

Він поширюється переважно через фішингові електронні листи, випадкові завантаження та шкідливі рекламні кампанії, замасковані під легітимні оновлення програмного забезпечення. Ці кампанії навмисно розроблені таким чином, щоб зливатися з повсякденною взаємодією та, таким чином, обманювати користувачів.

Після розгортання Vidar збирає широкий спектр даних, включаючи файли cookie браузера, облікові дані та дані кредитних карток для криптовалютних гаманців, дані додатків двофакторної автентифікації та токени автентифікації з месенджерів та ігрових платформ.

Vidar працює на базі скрипта PowerShell, який може красти дані з віддаленого сервера за допомогою прихованих методів, таких як рандомізовані імена файлів та підроблені агенти користувачів. Скрипт також вимикає інтерфейс сканування антивірусного програмного забезпечення Microsoft, встановлює виключення Захисника Windows та створює заплановані завдання для забезпечення збереження даних.

Після запуску Vidar впроваджує код у довірені процеси, такі як msbuild.exe, та захоплює інтерфейс прикладного програмування CryptProtectMemory для перехоплення конфіденційних даних браузера перед шифруванням. Інфраструктура командування та управління динамічно витягується за допомогою методу пошуку мертвих даних, який використовує профілі Telegram та Steam, що ще більше ускладнює виявлення.

Дослідники Aryaka зазначають, що багаторівневий підхід Vidar, який включає обхід інтерфейсу сканування антивірусного програмного забезпечення, ін'єкцію процесів, перехоплення API та витік даних із шифруванням Transport Layer Security, дозволяє йому обходити як захист на основі сигнатур, так і захист на

основі поведінки. До того ж, він має здатність перехоплювати облікові дані перед шифруванням, а також динамічно приховувати інфраструктуру, що підвищує його стійкість і робить його серйозним інструментом для фінансово мотивованих кіберзлочинів.

У звіті рекомендується, щоб для захисту від шкідливого програмного забезпечення, такого як Vidar, підприємствам впроваджували багаторівневу стратегію захисту. В ідеалі, вона включає безпечне розгортання граничних служб доступу з кількома контрольними точками, включаючи DNS-фільтрацію, безпечні веб-шлюзи, брандмауери з урахуванням додатків, засоби виявлення вторгнень та контроль кінцевих точок». ***(Duncan Riley. Vidar infostealer gains traction among cybercriminals as ease of use drives adoption // SiliconANGLE Media Inc. (https://siliconangle.com/2025/09/04/vidar-infostealer-gains-traction-among-cybercriminals-ease-use-drives-adoption/). 04.09.2025).***

***

«Новий бекдор для Outlook, який приписують пов'язаній з Росією групі APT28, завдав шкоди багатьом компаніям у різних вертикальних секторах країн НАТО.

Бекдор, який отримав назву «NotDoor» через слово «Nothing» у коді, працює як макрос VBA для Outlook, призначений для моніторингу вхідних електронних листів на наявність певного слова-тригера.

Коли один із листів виявляється шкідливим кодом, він дозволяє зловмиснику викрасти дані, завантажити файли та виконати команди на комп'ютері жертви, згідно з повідомленням від 3 вересня в блозі LAB52, розвідувальної команди S2 Grupo.

«Цей [випадок] підкреслює постійну еволюцію APT28, демонструючи, як вона постійно генерує нові артефакти, здатні обходити встановлені механізми захисту», — написали дослідники LAB52…» ***(Steve Zurier. 'NotDoor' malware tied to Russia's APT28 exploits Microsoft Outlook // CyberRisk Alliance (https://www.scworld.com/news/notdoor-malware-tied-to-russias-apt28-exploits-microsoft-outlook). 05.09.2025).***

***

«З березня 2025 року на сцену вийшов висококваліфікований зловмисник під псевдонімом TAG-150, який випустив три самостійно створені сімейства шкідливого програмного забезпечення — CastleLoader, CastleBot і нещодавно виявлений CastleRAT — і поєднав їх із витонченими приманками соціальної інженерії. Зараження починається з електронних листів «ClickFix», що імітують квитки Cloudflare, або з підроблених репозиторіїв GitHub; жертв обманом змушують вставляти команди PowerShell, тому компрометація виглядає як самоініційована і проходить повз багато засобів контролю. Хоча лише деякі цілі реагують на це, майже третина (28,7 %) тих, хто натискає на посилання, успішно заражаються, що свідчить про досконалість фішингових методів TAG-150…

TAG-150 використовує чотирирівневу архітектуру управління та контролю: сервери рівня 1 доставляють шкідливе програмне забезпечення, хости рівня 2 RDP

передають трафік, а вузли рівня 3 і 4 обробляють управління та резервне копіювання — така організація демонструє як оперативну досконаліть, так і вбудовану надмірність. Початкові дропери направляють жертв у широку екосистему шкідливого програмного забезпечення — SectopRAT, WarmCookie, HijackLoader, NetSupport RAT і крадіїв, таких як Stealc, RedLine і Rhadamanthys, — що свідчить про бізнес «шкідливе програмне забезпечення як послуга» або тісні союзи з іншими угрупованнями…

CastleRAT, флагманський корисний вантаж, доступний у версіях Python і C, які спілкуються за допомогою спеціального протоколу з шифруванням RC4 і запитують ip-api.com для геопозиціонування хостів. Версія C додає функцію запису клавіш, зняття знімків екрана, крадіжки вмісту буфера обміну та розширеного введення процесів, а останні оновлення приховують C2 «deaddrops» на сторінках спільноти Steam, щоб злитися з трафіком геймерів. Стійкість досягається за допомогою налаштувань реєстру та маскування процесів браузера; варіант Python може самостійно видалити себе за допомогою команди PowerShell. TAG-150 також запускає корисні навантаження через служби проти виявлення, такі як Kleenscan, підкреслюючи свою орієнтацію на прихованість та стійкість…» ***(Tushar Subhra Dutta. TAG-150 Hackers Deploying Self-Developed Malware Families to Attack Organizations // Cyber Security News (https://cybersecuritynews.com/tag-150-hackers-deploying-self-developed-malware/). 05.09.2025).***

***

«…Сполучені Штати стали провідним фінансистом комерційного шпигунського програмного забезпечення, випередивши традиційні центри в Європі, оскільки американський венчурний капітал вкладає мільярди в компанії, що розробляють інструменти, здатні проникати в пристрої без згоди користувачів. Під впливом геополітичної напруженості та сприйняття шпигунського програмного забезпечення як сектора з високим рівнем зростання, подібного до штучного інтелекту та хмарних обчислень, інвестиції США різко зросли в 2024 році, перевищивши 50 угод на загальну суму понад 2 мільярди доларів. Атлантична рада попереджає, що цей бум становить загрозу національній безпеці та правам людини, оскільки продукти, що підтримуються США, пов'язані з несанкціонованим стеженням за журналістами, активістами та чиновниками, а нові користувачі в Південно-Східній Азії та Латинській Америці розширюють ринок, який раніше домінували ізраїльські компанії, такі як NSO Group. Швидкі інновації, такі як експлойти для смартфонів без кліків, процвітали в умовах слабкого нагляду, тоді як політика залишається непослідовною: указ 2023 року обмежує використання таких інструментів на федеральному рівні, але приватні інвестиції в основному не регулюються, що створює лазівку, яка може сприяти іноземному шпигунству та репресіям. Хоча деякі інвестори обіцяють стриманість, суперечності залишаються, що спонукає до закликів щодо посилення експортного контролю, вимог прозорості та розкриття інформації про фінансування, пов'язане зі шпигунським програмним забезпеченням. Мережі, такі як Intellexa Consortium, підкреслюють ризики розповсюдження, а інвестори стикаються з ризиком втрати репутації та потенційним внесенням до чорного списку. Без втручання домінування

США може посилитися, а ринок роздвоїтися, що змусить політиків і фінансистів прийняти більш відповідальну модель, яка поєднує інновації з безпекою та громадянськими свободами…» ***(Maya Perez. US Tops Global Spyware Investment with Billions Amid Security Risks // iEntry, Inc. (https://www.webpronews.com/us-tops-global-spyware-investment-with-billions-amid-security-risks/). 12.09.2025).***

***

«Складне шкідливе програмне забезпечення з бекдором, відоме як Backdoor.WIN32.Buterat, стало значною загрозою для корпоративних мереж, демонструючи передові методи збереження та прихованості, що дозволяють зловмисникам підтримувати тривалий несанкціонований доступ до скомпрометованих систем.

Шкідливе програмне забезпечення було виявлено та спрямоване на урядові та корпоративні середовища через ретельно сплановані фішингові кампанії, шкідливі вкладення електронної пошти та завантаження троянського програмного забезпечення.

На відміну від традиційного шкідливого програмного забезпечення, орієнтованого на негайну шкоду або вилучення даних, Buterat надає пріоритет довговічності та прихованим операціям.

Бекдор встановлює зашифровані канали зв'язку з віддаленими серверами командного управління, дозволяючи зловмисникам виконувати довільні команди, розгортати додаткові корисні навантаження та переміщатися по мережевій інфраструктурі, уникаючи традиційних механізмів виявлення…» ***(Tushar Subhra Dutta. Buterat Backdoor Attacking Enterprises to Establish Persistence and Control Endpoints // Cyber Security News (https://cybersecuritynews.com/buterat-backdoor-attacking-enterprises/). 13.03.2025).***

***

«З'явилася складна кампанія шкідливої реклами, яка використовує репозиторії GitHub через завислі коміти для розповсюдження шкідливого програмного забезпечення через підроблені клієнти GitHub Desktop.

Цей новий вектор атаки являє собою значну еволюцію в тактиці кіберзлочинців, використовуючи довіру та легітимність, пов'язані з платформою GitHub, щоб обманом змусити нічого не підозрюючих користувачів завантажити шкідливе програмне забезпечення.

Кампанія працює шляхом просування скомпрометованих репозиторіїв GitHub, що містять завислі коміти, що служать механізмами доставки корисних даних шкідливого програмного забезпечення.

Коли користувачі шукають GitHub Desktop через скомпрометовану рекламу, їх перенаправляє до шкідливих репозиторіїв, які виглядають легітимними, але містять приховане шкідливе програмне забезпечення, вбудоване в структуру репозиторію.

Атака використовує знайомство користувачів з інтерфейсом GitHub та їхню довіру до безпеки платформи.

Після успішного зараження шкідливе програмне забезпечення встановлює стійкість на системах жертви, підтримуючи приховані канали зв'язку з серверами командного та контрольного зв'язку.

Дослідники Unit 42 виявили цю кампанію за допомогою поведінкового аналізу підозрілої активності репозиторію GitHub та аномальних моделей завантаження, пов'язаних з підробленими інсталяторами GitHub Desktop…» ***(Tushar Subhra Dutta. New Malvertising Campaign Leverages GitHub Repository to Deliver Malware // Cyber Security News (https://cybersecuritynews.com/new-malvertising-campaign/). 13.09.2025).***

***

«…Через рік після того, як програмна помилка CrowdStrike спричинила глобальний збій комп'ютерних систем, компанія знову стала центром уваги через серйозний інцидент із безпекою — цього разу пов'язаний із самовідтворювальним черв'яком у ланцюжку поставок під назвою «Shai-Hulud». Вперше виявлене журналістом Браяном Кребсом, шкідливе програмне забезпечення проникло приблизно в 25 пакетів, що підтримуються CrowdStrike, у широко використовуваному репозиторії Node Package Manager (NPM) і на даний момент зачепило щонайменше 187 модулів. Shai-Hulud встановлюється, коли розробник несвідомо завантажує інфікований пакет NPM, збирає токени доступу NPM жертви, а потім автоматично інфікує 20 найпопулярніших пакетів, пов'язаних з обліковим записом цього розробника, створюючи каскадний ланцюжок компрометації. Повноваження, викрадені з кожного нового хоста, публікуються у відкритому файлі GitHub, що носить наукову фантастичну назву черв'яка — це відсилання до гігантських піщаних черв'яків у романі Френка Герберта «Дюна». Шкідливе програмне забезпечення націлене на середовища Linux і macOS, навмисно оминаючи комп'ютери з Windows. NPM і CrowdStrike видалили заражені пакети та змінили ключі доступу, що сповільнило, але не усунуло загрозу. Дослідники попереджають, що черв'як може перебувати в стані спокою і знову активуватися, якщо навіть один розробник-«суперрозповсюджувач» буде заражений повторно…» ***(Joe Wilkins. CrowdStrike Infested With "Self-Replicating Worms" // Recurrent (https://futurism.com/crowdstrike-infested-self-replicating-worms). 16.09.2025).***

***

«Дослідники в галузі безпеки та федеральні агентства попереджають, що сучасні ботнети переросли свою традиційну роль інструментів для виведення окремих веб-сайтів з ладу і тепер становлять системну загрозу для самої основи Інтернету. На відміну від попередніх мереж, побудованих на базі маршрутизаторів та веб-камер з низькою потужністю, найновіші армії ботів захоплюють пристрої з високою пропускною здатністю — Android TV-приставки, сервери, навіть корпоративне обладнання — надаючи злочинцям безпрецедентну потужність. Небезпека була підкреслена після того, як американські власті ліквідували ботнет, яким керував 22-річний житель Орегону: після вилучення командних серверів конкурентні угруповання швидко захопили 95 000 все ще

інфікованих комп'ютерів. Одна з відокремлених груп, названа Aisuru, незабаром створила рекордний розподілений відмову в обслуговуванні з швидкістю 11,5 терабіт на секунду — це достатній трафік, щоб перевантажити сукупну пропускну здатність понад 50 000 домашніх інтернет-підключень…

Cloudflare, Google, Nokia Deepfield і Lumen's Black Lotus Labs зараз відстежують ботнети, що налічують мільйони або навіть десятки мільйонів вузлів. Нещодавно Google деактивував шахрайську мережу, яка розрослася з 74 000 Android TV-приставок у 2023 році до понад 10 мільйонів цього року; Nokia виявила інший кластер, «ResHydra», порівнянного розміру. Аналітики побоюються, що такі рої можуть бути перенаправлені з шахрайства з кліками на рекламу або дрібного вимагання до стратегічних зривів, що за лічені хвилини можуть паралізувати фінансові мережі або національну мережу зв'язку. «Раніше проблема стосувалася веб-сайтів, а тепер — країн», — каже Крейг Лабовіц із Nokia. Короткі, але масштабні тестові атаки свідчать про те, що оператори оцінюють свої можливості для майбутніх, більш руйнівних кампаній, що викликає нагальні питання про те, чи зможуть хмарні провайдери та магістральні оператори зв'язку й надалі витримувати удари, і чи не сприяють швидкі відключення без усунення несправностей пристроїв лише появі наступної, ще сильнішої хвилі атак…» ***(*Skye Jacobs. *The rise of mega botnets weaponizing hacked devices for internet-scale attacks // TechSpot, Inc. (https://www.techspot.com/news/109515-rise-mega-botnets-weaponizing-hacked-devices-internet-scale.html). 18.09.2025).***

***

«…**Зловмисники створюють шахрайські репозиторії, що імітують відомі бренди — спочатку LastPass, а також 1Password, Robinhood, Citibank, Docker, Shopify, Basecamp та інші — щоб заманити жертв, які шукають в Інтернеті інсталятори для Mac.** Коли користувачі натискають посилання «Встановити на MacBook», їх перенаправляють через кілька підроблених сайтів і, зрештою, просять ввести команду в терміналі. Ця команда непомітно завантажує та виконує скрипт, закодований у base64, який завантажує файл «оновлення», що встановлює Atomic Stealer (AMOS) — програму для викрадення інформації, яка діє з 2023 року. Після встановлення AMOS збирає паролі, дані браузера та криптовалютні гаманці…

Шахраї змінюють імена користувачів GitHub і використовують оптимізацію пошукових систем, щоб їхні шкідливі сторінки з'являлися у верхній частині результатів пошуку Google і Bing. Хоча GitHub видаляє репозиторії після отримання повідомлення про них, зловмисники швидко повертаються під новими псевдонімами, що підкреслює складність контролю відкритих хостингових платформ.

Команда Threat Intelligence компанії LastPass стежить за операцією, координує видалення та обмінюється показниками компрометації. Тим часом експерти радять користувачам Mac завантажувати програмне забезпечення тільки з перевірених сайтів постачальників або з Mac App Store, уникати виконання команд, скопійованих з невідомих веб-сторінок, підтримувати macOS і додатки в актуальному стані, використовувати надійні засоби безпеки з захистом від програм-вимагачів, вмикати регулярне резервне копіювання, бути обережними з

небажаними посиланнями або спливаючими вікнами, дотримуватися офіційних рекомендацій постачальників і захищати важливі облікові записи за допомогою надійних паролів і двофакторної автентифікації…» ***(Efosa Udinmwen. Are you an Apple Mac user? Cybercriminals are using this popular website to target you with malware and infostealers - here's what you need to stay safe // Future US, Inc. (https://www.techradar.com/pro/security/are-you-an-apple-mac-user-cybercriminals-are-using-this-popular-website-to-target-you-with-malware-and-infostealers-heres-what-you-need-to-stay-safe). 24.09.2025).***

***

«Дослідники виявили першу в природі атаку «FileFix» — техніку соціальної інженерії, яка зловживає діалоговим вікном завантаження HTML-файлів замість командного рядка, щоб змусити користувачів запускати команди PowerShell, вставлені в адресний рядок Провідника Windows. Операція використовує багатомовні фішингові сайти, які імітують сторінки безпеки Facebook/Meta 16 мовами, попереджаючи жертв, що їхні облікові записи будуть заблоковані, якщо вони не відкриють фальшивий «звіт про інцидент». Виконання інструкцій відкриває локальний шлях до файлу, який непомітно запускає шкідливу команду…

Ця команда завантажує зображення JPG із пасторальним виглядом із Bitbucket. Використовуючи стеганографію, зловмисники приховали скрипт PowerShell другого рівня та виконуваний файл, зашифрований за допомогою RC4, у певних діапазонах байтів зображення. Початковий скрипт (сильно заплутаний і закодований Base64 для уникнення виявлення) витягує прихований код, розшифровує і розпаковує його, а потім запускає завантажувач на базі Go з анти-VM-перевірками і шифруванням рядків. На останньому етапі встановлюється StealC, програма для викрадення інформації, яка збирає паролі браузерів, криптогаманці, дані Discord/Telegram, конфігурації VPN та ключі AWS/Azure, а також підтримує стійкість для продовження викрадення даних…

Компанія Acronis, яка проаналізувала цю кампанію, стверджує, що інфраструктура охоплює подані матеріали зі США, Бангладеш, Німеччини, Китаю та кількох інших країн, що вказує на скоординовану глобальну операцію. Використання зловмисниками стеганографії, багатоступеневих корисних навантажень, широкого заплутування та багатомовних фішингових приманок свідчить про значну еволюцію порівняно з попередніми концептуальними доказами ClickFix і розширює коло потенційних жертв до будь-кого, хто може завантажити файл, без необхідності володіння навичками роботи з командним рядком». ***(Tushar Subhra Dutta. New Innovative FileFix Attack in The Wild Leverages Steganography to Deliver StealC Malware // Cyber Security News (https://cybersecuritynews.com/new-innovative-filefix-attack-in-the-wild/). 17.09.2025).***

***

«…Дослідники виявили масштабну операцію з рекламного шахрайства в Google Play під назвою «SlopAds», в якій брали участь 224 шкідливі програми з понад 38 мільйонами завантажень, що генерували до 2,3 мільярда рекламних

запитів на день. Хоча рекламне шахрайство в першу чергу виснажує рекламодавців, завищуючи кількість переглядів, постраждалі користувачі також страждають від уповільнення роботи, оскільки програми виконують приховані дії у фоновому режимі. Щоб уникнути перевірки, програми працюють нормально, якщо їх встановити безпосередньо з Play Store; однак, якщо установка запускається через рекламу кампанії, програма завантажує зашифрований стеганографічно корисний вантаж: чотири зображення у форматі PNG, які розшифровуються і збираються в APK. Цей шкідливий модуль використовує WebView для збору даних про пристрій і браузер і зв'язується з C2 на ad2[.]cc, який потім направляє приховані WebViews для відвідування певних доменів. Слідчі також виявили докази навчання інструменту штучного інтелекту на тому самому домені та ідентифікували понад 300 пов'язаних доменів, що просувають відповідні програми, що свідчить про те, що відомі 224 програми є лише частиною загального масиву. Google видалив виявлені програми та заявляє, що Play Protect тепер блокує поведінку, схожу на SlopAds, під час інсталяції, навіть для програм, завантажених з інших джерел…

Оскільки шкідливі програми все ще можуть проникати в офіційні магазини, користувачам слід перевіряти дозволи (та зміни після оновлень), періодично видаляти невикористовувані програми, оновлювати пристрої та ключові програми, використовувати надійні засоби мобільної безпеки та перевіряти легітимність розробника перед завантаженням схожих програм (наприклад, підтвердити, що OpenAI є розробником ChatGPT для Android)». ***(Pieter Arntz. 224 malicious apps removed from the Google Play Store after ad fraud campaign discovered // Malwarebytes (https://www.malwarebytes.com/blog/news/2025/09/224-malicious-apps-removed-from-the-google-play-store-after-ad-fraud-campaign-discovered). 17.09.2025).***

***

«Вірус «Троянський кінь» є однією з найтриваліших загроз кібербезпеці. Він отримав свою назву від давньогрецького міфу, в якому солдати сховалися всередині дерев'яного коня, щоб проникнути в Трою. Як і його міфологічний тезка, троянське шкідливе програмне забезпечення обманює користувачів, маскуючись під легальне програмне забезпечення — нешкідливий PDF-файл, оновлення програмного забезпечення або безкоштовну програму — щоб отримати доступ до систем. Після запуску ці шкідливі програми можуть викрадати конфіденційну інформацію, включаючи паролі та банківські реквізити, створювати «задні двері» для віддаленого контролю, встановлювати додаткове шкідливе програмне забезпечення, таке як програми-вимагачі або шпигунські програми, а також вимикати засоби безпеки, змінюючи або видаляючи файли….

Історія троянських вірусів налічує кілька десятиліть, починаючи з ранніх тестових програм 1970-х і 1980-х років, які демонстрували, як програмне забезпечення може виглядати легітимним, виконуючи шкідливі дії. Троянський вірус AIDS 1989 року став однією з перших широкомасштабних атак, поширюваною на дискетах під виглядом програмного забезпечення для медичних досліджень, але насправді шифрував файли і вимагав оплату. З розширенням Інтернету в 1990-х роках трояни швидко поширювалися через вкладення в

електронні листи та піратське програмне забезпечення. У 2000-х роках з'явилися складні банківські трояни, такі як Zeus, які масово викрадали фінансові дані, а в 2010-х роках з'явилися модульні завантажувачі шкідливого програмного забезпечення, такі як Emotet і Dridex, які часто слугують механізмами доставки програм-вимагачів і складних постійних загроз.

Троянські програми діють за допомогою багатоетапного процесу, що починається з доставки через фішингові електронні листи, шкідливі веб-сайти, пакетне програмне забезпечення, соціальну інженерію або скомпрометовані оновлення. На відміну від самореплікуючих вірусів або черв'яків, троянські програми вимагають дій користувача для виконання, будь то запуск виконуваного файлу, увімкнення макросів у документі або виконання скриптових корисних навантажень. Після активації вони забезпечують стійкість за допомогою модифікацій реєстру, запланованих завдань або руткіт-технік, щоб вижити після перезавантаження системи. Більшість троянських програм потім встановлюють канали управління та контролю для зв'язку з зловмисниками, що дозволяє здійснювати дистанційне керування, викрадення даних та розгортання додаткових корисних навантажень. Їхні зловмисні дії дуже різноманітні: від отримання доступу через «задні двері» і крадіжки облікових даних до кейлоггінгу, вербування ботнетів і горизонтального переміщення по мережах з використанням викрадених облікових даних і інструментів, що використовують наявні ресурси…

До поширених типів троянських програм належать варіанти з функцією віддаленого управління, банківські трояни, що націлені на фінансові дані, трояни-завантажувачі, які встановлюють додаткове шкідливе програмне забезпечення, шпигунські трояни, що записують дії користувача, трояни-руткіти, які приховують шкідливі процеси, підроблені антивірусні програми, трояни DDoS, що створюють ботнети, та трояни-вимагачі, які шифрують дані з метою вимагання викупу. Ознаки зараження включають погіршення продуктивності системи, незрозумілі спливаючі вікна, вимкнене програмне забезпечення безпеки, ненормальний мережевий трафік, несанкціоновані зміни файлів та незвичайну поведінку процесів, наприклад, коли легітимні програми створюють підозрілі дочірні процеси.

Сучасний захист від троянських програм вимагає використання складних підходів, що виходять за рамки традиційних антивірусних сигнатур. Системи виявлення та реагування на кінцевих точках, що базуються на поведінці, відстежують аномальну активність, а моніторинг мережі виявляє підозрілі моделі комунікації та сигнали управління та контролю. Технології штучного інтелекту та машинного навчання корелюють події на кінцевих точках, у мережах та хмарних середовищах для виявлення прихованих кампаній. Додаткові заходи захисту включають впровадження контролю доступу з мінімальними привілеями, багатофакторну автентифікацію, регулярне встановлення виправлень, сегментацію мережі, комплексне резервне копіювання та навчання користувачів для запобігання початковим векторам інфікування, таким як фішинг…

Такі платформи, як система Open Threat Management від Seceon, є прикладом захисту від троянських програм нового покоління за допомогою виявлення на основі штучного інтелекту та машинного навчання, яке ідентифікує ненормальну поведінку та приховані дії, що обходять традиційні інструменти. Їх динамічне

моделювання загроз постійно створює базові показники поведінки для виявлення аномалій, що сигналізують про діяльність троянських програм, а автоматизовані функції реагування на загрози можуть ізолювати скомпрометовані кінцеві точки, блокувати команди та комунікації управління, а також припиняти шкідливі процеси в режимі реального часу. Забезпечуючи єдину видимість у всіх середовищах та безперервну оцінку ризиків, такі платформи скорочують час перебування зловмисника з тижнів до хвилин, одночасно спрощуючи операції з безпеки…

Вірус «Троянський кінь» залишається потужною кіберзброєю саме тому, що він використовує довіру людей, а не технічні вразливості. Його успіх полягає не в грубій силі, а в обмані, тому освіта користувачів і вдосконалене виявлення поведінки є критично важливими компонентами захисту. Оскільки троянські програми продовжують розвиватися, використовуючи безфайлові техніки, шифрування та поліморфні варіанти, які обходять традиційні засоби захисту, організації повинні застосовувати комплексні стратегії безпеки, що поєднують технології, процеси та людей, щоб виявляти, стримувати та нейтралізувати цих прихованих зловмисників, перш ніж вони зможуть завдати тривалого збитку…» ***(Pushpendra Mishra. Trojan Horse Virus: Understanding, Detecting, and Defending with Seceon // Techstrong Group Inc. (https://securityboulevard.com/2025/09/trojan-horse-virus-understanding-detecting-and-defending-with-seceon/). 19.09.2025).***

***

«Нова і дуже складна кампанія з використанням шкідливого програмного забезпечення під назвою «fezbox» проникла в екосистему npm, використовуючи інноваційну стеганографічну техніку для приховування шкідливого коду в QR-кодах. Замаскована під легітимну бібліотеку утиліт JavaScript/TypeScript, «fezbox» таємно виконує операції з викрадення паролів за допомогою цього хитро прихованого QR-коду, що знаменує значну еволюцію в загрозах ланцюжку поставок і демонструє зростаючу креативність кіберзлочинців в обході систем безпеки та уникненні виявлення…

Пакет «fezbox» позиціонується як комплексна утиліта, що пропонує підтримку TypeScript і модульні допоміжні функції, а в його README згадується модуль QR-кодів. Однак у ньому навмисно опущено важливі деталі про його здатність отримувати QR-коди з віддалених URL-адрес і виконувати вбудований шкідливий код. Аналітики Socket.dev виявили шкідливе програмне забезпечення після виявлення підозрілих моделей поведінки та декількох рівнів заплутування, включаючи обернення рядків, мінімізацію коду та нове стеганографічне використання QR-кодів для приховування кінцевого корисного навантаження. Шкідливий пакет був активним у реєстрі npm на момент виявлення, що спонукало Socket.dev вимагати його негайного видалення та призупинення дії облікового запису зловмисника…

Складний багатоетапний процес виконання шкідливого програмного забезпечення починається з перевірки середовища та затримки часу (120 секунд) для уникнення виявлення пісочницею, забезпечуючи виконання тільки в легітимних середовищах браузера шляхом перевірки наявності об'єктів вікна та

документа. Основна шкідлива функціональність обертається навколо зворотного URL-рядка, який приховує розташування стеганографічного QR-коду. Після зворотного перетворення цей рядок перетворюється на зображення QR-коду, розміщене на Cloudinary, яке містить кінцевий корисний вантаж. Це зображення QR-коду — не просто посилання, а стеганографічний контейнер, який приховує JavaScript-код, призначений для вилучення значень імені користувача та пароля з файлів cookie браузера.

Після декодування корисний вантаж використовує додаткове заплутування рядків для пошуку файлів cookie, що містять облікові дані для автентифікації, зокрема поля «ім'я користувача» та «пароль». Зібрані облікові дані потім виводяться за допомогою HTTPS POST-запиту на сервер управління, розміщений на хмарній платформі Railway. Ця складна багаторівнева атака, що поєднує в собі уникнення виявлення, затримки, зворотне впорядкування рядків, стеганографічне приховування та вилучення облікових даних, є значним кроком вперед у атаках на ланцюжок поставок на основі npm, що вимагає від команд безпеки адаптувати свої засоби захисту для протидії цим сучасним технікам…» ***(Tushar Subhra Dutta. New Malware in npm Package Steals Browser Passwords Using Steganographic QR Code // Cyber Security News (https://cybersecuritynews.com/new-malware-in-npm-package-steals-browser-passwords/). 23.09.2025).***

***

Програми-вимагачі

«26 серпня компанія ESET заявила, що виявила перше в світі програмне забезпечення для вимагання викупу на базі штучного інтелекту, яке вона назвала PromptLocker. Але, схоже, це не так: дослідники Нью-Йоркського університету (NYU) взяли на себе відповідальність за виявлене ESET шкідливе програмне забезпечення.

Виявляється, PromptLocker насправді є експериментом під назвою «Ransomware 3.0», проведеним дослідниками Інженерної школи Тандона Нью-Йоркського університету. Представник школи повідомив Tom's Hardware, що зразок Ransomware 3.0 був завантажений на VirusTotal, платформу для аналізу шкідливого програмного забезпечення, а потім помилково виявлений дослідниками ESET.

ESET заявила, що шкідливе програмне забезпечення «використовує скрипти Lua, згенеровані з жорстко закодованих підказок, для переліку локальної файлової системи, перевірки цільових файлів, вилучення вибраних даних та виконання шифрування». Компанія зазначила, що зразок не мав руйнівних можливостей, що є логічним для контрольованого експерименту.

Але шкідливе програмне забезпечення справді працює: Нью-Йоркський університет заявив, що «симуляційна шкідлива система штучного інтелекту, розроблена командою Tandon, виконувала всі чотири фази атак програм-вимагачів — картографування систем, ідентифікацію цінних файлів, крадіжку або

шифрування даних та генерування записок з вимогою викупу — на персональних комп’ютерах, корпоративних серверах та промислових системах керування».

Це викликає занепокоєння? Безперечно. Але є суттєва різниця між академічними дослідниками, які демонструють перевірку концепції, та справжніми хакерами, які використовують ту саму техніку в реальних атаках. Тепер дослідження, ймовірно, надихне невдах застосувати подібні підходи, особливо враховуючи, що воно здається надзвичайно доступним…» ***(Nathaniel Mott. AI-powered PromptLocker ransomware is just an NYU research project — the code worked as a typical ransomware, selecting targets, exfiltrating selected data and encrypting volumes // Future US, Inc. (https://www.tomshardware.com/tech-industry/cyber-security/ai-powered-promptlocker-ransomware-is-just-an-nyu-research-project-the-code-worked-as-a-typical-ransomware-selecting-targets-exfiltrating-selected-data-and-encrypting-volumes). 05.09.2025).***

***

«Нова загроза від програм-вимагачів стала однією з найактивніших кіберзлочинних операцій 2025 року: тільки в червні програма-вимагач SafePay здійснила атаки на 73 організації, а в липні — ще на 42.

Цей сплеск зробив SafePay значущим загрозою, яку команди з безпеки по всьому світу повинні розуміти і до якої вони повинні бути готові захищатися.

На відміну від традиційних моделей «програм-вимагачів як послуги» (RaaS), які покладаються на партнерські мережі, SafePay працює як закрита, незалежна група, яка дотримується суворої оперативної безпеки.

Методика швидких атак цієї групи виявилася надзвичайно ефективною: протягом 2025 року було задокументовано понад 270 заявлених жертв.

Їхні операції спрямовані в першу чергу на середні та великі підприємства в США, Німеччині, Великій Британії та Канаді, з особливим акцентом на галузях, критично важливих для повсякденної діяльності, включаючи виробництво, охорону здоров'я та будівництво.

Виникнення групи можна простежити до вересня 2024 року, після значних операцій правоохоронних органів, які ліквідували ALPHV (Чорний кіт) та серйозно порушили інфраструктуру LockBit в рамках операції «Кронос»…» ***(Tushar Subhra Dutta. SafePay Ransomware Claiming Attacks Over 73 Victim Organizations in a Single Month // Cyber Security News (https://cybersecuritynews.com/safepay-ransomware-claiming-attacks-over-73-victim/). 05.09.2025).***

***

«Згідно з результатами загальноєвропейського дослідження, проведеного TicTac Cyber Security і Social Active, програми-вимагачі завдають європейській промисловості більшого удару, ніж будь-коли раніше. Висновки є суворими.

З 2023 по середину 2025 року атаки програм-вимагачів постійно зосереджувалися на секторах, які стимулюють національну економічну діяльність і обробляють критично важливі дані. Промисловість, технології та охорона здоров'я залишаються постійною мішенню кіберзлочинних угруповань. Дані чітко

показують, що ці сектори неодноразово стають об'єктами атак, оскільки зловмисники навмисно вибирають жертв, для яких простої є дороговартісними, а відновлення — складним.

За останні два роки кількість нападів зросла з тривожною швидкістю. У 2023 році було зафіксовано 713 інцидентів. У 2024 році ця цифра стрибнула до 1288, що становить зростання на понад 80 відсотків. До липня 2025 року на континенті вже було зареєстровано 921 атаку, і за прогнозами, до кінця року їхня загальна кількість перевищить 1746, що стане новим рекордом.

Експерти наголошують, що це не тимчасовий сплеск, а чіткий доказ того, що загроза не тільки зростає, а й швидко еволюціонує. Кожна організація в кожному секторі повинна ставитися до цього з максимальною серйозністю.

Виробництво залишається головним об'єктом атак, який кіберзлочинці вважають дуже цінним, а частка успішних атак на нього зросла з 26,92% до 28,79%. На другому місці — технологічний сектор, частка атак на який зросла з 10,3% до 11,72%. Атаки на сектор охорони здоров'я зросли до 8,97%, що підкреслює, наскільки привабливим він став для зловмисників, які шукають конфіденційні дані пацієнтів.

Роздрібна торгівля, разом з іншими ключовими секторами, такими як готельний бізнес і транспорт, залишається під постійним тиском. Урядові та судові системи також є частими цілями, оскільки їхні системи містять дані громадян, а інтенсивний суспільний попит на швидке відновлення після інциденту робить їх головними кандидатами для вимагання. Енергетика та фінансові послуги також піддаються атакам, хоча і рідше, ймовірно, через більш суворі заходи безпеки та регулювання…» ***(New Research Confirms Europe's Ransomware Attacks set a 2025 Record // Cision US Inc. (https://www.prweb.com/releases/new-research-confirms-europes-ransomware-attacks-set-a-2025-record-302547621.html). 06.09.2025).***

***

«…Програми-вимагачі перетворилися на кримінальну індустрію, обсяг якої сягає мільярдів доларів. Тільки в період з 2020 по 2022 рік було зафіксовано понад 865 атак на організації в Австралії, Канаді, Новій Зеландії та Великій Британії. Сучасні хакери не обмежуються лише шифруванням файлів: їхні «подвійні» і навіть «потрійні» схеми вимагання включають погрози витоку або продажу викрадених даних, що значно посилює тиск на жертв. Доступ отримується за допомогою ботнетів, заражених безкоштовних програм, наповнення облікових даних та високоспеціалізованого фішингу, що використовує людські упередження; потрапивши всередину, оператори переміщуються по горизонталі за допомогою легальних інструментів, таких як PowerShell і WMI, встановлюють кілька «задніх дверей», створюють карту мережі та резервних копій, а потім запускають гібридне (симетричне + асиметричне) шифрування, яке є одночасно швидким і криптографічно надійним…

Екосистема зараз працює на ринку Ransomware-as-a-Service, який відокремлює основних розробників від мобільних груп партнерів: перші підтримують код, платіжні сайти та блоги про витоки, а другі займаються вторгненнями, розгортанням та переговорами. Така структура дозволяє злочинцям

легко переходити між брендами, обходити заходи правоохоронних органів та швидко розширюватися. Conti лідирував у цій галузі з 141 інцидентом, за ним слідували варіанти LockBit з 129 інцидентами; RaaS-організації, що існували протягом декількох років, значно перевершували за обсягами одноразові або «традиційні» угруповання, такі як Pysa або NetWalker…

Промислові підприємства виявилися найбільш вразливими цілями — 239 атак було скоєно проти заводів з виробництва та будівельних матеріалів, оскільки простої на цих підприємствах обходяться досить дорого, що робить викуп привабливим. Неподалік від них опинилися компанії, що займаються споживчими товарами, нерухомістю, фінансами та технологіями. Коротко кажучи, програмне забезпечення для вимагання викупу перетворилося на стійку сервісну економіку, технічна досконалість, гнучкий ринок праці та стратегічний вибір жертв якої становлять дедалі більшу загрозу для критичної інфраструктури в усьому світі…» ***(Tushar Subhra Dutta. Australian Authorities Uncovered Activities and Careers of Ransomware Criminal Groups // Cyber Security News (https://cybersecuritynews.com/australian-authorities-uncovered-activities/). 08.09.2025).***

***

«…Огляд компанії Resilience за середину 2025 року показує, що випадки використання програм-вимагачів стають менш частими, але набагато більш руйнівними. Хоча компанія зафіксувала 53-відсоткове зниження кількості повідомлень про кіберінциденти в першій половині 2025 року порівняно з попереднім роком, середня сума виплат за вимогами програм-вимагачів зросла на 17 відсотків до понад 1,18 мільйона доларів — порівняно з 705 000 доларів у 2024 році. Програми-вимагачі зараз становлять 76% всіх збитків (91%, якщо врахувати порушення з боку постачальників), а шахрайство з використанням соціальних інженерних методів — 60% збитків…

Обсяг атак також зростає: у першому півріччі 2025 року було зафіксовано 4310 публічно розкритих випадків використання програм-вимагачів проти 3057 у попередньому півріччі, що порушило дворічну стабільність на рівні 2000 випадків. Interlock, Chaos і Scattered Spider очолили атаки на компанії, застраховані Resilience, причому нові, нестабільні угруповання все частіше віддають перевагу низькотехнологічним тактикам, таким як переконливі телефонні дзвінки та підробка особи, а не експлойтам нульового дня…

Незважаючи на те, що 79% постраждалих клієнтів відмовляються платити викуп, фінансовий збиток від успішних вторгнень продовжує зростати, що підкреслює те, що генеральний директор Resilience Вішаал Харіпрасад називає «хвильовою» природою кіберзлочинності: злочинці вдосконалюють прибутковий метод, поки захисники не наздоганяють їх, а потім переходять до нових слабких місць. Дані свідчать про те, що швидке стримування, управління ризиками постачальників та страхові стратегії повинні зосередитися насамперед на програмному забезпеченні для вимагання викупу, оскільки воно залишається єдиним найбільшим чинником серйозних кіберзбитків…» ***(Allen Laman. Report: Ransomware Attacks Costlier as***

Threat Actors Become More Systematic // Wells Media Group, Inc. (https://www.claimsjournal.com/news/national/2025/09/09/332864.htm). 09.09.2025).

***

«Нещодавно виявлена група хакерів, що використовує програми-вимагачі, націлена на жертв у всьому Азіатсько-Тихоокеанському регіоні, використовуючи спеціально розроблені засоби ухилення, які можуть становити «значну загрозу» для організацій, попереджають дослідники з компанії Trend Micro, що спеціалізується на питаннях безпеки.

У серпні компанія Trend Micro вперше виявила кампанію з використанням програм-вимагачів, організовану групою The Gentlemen, «новою і раніше не задокументованою групою зловмисників».

На відміну від груп, які використовують загальні методи обходу антивірусних програм, The Gentlemen застосовує індивідуальні методи, адаптовані до кожної конкретної цілі…

Група вже атакувала щонайменше 17 організацій у виробничому, будівельному, медичному та страховому секторах. Більшість випадків було зареєстровано в Таїланді, але Trend Micro також виявила цілі у Сполучених Штатах.

Виходячи з кількості жертв та складності атаки, дослідники Trend Micro стверджують, що The Gentlemen, ймовірно, є ребрендингом групи досвідчених операторів або ініціативою добре фінансованої організації з боротьби з кіберзлочинністю.

Аналіз показує, що зловмисники отримують початковий доступ, використовуючи інтернет-сервіси або скомпрометовані облікові дані…» ***(Akshaya Asokan. 'The Gentlemen' Ransomware Targets Asia Pacific // Information Security Media Group, Corp. (https://www.inforisktoday.com/the-gentlemen-ransomware-targets-asia-pacific-a-29408). 10.09.2025).***

***

«…Вперше виявлена 5 вересня, Yurei — це нещодавно виявлена група програм-вимагачів, першою жертвою якої стала шрі-ланкійська компанія з виробництва продуктів харчування. Група дотримується моделі подвійного вимагання: вони шифрують файли жертви та викрадають конфіденційні дані, а потім вимагають викуп за розшифрування та утримання від публікації викраденої інформації.

Дослідницька компанія Check Point Research (CPR) визначила, що програма-вимагач Yurei походить лише з незначними модифікаціями від Prince-Ransomware, сімейства програм-вимагачів з відкритим кодом, написаних на Go. Це показує, як шкідливе програмне забезпечення з відкритим кодом значно знижує поріг входу для кіберзлочинців, дозволяючи навіть менш кваліфікованим зловмисникам запускати операції з програмами-вимагачами.

Програма-вимагач від Yurei містить недолік, який може дозволити часткове відновлення даних за допомогою Shadow Copies, але група в основному покладається на вимагання на основі крадіжки даних. У їхньому блозі страх та

наслідки витоку даних є головним чинником тиску, щоб змусити жертв сплатити викуп.

З моменту публікації першої жертви 5 вересня їх кількість зросла до трьох, що вказує на швидкозростаючу операцію.

Розслідування виявило натяки на те, що походження зловмисника може бути з Марокко…» ***(Yurei & The Ghost of Open Source Ransomware // Check Point Software Technologies LTD. (https://research.checkpoint.com/2025/yurei-the-ghost-of-open-source-ransomware/). 12.09.2025).***

***

«…Після того, як у липні атака програм-вимагачів змусила повністю вимкнути ІТ-мережу міста Сент-Пол, міська влада заявляє, що зараз вона «відновлюється». Мер Мелвін Картер, який оголосив надзвичайний стан і залучив підрозділ кіберзахисту Національної гвардії Міннесоти, наголосив, що «витонченому зовнішньому зловмиснику», який стоїть за цією атакою, не було виплачено викуп, а 3500 муніципальних службовців були змушені змінити свої паролі. З того часу першими відновили роботу пріоритетні телефонні лінії (включно з 911), а зараз працюють усі телефонні служби департаментів; відновлено роботу порталів для оплати рахунків за воду, басейн і поле для гольфу без нарахування штрафів за прострочення; бібліотечний каталог і системи реєстрації працюють, хоча публічний доступ до Інтернету там залишається недоступним; знову доступні інструменти для співпраці, такі як SharePoint, Outlook, Teams, Legistar і Granicus, а також ключові спільні диски. Платежі за комунальні послуги ніколи не були під загрозою, оскільки вони здійснюються через окремого постачальника. У майбутньому місто планує 17 вересня запустити систему «PAULIE» (Permitting and Utilities, Licensing, Inspection Engine) для забезпечення більш сучасної та безпечної платформи для обслуговування мешканців, оскільки розслідування та посилення систем безпеки тривають…» ***(Kilat Fitzgerald. Most St. Paul services restored following ransomware attack // FOX Television Stations (https://www.fox9.com/news/most-st-paul-services-restored-ransomware-attack). 12.09.2025).***

***

«Невада відновлюється після атаки програм-вимагачів, що сталася 24 серпня і спочатку вивела з ладу кілька державних веб-сайтів і служб. Губернатор Джо Ломбардо повідомив про 300-відсотковий сплеск спроб кібератак — близько 150 мільйонів атак на державні брандмауери протягом 72 годин після першої прес-конференції — порівняно з типовими 150 000 на день. Серед цих атак були спроби фішингу в режимі реального часу після перезавантаження паролів співробітників по всьому штату, але підвищена пильність допомогла їх запобігти… Близько 90% веб-сайтів та сервісів, доступних для громадськості, вже відновлено, а протягом вихідних очікується відновлення ще більшої кількості; Департамент транспортних засобів (DMV) працює в повному обсязі, тоді як деякі системи, зокрема реєстр сексуальних злочинців та портал перевірки анкетних даних продавців зброї, залишаються пріоритетними для відновлення. Хоча чиновники не

розголошують технічних деталей у зв'язку з федеральним розслідуванням, головний інформаційний директор Тімоті Галлузі вказав, що відбулася крадіжка даних; Ломбардо підтвердив витік інформації, але заявив, що немає доказів того, що особисті дані резидентів або фінансові дані штату були скомпрометовані, а інформація, що зазнала впливу, обмежується даними про процеси, запаси та бази даних штату. Держава посилює контроль управління, впроваджує більш надійні паролі та розширює багатофакторну автентифікацію, щоб запобігти повторному використанню скомпрометованих облікових даних, обіцяючи постійну прозорість відповідно до оперативної безпеки…» ***(Keely Quinlan. Cyberattack attempts on Nevada state websites increased 300% after August ransomware attack // StateScoop (https://statescoop.com/cyberattack-attempts-on-nevada-state-websites-increased-300-after-august-ransomware-attack/). 12.09.2025).***

***

«19 вересня авіаперевезення по всій Європі були паралізовані, коли атака програм-вимагачів на Collins Aerospace, ключового постачальника IT-послуг для авіації, порушила роботу систем реєстрації в основних аеропортах, включаючи Лондон-Хітроу, Берлін-Бранденбург і Брюссель. Пасажири зіткнулися із затримками, скасуванням рейсів та довгими чергами, оскільки аеропорти були змушені повернутися до ручного оброблення даних. Хоча з того часу робота аеропортів нормалізувалася, цей інцидент продемонстрував вразливість високоцифрових секторів, таких як авіація, та нагальну необхідність забезпечення кіберстійкості критичної інфраструктури…

Аеропорти є особливо вразливими, оскільки мають численні взаємопов'язані системи — від обробки пасажирів і багажу до управління повітряним рухом — які експлуатуються різними постачальниками. Ця складність створює слабкі місця і окремі збої, які можуть поширюватися по всій екосистемі…

Зловмисники стають все більш витонченими, часто атакуючи критичну інфраструктуру сотні разів на день, причому атаки все частіше поєднують кібернетичні та фізичні тактики, такі як вторгнення дронів поблизу енергетичних об'єктів. Минулі випадки, такі як шкідливе програмне забезпечення NotPetya, яке коштувало судноплавному гіганту Maersk 300 мільйонів доларів і порушило роботу 76 портів, демонструють, наскільки руйнівними можуть бути такі атаки з економічної та операційної точки зору. В авіації, де кожна затримка має ланцюгові наслідки, стійкість стосується не тільки кібербезпеки, але й безпеки та довіри пасажирів…

Для посилення захисту експерти виділяють три пріоритети. По-перше, зацікавлені сторони повинні визначити системні слабкі місця та ретельно перевірити резервні системи, такі як ручна реєстрація. По-друге, керівники повинні вимагати від сторонніх постачальників більшої прозорості та підтвердження безпеки, використовуючи такі інструменти, як інвентаризація програмних компонентів та тестування на проникнення. По-третє, оператори повинні створювати екосистеми співпраці, в яких можна обмінюватися досвідом, встановлювати базові вимоги до постачальників, проводити спільні навчання та впроваджувати стандарти безпеки на етапі проектування.

В епоху зростаючої геополітичної напруженості та нерівномірного рівня кібербезпеки в ланцюгах постачання, вбудовування стійкості на всіх рівнях авіаційної системи стало надзвичайно важливим. Координовані дії, прозорість та співпраця будуть ключовими факторами для зменшення вразливості та забезпечення безперебійності глобальних авіаперевезень…» ***(Filipe Beato, Tal Goldstein. Grounded. Why the European airports cyber incident is a wake-up call // World Economic Forum (https://www.weforum.org/stories/2025/09/european-airports-cyber-incident-critical-infrastructure/). 25.09.2025).***

***

«Активність програм-вимагачів протягом п'яти місяців поспіль залишалася на рівні менше 500 інцидентів, але загроза залишається серйозною: NCC Group зафіксувала 328 атак у серпні, що лише на 13% менше, ніж у липні, і приблизно на рівні середнього показника за квітень-серпень минулого року. Головними цілями знову стали промислові підприємства (121 злом), за ними йдуть компанії, що виробляють товари широкого вжитку (66), та IT-провайдери (31); атака на шведського постачальника програмного забезпечення для управління персоналом Miljödata порушила роботу 200 місцевих органів влади. У регіональному розрізі 81% всіх атак припало на Північну Америку та Європу, Азія та Південна Америка зазнали відповідно 9% та 4% атак…

Серед груп, що становлять загрозу, Qilin знову посіла перше місце, відповідаючи за 53 інциденти (16 відсотків). Akira (43) і Safepay (26) також залишалися активними. Примітно, що фахівці з соціальної інженерії, відомі як Scattered Spider, передають фактичні корисні навантаження програм-вимагачів на аутсорсинг афілійованим компаніям, що надають послуги «програм-вимагачів як послуги» за високу комісію, таким як ALPHV, RansomHub, DragonForce і Qilin, що дозволяє команді поєднувати свої фішингові навички з технічно досконалим шкідливим програмним забезпеченням і підтримувати діяльність навіть тоді, коли одна платформа порушується правоохоронними органами.

NCC Group попереджає, що такі мінливі партнерські відносини надають економіці програм-вимагачів «безжальну, ділову структуру», яку захисники та слідчі повинні враховувати у своїх стратегіях. Геополітичні суперечності, такі як нові мита США на товари з Індії на тлі зближення Індії, Китаю та Росії, можуть ще більше загострити ситуацію, оскільки зловмисники історично використовують моменти дипломатичної напруги. Висновок, за словами керівника відділу Threat-Intelligence Метта Халла: незважаючи на нещодавнє стабілізування ситуації, обсяги програм-вимагачів все ще залишаються високими, і кіберстійкість повинна бути головним пріоритетом як для бізнесу, так і для урядів…» ***(Report: Ransomware Decreased by 13% in August // Automation.com (https://www.automation.com/en-us/articles/september-2025/cyber-threat-groups-collaborate?listname=Automation). 17.09.2025).***

***

«…Нова група хакерів, що використовує програмне забезпечення для вимагання викупу під назвою «Warlock» (також відома як Gold Salem від

Sophos і Storm-2603 від Microsoft), з моменту свого появи в березні 2025 року атакувала понад шістдесят організацій, швидко завоювавши репутацію як за свої технічні навички, так і за зухвалість. Група швидко здійснила наступні дії:

• зламала Microsoft SharePoint за допомогою спеціальної ланцюжка експлойтів ToolShell;

• проклала тунель для трафіку через легальний інструмент Velociraptor, щоб залишитися прихованою;

• зібрала облікові дані за допомогою Mimikatz;

• поширилася всередині мережі за допомогою PsExec та Impacket;

• використала об'єкти групової політики для поширення своїх програм-вимагачів.

Warlock активно купує експлойти та доступ до мережі на підпільних форумах, незважаючи на те, що раніше не залишав публічних слідів. Microsoft позначає операторів як таких, що базуються в Китаї, але Sophos стверджує, що остаточна атрибуція залишається недоведеною; очевидним є те, що угруповання навмисно уникає більшості російських і китайських цілей — на його сайті з витоками інформації з'явилася лише одна російська жертва, що свідчить про операції за межами сфери впливу Росії…

З понад шістдесяти названих жертв, Warlock стверджує, що продав вкрадені дані 27 з них приватно і публічно оприлюднив дані приблизно третини (32 %), що свідчить про те, що багато хто або заплатив викуп, або був монетизований через приватні продажі. Sophos застерігає, що цифра 45 % «приватних продажів» може бути перебільшеною, що є поширеною тактикою для завищення сприйнятого впливу банди та тиску на майбутніх жертв…» ***(Sead Fadilpašić. New Gold Salem ransomware could be the most worrying new strain we've seen for a while // Future US, Inc. (https://www.techradar.com/pro/security/new-gold-salem-ransomware-could-be-the-most-worrying-new-strain-weve-seen-for-a-while). 19.09.2025).***

***

«Нещодавня атака програм-вимагачів на Французький музей природної історії в липні 2025 року, що стала продовженням більш масштабної кампанії серпня 2024 року, яка зачепила численні французькі музеї, мала несподівані фізичні наслідки: злодії скористалися перебоями в роботі системи, спричиненими кібератакою, щоб викрасти золоті самородки на суму приблизно 705 000 доларів. Системи музею були настільки серйозно пошкоджені, що виставку було скасовано, а системи сигналізації та відеоспостереження виведені з ладу, що дозволило злодіям за допомогою кутової шліфувальної машини прорізати двері та паяльною лампою відкрити вітрину. Еммануель Скуліос, заступник генерального директора музею, повідомив, що було викрадено шість кілограмів золота, яке, ймовірно, було переплавлено, що унеможливило його повернення. Поліція підозрює, що злодії знали про виведення з ладу системи сигналізації…

Тим часом ФБР опублікувало нове попередження про «зловмисників», які підробляють веб-сайт Центру скарг на інтернет-злочини (IC3). Ці зловмисники створюють платні спонсоровані посилання в пошукових системах, які

перенаправляють користувачів на шахрайські сайти з дещо зміненими URL-адресами, з метою збирання особистої інформації, такої як імена, адреси, номери телефонів та банківські реквізити. ФБР радить громадськості ігнорувати результати пошукових систем і безпосередньо вводити в браузері адресу «www.ic3.gov», ретельно перевіряючи домен «.gov». Це вже друге таке попередження цього року після квітневого попередження про понад 100 підроблених URL-адрес IC3 та спроби шахраїв видати себе за вигаданого «головного директора IC3 Хайме Квіна»…

Нарешті, сектор розкішних товарів також зазнає атак: французький конгломерат Kering, власник таких брендів, як Gucci та Balenciaga, повідомив, що неавторизована третя сторона тимчасово отримала доступ до його систем і викрала обмежену кількість даних про клієнтів, включаючи історію покупок, хоча фінансова інформація не була скомпрометована. Ці інциденти в сукупності підкреслюють різноманітний і мінливий характер кіберзагроз, від фізичних пограбувань до складних фішингових кампаній та витоків даних, що зачіпають як державні установи, так і приватні підприємства…» ***(Iain Thomson. Ransomware attack linked to museum break-in and theft of golden exhibits // The Register (https://www.theregister.com/2025/09/22/infosec_in_brief/). 22.09.2025).***

***

Шпигунське програмне забезпечення

«У середу дослідники цифрової криміналістики звинуватили кенійську владу у встановленні шпигунського програмного забезпечення на телефонах двох кінематографістів, які допомагали створювати документальний фільм про повстання молоді в країні.

Кінорежисерів Браяна Адагалу та Ніколаса Вамбугу було заарештовано 2 травня та звільнено наступного дня, але влада затримала їхні телефони до 10 липня. За словами Ієна Мутісо, адвоката, який представляє інтереси кінематографістів, ймовірно, уряд Кенії встановив шпигунське програмне забезпечення FlexiSPY, поки влада зберігала пристрої.

FlexiSPY, який є комерційно доступним, легше виявити, ніж набагато дорожче шпигунське програмне забезпечення-найманці, доступне державам, але має аналогічні можливості після встановлення, сказав Джон Скотт-Рейлтон, судовий дослідник з The Citizen Lab, який допоміг підтвердити зараження.

Компанія орієнтує свій продукт на батьків та роботодавців, які хочуть «знати все, що відбувається» на пристрої. Її шпигунське програмне забезпечення може записувати дзвінки, відстежувати місцезнаходження, прослуховувати через мікрофони, завантажувати фотографії та перехоплювати електронні листи й текстові повідомлення.

Адагалу та Вамбугу заарештували за нібито публікацію неправдивої інформації, сказав Мутісо, але їм так і не було висунуто звинувачень…» ***(Suzanne Smalley. Researchers find spyware on phones belonging to Kenyan filmmakers //***

Recorded Future News (https://therecord.media/researchers-spyware-kenya-filmmaker-phone). 10.09.2025).

***

«Після гучного скандалу в Італії, де WhatsApp виявив, що 90 журналістів та діячів громадянського суспільства стали жертвами шпигунського програмного забезпечення Graphite від Paragon, а уряд визнав, що шпигував за активістами, які захищають права біженців, що змусило Paragon розірвати контракт, та сама технологія стеження може бути впроваджена в імміграційній службі США. Міністерство внутрішньої безпеки тихо скасувало наказ про припинення роботи над контрактом Імміграційної та митної служби (ICE) на суму 2 мільйони доларів на повністю налаштоване рішення Paragon (ліцензії, обладнання, гарантія, технічне обслуговування, навчання), який адміністрація Байдена спочатку підписала і заморозила в жовтні 2024 року після ретельного вивчення пресою, заявивши, що вона перевіряє дотримання директиви президента, щоб використання урядовим шпигунським програмним забезпеченням не підривало демократію та громадянські свободи… Подробиці перегляду та контракту залишаються невідомими, але ICE, схоже, отримала дозвіл на продовження роботи; ні ICE, ні Paragon не надали коментарів. Citizen Lab виявила, що Graphite використовує експлойт WhatsApp без кліків — додавання цілі до групи може змусити телефон прочитати заражений PDF-файл, що робить атаки ефективними навіть у разі ігнорування повідомлень; WhatsApp заявляє, що додала нові засоби захисту. Компанія Paragon, заснована колишніми ізраїльськими чиновниками Ехудом Бараком та Ехудом Шнеорсоном і придбана американською приватною інвестиційною компанією за 500 мільйонів доларів для злиття з RED Lattice, позиціонує себе як етичну альтернативу NSO Group, скандал навколо якої з Pegasus призвів до санкцій з боку США…

Агентство з боротьби з наркотиками (DEA) використовувала Graphite проти іноземних картелів, але впровадження ICE розширить такі можливості на внутрішнє імміграційне правозастосування, оскільки агентство збирає дані (медичні та страхові заяви, мережі номерних знаків) і створює «ImmigrationOS» від Palantir, що працює майже в режимі реального часу. Які дані будуть подаватися в систему, чи буде ICE зламувати телефони і як будуть захищені американці, залишається без відповіді, оскільки чиновники обох адміністрацій не забезпечують достатньої прозорості…» ***(Matthew Petti. What Is ICE Doing With This Israeli Spyware Firm? // Reason Foundation (https://reason.com/2025/09/08/what-is-ice-doing-with-this-israeli-spyware-firm/). 08.09.2025).***

***

Фішингові атаки

«…У новому попередженні для користувачів PayPal, яке повторює нещодавні попередження для Amazon та Facebook, йдеться про сплеск фішингових електронних листів, які підробляють повідомлення системи

безпеки PayPal та сповіщення про "підозрілий вхід". Зловмисники підробляють адресу відправника і клонують зовнішній вигляд PayPal, а потім перенаправляють жертв на фальшиві сторінки входу, щоб викрасти облікові дані. Порада з безпеки проста: великі технологічні компанії не надсилають попереджень про безпеку або облікові записи з посиланнями для входу, тому ігноруйте і видаляйте такі електронні листи; ніколи не входьте в систему за небажаними посиланнями (використовуйте тільки ті посилання, які ви самі запросили для перевірки або зміни пароля). Якщо вас турбує активність вашого облікового запису, відкрийте безпосередньо додаток або веб-сайт PayPal і перевірте свій обліковий запис/налаштування там. MalwareBytes зазначає, що ці шахрайські листи можуть виглядати переконливо - часто скопійовані з реальних листів PayPal - але мають класичні ознаки: терміновість, занадто велику суму (наприклад, 900 доларів), а також загальні або некоректні привітання на кшталт "Шановний клієнт" або взагалі жодного. З огляду на те, як легко підробити поле "від кого" в електронному листі, найбезпечнішим варіантом за замовчуванням буде вважати кожен небажаний запит на вхід як зловмисний…» ***(Zak Doffman. Your PayPal Account Is Under Attack If You See This Message // Forbes (https://www.forbes.com/sites/zakdoffman/2025/09/06/your-paypal-account-is-under-attack-if-you-see-this-message/). 06.09.2025).***

***

«Tycoon, популярний фішинг-набір, відповідальний за більшість сучасних атак через електронну пошту, очевидно, був оновлений новими техніками, що допомагають зловмисникам приховувати шкідливе програмне забезпечення та шкідливі посилання в електронних листах.

Дослідники безпеки Barracuda опублікували детальний звіт, що охоплює численні нові тактики, які спостерігаються в реальному житті, включаючи кодування URL-адрес, підроблені CAPTCHA, техніку надлишкового префікса протоколу, використання символу «@» та зловживання розділенням піддоменів.

За допомогою техніки кодування URL зловмисники вставляють серію невидимих пробілів у веб-адреси, щоб приховати шкідливі частини посилання від сканування безпеки, або додають дивні символи, такі як символи Unicode.

«Використовуючи несподівані та незвичайні коди і символи, а також роблячи видиму веб-адресу менш підозрілою і більш схожою на звичайний веб-сайт, техніка кодування призначена для обману систем безпеки і ускладнення розпізнавання загрози одержувачами та традиційними фільтрами», — пояснює Barracuda.

З іншого боку, підроблені CAPTCHA роблять веб-сайт більш легітимним, одночасно обходячи базові перевірки безпеки.

Техніка надлишкового префікса протоколу передбачає створення URL-адреси, яка лише частково містить гіперпосилання або містить недійсні елементи (наприклад, два «https» або відсутність //). Це приховує справжнє призначення посилання, водночас роблячи активні частини законними. Символ @ можна використовувати у веб-адресі, щоб приховати шкідливу частину URL-адреси.

Оскільки все, що знаходиться перед «@», браузери розглядають як «інформацію про користувача», зловмисники можуть розмістити там щось надійне,

наприклад «office365». Фактичне місце призначення посилання — шкідлива цільова сторінка — знаходиться після «@».

Набір Thy Tycoon також здатний розділяти піддомени на доброякісні та зловмисні. Тепер він дозволяє зловмисникам створювати фальшиві веб-сайти, використовуючи імена, які на перший погляд пов'язані з відомими компаніями (наприклад, «office365Scaffidips.azgcvhzauig.es»). Це може ввести жертв в оману, змусивши їх думати, що вони мають справу з піддоменом Microsoft, але остання частина адреси є фактичним фішинговим сайтом, що належить зловмиснику.

Фішинг стає дедалі складнішим, витонченішим і, отже, дедалі важчим для виявлення. Barracuda стверджує, що найкращим захистом є багаторівневий підхід із різними рівнями безпеки, який дозволяє виявляти, перевіряти та блокувати незвичайну або несподівану активність.

Вони також рекомендують рішення на основі штучного інтелекту або машинного навчання в поєднанні з регулярним навчанням співробітників». ***(Sead Fadilpašić. Phishing emails are getting smarter - and using some new tricks to snare victims // Future US, Inc. (https://www.techradar.com/pro/security/phishing-emails-are-getting-smarter-and-using-some-new-tricks-to-snare-victims). 04.09.2025).***

***

«Швидко зростаюча фішингова кампанія під назвою «Ваше хмарне сховище заповнене» (Your Cloud Storage Is Full) імітує сповіщення від таких сервісів, як Google Drive та iCloud, попереджаючи, що користувачі перевищили обсяг сховища і ризикують остаточним видаленням фотографій та документів, якщо не вживуть негайних заходів. Посилання в цих електронних листах ведуть до переконливо оформлених підроблених порталів, які збирають дані для входу, а в деяких випадках і платіжні реквізити, ставлячи під загрозу особисті та навіть корпоративні рахунки в умовах широкого використання хмарних технологій та віддаленої роботи. Шахраї використовують страх перед втратою даних і часто обходять спам-фільтри, використовуючи персоналізацію, отриману в результаті зломів або придбаних списків, що спонукало FTC нагадати користувачам, що законні постачальники не запитують конфіденційні дані через небажані посилання. Рекомендації з безпеки, отримані в результаті аналізу галузі, рекомендують перевіряти домени відправників і наводити курсор на посилання, вмикати двофакторну автентифікацію та сканувати пристрої, якщо є підозра на витік інформації, а організації повинні посилити навчання щодо тактик створення терміновості, граматичних ознак та несподіваних запитів, а також застосовувати фільтрування на основі штучного інтелекту та інформацію про загрози, щоб блокувати приманки до надходження в поштову скриньку. Останні повідомлення включають випадки, коли жертви зазнали несанкціонованих витрат після введення даних на підроблених сторінках оновлення; рекомендовані заходи включають негайну зміну пароля, моніторинг облікового запису та повідомлення відповідних органів. В кінцевому рахунку, для протидії таким схемам необхідний багаторівневий підхід — освіта користувачів, технічні заходи безпеки та захист на рівні постачальника послуг — у поєднанні зі здоровим скептицизмом щодо небажаних повідомлень про «заповнення пам'яті», щоб зручність хмарних

технологій не перетворилася на загрозу безпеці…» ***(Ava Callegari. Cloud Storage Full' Phishing Scam: Tips to Stay Safe // iEntry, Inc. (https://www.webpronews.com/cloud-storage-full-phishing-scam-tips-to-stay-safe/). 08.09.2025).***

***

«З травня 2025 року зловмисники перетворили Amazon Simple Email Service (SES) на повноцінну фабрику фішингу, яка може розсилати понад 50 000 шахрайських повідомлень на день. Операція починається, коли зловмисники отримують ключі доступу до AWS — витікших у публічних репозиторіях коду, викрадених з неправильно налаштованих хмарних ресурсів або вкрадених з комп'ютерів розробників — і негайно запитують GetCallerIdentity, щоб оцінити дозволи свого нового облікового запису. Якщо доступ до SES доступний, вони запускають автоматизовану багаторегіональну атаку: за лічені секунди вони запускають виклики PutAccountDetails у кожному регіоні AWS, що, за словами дослідників Wiz, раніше не було задокументовано, щоб обійти обмеження SES на 200 електронних листів на день і перейти безпосередньо в режим виробництва…

Після скасування обмежень на відправлення листів злочинці перевіряють низку доменів за допомогою CreateEmailIdentity — деякі з них належать їм безпосередньо (managed7.com, street7news.org, docfilessa.com), інші є законними доменами зі слабкими або відсутніми налаштуваннями DMARC — і створюють правдоподібні адреси, такі як admin@ або noreply@. Потім жертви отримують вишукані приманки під назвою «Ваші податкові форми за 2024 рік готові до перегляду та друку», які направляють їх на сайти для збору облікових даних, такі як irss.securesusa.com; служби аналізу трафіку приховують інфраструктуру від базових сканерів…

Коли потрібні ще вищі квоти, актори автоматично відкривають квитки підтримки AWS (CreateCase) і намагаються додати політику IAM під назвою «ses-support-policy», хоча ці спроби підвищення привілеїв поки що не увінчалися успіхом. Проте зловживання самообслуговуванням все ще дозволяє їм щодня надсилати десятки тисяч фішингових електронних листів і збирати облікові дані або платіжні дані у великих обсягах.

Кампанія підкреслює, як неактивні або забуті ключі AWS та міжрегіональні аномалії API можуть бути використані як зброя, і наголошує на необхідності більш суворого моніторингу діяльності SES, більш жорсткого контролю перевірки доменів та швидкого скасування невикористаних облікових даних у хмарних середовищах…» ***(Tushar Subhra Dutta. Hackers Weaponize Amazon Simple Email Service to Send 50,000+ Malicious Emails Per Day // Cyber Security News (https://cybersecuritynews.com/hackers-weaponizee-amazon-simple-email-service/). 08.09.2025).***

***

«Державний департамент США цього тижня оголосив про винагороду до 10 мільйонів доларів за інформацію про трьох співробітників Федеральної служби безпеки Росії (ФСБ).

За твердженням уряду, троє зловмисників, Павло Олександрович Акулов, Михайло Михайлович Гаврилов та Марат Валерійович Тюков, змовилися з метою злому мереж сотень енергетичних компаній у США та за кордоном.

Метою атак, за словами Державного департаменту, було дати змогу «російському уряду порушити роботу таких об'єктів та пошкодити їх».

Троє офіцерів та їхні спільники «націлилися на понад 380 іноземних компаній енергетичного сектору у 135 країнах», зазначає департамент на своєму «Нагороди за правосуддя» вебсайті.

Підозрювані, члени підрозділу «Центр 16» ФСБ, атакували американські та іноземні нафтогазові компанії, атомні електростанції, компанії з відновлюваної енергетики, комунальні та електромережеві підприємства, консалтингові та інженерні групи, а також компанії з передових технологій.

У серпні 2021 року Акулову, Гаврилову та Тюкову в США було висунуто звинувачення у комп'ютерному шахрайстві та зловживаннях, шахрайстві з використанням електронних засобів зв'язку та крадіжці особистих даних за обтяжуючих обставин.

Згідно з обвинувальним висновком, вони атакували енергетичні компанії в рамках кампанії Dragonfly, яка включала отримання постійного доступу до мереж жертв та зараження їх шкідливим програмним забезпеченням Havex шляхом компрометації ланцюга поставок.

На другому етапі кампанії, відомої як Dragonfly 2.0, троє зловмисників нібито атакували понад 3300 користувачів понад 500 американських та міжнародних компаній та організацій, включаючи урядові установи США, за допомогою фішингових атак.

У серпні 2025 року ФБР попередило, що підрозділ Центру 16 ФСБ, відомий у спільноті кібербезпеки як Berserk Bear, Blue Kraken, Castle, Crouching Yeti, Dragonfly, Ghost Blizzard та Koala Team, атакував старі вразливості в мережевих пристроях Cisco.

Cisco, яка приписала цю активність Static Tundra, підгрупі в рамках державної APT-групи, відомої як Energetic Bear, заявила, що основною метою атак було встановлення постійного доступу та збір інформації про конфігурацію». ***(Ionut Arghire. US Offers $10 Million for Three Russian Energy Firm Hackers // SecurityWeek (https://www.securityweek.com/us-offers-10-million-for-three-russian-energy-firm-hackers/). 04.09.2025).***

***

«У вівторок Міністерство юстиції США оголосило про висунення звинувачень проти громадянина України, якого уряд звинувачує у сотнях

атак з використанням програм-вимагачів, спрямованих проти американських та міжнародних компаній.

Володимир Тимощук, також відомий як «deadforz», «Boba», «msfv» і «farnetwork», був звинувачений Міністерством юстиції за участь у схемах, в результаті яких було вимагано викуп у понад 250 компаній у США та сотень інших по всьому світу. Тимощук залишається в розшуку.

«Тимощук — серійний злочинець, який використовував програми-вимагачі, націлені на провідні американські компанії, медичні установи та великі іноземні промислові підприємства, і погрожував оприлюднити їхні конфіденційні дані в Інтернеті, якщо вони відмовляться платити», — заявив у офіційній заяві прокурор США Джозеф Ночелла-молодший…

У кримінальному обвинувальному акті, поданому до Східного округу Нью-Йорка, стверджується, що між груднем 2018 року та жовтнем 2021 року Тимощук та його спільники використовували варіанти програм-вимагачів Nefilim, LockerGoga та MegaCortex для проникнення та шифрування мереж сотень компаній у Сполучених Штатах та за кордоном. Прокурори стверджують, що атаки завдали значних збитків жертвам у США, як через виплату викупу, так і через зусилля щодо повернення коштів…» ***(Jim Morley. DOJ Charges Ukrainian National for Over 250 Ransomware Attacks // Newsmax Media, Inc. (https://www.newsmax.com/politics/ransomware-cyberattack-volodymyr-tymoshchuk/2025/09/09/id/1225700/). 09.09.2025).***

***

«…Фінський хакер Алексантері Ківімакі, який вже був засуджений до шести років і трьох місяців ув'язнення за спробу шантажувати понад 20 000 пацієнтів психотерапевтів, чиї файли він викрав з клініки Vastaamo, у четвер вийшов на свободу після того, як Апеляційний суд Гельсінкі погодився звільнити його на час оскарження вироку. Суд послався на тривалий термін його попереднього ув'язнення (він перебуває у в'язниці з моменту арешту у 2023 році у Франції та екстрадиції до Фінляндії), але підкреслив, що вирок залишається в силі і що, згідно з фінським законодавством, він вважається невинуватим під час апеляційного процесу, який триватиме до листопада. Ківімакі, який у підлітковому віці був членом групи «гріферів» Lizard Squad, заперечує всі звинувачення і стверджує, що справа проти нього базується на непрямих доказах; прокурори натомість наводять судові докази, що пов'язують його з журналами сервера, платежами в біткойнах, особистими фотографіями та записами електронної пошти, знайденими в витоку даних. Про злом 2018 року стало відомо лише в 2020 році, коли зловмисник почав надсилати електронні листи жертвам, серед яких були діти та пацієнти з важкими травмами, погрожуючи опублікувати їхні терапевтичні записи, якщо вони не заплатять. Понад 24 000 осіб повідомили про спроби вимагання, що зробило цю справу одним із найбільших злочинів проти конфіденційності даних у Європі і, як висловилися фінські ЗМІ, «поворотним моментом для Фінляндії». Адвокати жертв заявляють, що їхні клієнти досі страждають від оприлюднення інформації, а остаточне рішення апеляційного суду очікується пізніше цього року…» ***(Alexander Martin. Hacker convicted of extorting 20,000 psychotherapy victims walks free during appeal // Recorded Future News***

(https://therecord.media/finland-vastaamo-hacker-free-during-appeal-conviction). 12.09.2025).

***

«Секретна служба США ліквідувала мережу електронних пристроїв, розташованих у триштатному районі Нью-Йорка, які використовувалися для здійснення численних телекомунікаційних погроз на адресу високопоставлених урядовців США, що становило безпосередню загрозу для захисних операцій агентства.

Це захисне розвідувальне розслідування призвело до виявлення понад 300 SIM-серверів, розташованих в одному місці, та 100 000 SIM-карт у різних місцях.

Окрім здійснення анонімних телефонних погроз, ці пристрої можуть використовуватися для проведення широкого спектру телекомунікаційних атак. Це включає виведення з ладу базових станцій стільникового зв'язку, здійснення атак типу «відмова в обслуговуванні» та сприяння анонімному, зашифрованому спілкуванню між потенційними зловмисниками та злочинними угрупованнями.

Хоча криміналістична експертиза цих пристроїв ще триває, попередній аналіз вказує на наявність стільникового зв'язку між зловмисниками, що діють від імені держави, та особами, які відомі федеральним правоохоронним органам…

Ці пристрої були зосереджені в межах 35 миль від глобальної сесії Генеральної Асамблеї Організації Об'єднаних Націй, яка зараз триває в Нью-Йорку. Враховуючи час, місце розташування та потенціал значних перебоїв у роботі телекомунікацій у Нью-Йорку, спричинених цими пристроями, агентство швидко вжило заходів для зриву цієї мережі. Розслідування проводить Підрозділ розширеного запобігання загрозам Секретної служби США, новий підрозділ агентства, що займається запобіганням найбільш значним та неминучим загрозам для наших охоронців. Розслідування наразі триває…» ***(U.S. Secret Service dismantles imminent telecommunications threat in New York tristate area // United States Secret Service (https://www.secretservice.gov/newsroom/releases/2025/09/us-secret-service-dismantles-imminent-telecommunications-threat-new-york). 23.09.2025).***

***

«Чоловік у віці близько сорока років був заарештований у Західному Сассексі у зв'язку з кібератакою, яка спричинила кількаденні перебої в роботі основних європейських аеропортів, зокрема Хітроу, Берліна та Брюсселя. Національне агентство з боротьби зі злочинністю (NCA) підтвердило арешт за підозрою у скоєнні злочинів відповідно до Закону про неправомірне використання комп'ютерних систем, пов'язаних із атакою на компанію Collins Aerospace, через збій програмного забезпечення для обробки багажу та реєстрації пасажирів, що спричинило затримки рейсів, уповільнення роботи та необхідність використання паперових бортових квитків. Чоловік був звільнений під заставу, а NCA підкреслило, що розслідування перебуває на початковій стадії…

Атака програм-вимагачів, виявлена пізно в п'ятницю, паралізувала системи Collins Aerospace, які використовують кілька авіакомпаній, змусивши аеропорти покладатися на ручні обхідні шляхи, які зберігалися протягом тижня. Аеропорт

Хітроу залучив додатковий персонал для управління чергами, Берлін попередив про подовження часу обробки та подальші затримки, а аеропорт Брюсселя закликав пасажирів реєструватися онлайн, щоб уникнути заторів. Материнська компанія Collins Aerospace, RTX Corporation, підтвердила, що програмне забезпечення відновлюється після невдалих спроб перезапуску, і порадила авіакомпаніям готуватися до щонайменше ще одного тижня перебоїв у роботі…

Програми-вимагачі, які часто використовуються для паралізування систем до моменту здійснення платежу в криптовалюті, стали прибутковим інструментом для кіберзлочинних угруповань, приносячи сотні мільйонів щороку. Ця атака підкреслює більш широку загрозу для галузі, оскільки, за даними аерокосмічної компанії Thales, кількість кібератак на авіацію за останній рік зросла на 600%. Незважаючи на те, що більшість рейсів в аеропорту Хітроу зараз виконуються в звичайному режимі, цей інцидент підкреслює вразливість критичної авіаційної інфраструктури та більш широкі ризики, пов'язані з ескалацією організованої кіберзлочинності…» ***(Imran Rahman-Jones, Joe Tidy. Man arrested in connection with cyber-attack on airports // BBC (https://www.bbc.com/news/articles/c62ldxyj431o). 25.09.2025).***

***

«Поліція Лас-Вегаса заарештувала підозрюваного підлітка, причетного до серії кібератак 2023 року на казино Стріпу, які завдали збитків на суму щонайменше 100 мільйонів доларів. Поліція Лас-Вегаса заявила, що підлітку пред'явлені звинувачення, зокрема у вимаганні та незаконних діях з використанням комп'ютерних технологій, пов'язаних із «складною» кампанією, яка з серпня по жовтень була спрямована проти декількох казино і пов'язана з групами, відомими як Scattered Spider, Octo Tempest, UNC3944 та 0ktapus. Caesars Entertainment повідомила про крадіжку конфіденційних даних клієнтів у своїх документах, а MGM Resorts зазнала серйозних операційних збоїв; MGM відмовилася коментувати арешт, а Caesars не надала жодної відповіді. За даними влади, підозрюваного встановила кібергрупа ФБР у Лас-Вегасі. Арешт відбувся приблизно через місяць після окремого кібератаки на державні служби Невади 25 серпня, що змусило штат ізолювати системи; губернатор Джо Ломбардо пізніше заявив, що немає доказів витоку особистої інформації і що роботи з відновлення просуваються…» ***(James Powel, Amaris Encinas, Jeffrey Meehan. Teenage hacker arrested for cyberattacks against Las Vegas casinos // Gannett Co., Inc. (https://www.usatoday.com/story/news/crime/2025/09/22/teen-arrested-vegas-2023-casino-cyberattack/86299664007/). 22.09.2025).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Google випустила критичне попередження про безпеку Android, яке підтверджує наявність двох вразливостей нульового дня - CVE-2025-38352 (ядро Linux) та CVE-2025-48543 (виконання Android), які дозволяють локальне підвищення привілеїв без додаткових привілеїв або взаємодії з користувачем; відповідні пристрої Pixel отримують виправлення негайно, тоді як інші виробники отримають код протягом 48 годин і випустять виправлення у своїх щомісячних бюлетенях. У цьому циклі також усуваються чотири інші критичні вразливості: CVE-2025-48539 в системі Android та три проблеми Qualcomm (CVE-2025-21450, -21483, -27034). Подробиць поки що небагато, але 4 вересня CISA додала ці дві експлуатовані CVE до свого каталогу відомих уразливостей, надавши федеральному персоналу час до 25 вересня, щоб оновити або припинити використання уражених пристроїв; CISA характеризує CVE-2025-38352 як високоефективну гонку між часом перевірки та часом використання в ядрі, а CVE-2025-48543 - як уразливість в Android Runtime, яка може дозволити втечу з пісочниці Chrome і локальну ескалацію. Попередження підкреслює ризик фрагментації Android: патчі отримають лише пристрої, які все ще перебувають у вікні підтримки, що залишить без захисту понад мільярд телефонів; за оцінками Zimperium, 25,3% пристроїв не можуть бути оновлені через вік, і в будь-який час більше половини з них працюють на застарілих версіях ОС, багато з яких вже скомпрометовані. Хоча мандат CISA поширюється на федеральних користувачів, його рекомендації та каталог KEV (Відома уразливість, що експлуатується) призначені для інформування широкої громадськості та приватних спільнот, що займаються кібербезпекою…» ***(Zak Doffman. Google Confirms Android Attacks—No Fix For 1 Billion Phones // Forbes (https://www.forbes.com/sites/zakdoffman/2025/09/06/google-confirms-android-attacks-no-fix-for-1-billion-phones/). 06.09.2025).***

***

«Чеське національне агентство з кібербезпеки попередило, що китайські сонячні інвертори становлять загрозу безпеці даних країни.

Зростаюча цифровізація та наявність «складних технологічних рішень» у критично важливих секторах, таких як енергетика, становлять загрозу безпеці, попередило вчора Національне агентство з кібербезпеки та інформаційної безпеки (NÚKIB).

Такі інфраструктурні системи, як енергетичні мережі, охорона здоров'я та транспорт, дедалі більше залежать від хмарного зберігання та обробки даних, а також дистанційного керування. NÚKIB зазначив, що це означає, що постачальники цих технологічних рішень «можуть суттєво впливати на роботу

критичної інфраструктури та/або отримувати доступ до важливих даних, що робить довіру до надійності постачальника абсолютно необхідною».

Ці пристрої все частіше підключаються до Інтернету, і їх виробники можуть керувати ними дистанційно. Агентство визначило фотоелектричні інвертори як продукт високого ризику поряд із моделями для великих мов, електромобілями, розумними лічильниками, медичними технологіями та персональними пристроями, такими як смартфони та годинники.

Як підставу для своїх занепокоєнь NÚKIB посилався на «підтверджену зловмисну діяльність суб'єктів, пов'язаних з КНР (Китайською Народною Республікою), спрямовану проти Чеської Республіки», зокрема на «кампанію» хакерської групи APT31.

У ньому додано, що «політичне та правове середовище КНР… дозволяє урядовим органам Китаю доступ до даних, що зберігаються на території КНР, або суттєве втручання урядових органів Китаю в діяльність приватних компаній». Це може викликати питання щодо протоколів безпеки китайських виробників інверторів. NÚKIB включив Гонконг та Макао до своєї оцінки ризиків.

Згідно з чеським Законом про кібербезпеку, компанії, що використовують сонячні інвертори китайського виробництва, «повинні враховувати цю загрозу у своїх аналізах ризиків та реагувати на виявлені ризики, впроваджуючи належні заходи безпеки»…» ***(Will Norman. Czech Republic warns of cybersecurity threat from Chinese solar inverters // Informa PLC (https://www.pv-tech.org/czech-republic-warns-of-cybersecurity-threat-from-chinese-solar-inverters/). 04.09.2025).***

***

«Критична вразливість (CVE-2025-42957) у програмному забезпеченні для планування ресурсів підприємства SAP S/4HANA використовується зловмисниками «в обмеженій мірі», попередив у п'ятницю Національний центр кібербезпеки Нідерландів (NCSC NL).

Їхнє попередження, схоже, ґрунтується на звіті Лабораторії дослідження загроз SecurityBridge, яка нібито підтвердила, що експлойт для цієї вразливості активно використовується.

CVE-2025-42957 — це вразливість, що дозволяє впроваджувати код і впливає на функціональний модуль SAP S/4HANA, доступний через RFC.

«Цей недолік дозволяє впроваджувати довільний код ABAP у систему, обходячи необхідні перевірки авторизації. Ця вразливість фактично функціонує як бекдор, створюючи ризик повної компрометації системи, підриваючи конфіденційність, цілісність та доступність системи», – йдеться у записі CVE .

Єдиною перешкодою для експлуатації є те, що зловмисники повинні бути автентифіковані як користувачі з низькими привілеями, щоб розгорнути експлойт – перешкоду, яку не так вже й важко подолати.

Ця вразливість впливає на SAP S/4HANA (приватна хмара або локальна среда), що містить такі версії основного компонента Enterprise Management S4CORE: 102, 103, 104, 105, 106, 107 та 108.

12 серпня 2025 року компанія SAP випустила патч для CVE-2025-42957 та низки інших вразливостей…» ***(Zeljka Zorz. Attackers are exploiting critical SAP***

S/4HANA vulnerability (CVE-2025-42957) // Help Net Security (https://www.helpnetsecurity.com/2025/09/05/attackers-are-exploiting-critical-sap-s-4hana-vulnerability-cve-2025-42957/). 05.09.2025).

***

«Двоє етичних хакерів заявили про виявлення масштабних вразливостей безпеки на платформах, що розміщуються на Restaurant Brands International (RBI).

RBI — одна з найбільших у світі компаній швидкого обслуговування. Вона була утворена у 2014 році в результаті злиття американської мережі швидкого харчування Burger King та канадської мережі кав'ярень та ресторанів Tim Hortons вартістю 12,5 мільярда доларів. Відтоді RBI розширила свій портфель брендів, включивши Popeyes Louisiana Kitchen, придбану у 2017 році, та Firehouse Subs. Вона керує глобальною мережею з понад 32 000 ресторанів у понад 120 країнах та територіях…

Дослідники стверджують, що виявили, що RBI використовує AWS Cognito, але забув вимкнути реєстрацію користувачів. AWS Cognito – це керований сервіс від Amazon Web Services, який допомагає розробникам керувати реєстрацією користувачів, входом у систему та контролем доступу, не створюючи ці функції з нуля.

Вимкнення реєстрації користувачів важливе для того, щоб лише уповноважений персонал отримував облікові записи, які можуть створювати та централізовано керувати IT-адміністратори. Такий підхід зменшує ризик атаки, блокуючи відкриту самостійну реєстрацію та несанкціоноване створення облікових записів, що є критично важливим для захисту конфіденційних внутрішніх ресурсів і служб. Потім адміністратори можуть перевіряти та затверджувати облікові записи, перш ніж надавати користувачам доступ до програм, якими керують через Cognito.

Після того, як дослідники змогли проникнути через цей шлюз, вони сказали, що зрозуміли, що могли б позбавити себе клопоту, оскільки знайшли ще простішу кінцеву точку реєстрації, яка повністю обходила перевірку електронної пошти, в результаті чого надходило електронного листа з паролем у вигляді звичайного тексту.

Дослідники стверджують, що виявили три платформи-асистенти (домени bk.com, popeyes.com та timhortons.com) вразливими та можуть дозволити зловмиснику:

- Доступ до голосових записів замовлень клієнтів
- Додавання/видалення/керування франчайзинговими магазинами
- Перегляд та редагування облікових записів співробітників
- Доступ до аналітики магазину та даних про продажі
- Завантажуйте файли та надсилайте сповіщення до систем будь-якого магазину
- Використовуйте систему замовлення пристроїв із самостійним встановленням (з паролем, жорстко закодованим у HTML-коді)

Вони також кажуть, що виявили, що голосові записи замовлень клієнтів, необроблені аудіофайли реальних людей, які замовляють їжу, разом із фоновими розмовами, автомобільними радіо, а іноді й особистою інформацією (PII) , були передані штучному інтелекту для аналізу таких речей, як:

- Настрої клієнтів
- Рівень дружелюбності співробітників
- Показники успішного продажу додаткових товарів
- Терміни обробки замовлення
- Скільки разів співробітники казали «Ти головний» (бо це, безумовно, вирішальний бізнес-метрика)

Єдиний позитивний момент у цій історії полягає в тому, що, незважаючи на те, що дослідники виявили всі ці вразливості за один день, RBI виправив їх того ж дня. Але, очевидно, без згадки про дослідників і коментарів щодо вразливостей…» ***(Pieter Arntz. Popeyes, Tim Hortons, Burger King platforms have "catastrophic" vulnerabilities, say hackers // Malwarebytes (https://www.malwarebytes.com/blog/news/2025/09/popeyes-tim-hortons-burger-king-platforms-have-catastrophic-vulnerabilities-say-hackers). 09.09.2025).***

***

«Американське агентство з кібербезпеки CISA попереджає, що зловмисники використовують критично важливу вразливість у програмному забезпеченні фабрики DELMIA Apriso.

Розроблене французькою компанією Dassault Systèmes, DELMIA Apriso – це програмне забезпечення для управління виробничими операціями (MOM) та системою виконання виробництва (MES), призначене для управління кожною деталлю виробничого процесу. Програмне забезпечення використовується в Північній Америці, Європі та Азії, зокрема в аерокосмічній та оборонній, автомобільній, високотехнологічній галузях та промисловому обладнанні.

Дефект безпеки , що відстежується як CVE-2025-5086 (оцінка CVSS 9.0), описується як проблема десеріалізації ненадійних даних і впливає на випуски DELMIA Apriso з 2020 по 2025 рік.

постачальника Про помилку було публічно розкрито в червні, але в рекомендаціях не було надано технічної інформації про неї, окрім того, що її можна використовувати для віддаленого виконання коду (RCE).

У четвер CISA додала цю вразливість до свого каталогу відомих експлуатованих вразливостей (KEV), попередивши, що вона була використана в реальних умовах, та закликавши федеральні агентства виправити її до 2 жовтня, як того вимагає Обов'язкова операційна директива (BOD) 22-01.

Агентство з кібербезпеки також не надало подробиць щодо спостережуваних атак і не уточнило, чи використовувався CVE-2025-5086 в атаках програм-вимагачів…» ***(Ionut Arghire. DELMIA Factory Software Vulnerability Exploited in Attacks // SecurityWeek (https://www.securityweek.com/delmia-factory-software-vulnerability-exploited-in-attacks/). 12.09.2025).***

***

«Microsoft покращує захист від шкідливих файлів і посилань у Microsoft Teams, проблема, яка останнім часом загострюється. Згідно з попередженням Центру повідомлень Microsoft 365, користувачі почнуть отримувати попередження, коли вони надсилатимуть або отримують повідомлення, класифіковані як шкідливі.

Крім того, повідомлення в чатах і каналах, що містять EXE-файли, будуть повністю заблоковані, оскільки EXE-файли є поширеним вектором поширення шкідливого програмного забезпечення. Завдяки покращеній інтеграції з Microsoft Defender, усі повідомлення із заблокованих доменів також будуть заборонені.

«Щоб допомогти користувачам захиститися від шкідливого контенту, ми впроваджуємо попередження про повідомлення в Microsoft Teams», – йдеться в попередженні. «Ця нова функція відображає попереджувальний банер у повідомленнях, що містять URL-адреси, позначені як спам, фішинг або шкідливе програмне забезпечення, незалежно від того, чи є повідомлення внутрішнім, чи зовнішнім. Ці попередження підвищують обізнаність користувачів і доповнюють існуючі засоби безпеки, такі як безпечні посилання та ZAP». Перегляньте офіційну сторінку підтримки, щоб дізнатися більше про те, як працює захист посилань у Teams.

Розгортання цієї нової функції безпеки Microsoft Teams розпочнеться з публічного попереднього перегляду пізніше у вересні та очікується, що вона стане загальнодоступною до листопада. Вона буде доступна для клієнтів Microsoft Defender для Office 365 (MDO) та корпоративних клієнтів Microsoft Teams». ***(Microsoft Teams will soon warn you of malicious links and files // Techzonez (https://www.techzonez.com/forums/showthread.php/33717-Microsoft-Teams-will-soon-warn-you-of-malicious-links-and-files?s=7e4c5f293b31fab1e39ad8dea81176d8&p=156395#post156395). 12.09.2025).***

***

«…Підозрювані хакери, які, ймовірно, підтримуються китайською державою, використовували раніше невідомі вразливості в брандмауерах Cisco Adaptive Security Appliance (ASA), що змусило уряд США вжити термінових заходів. У четвер Агентство з кібербезпеки та безпеки інфраструктури (CISA) видало рідкісну надзвичайну директиву, яка зобов'язує всі цивільні федеральні агентства до півночі п'ятниці перевірити своє обладнання брандмауерів Cisco та негайно відключити всі уражені пристрої. Сотні вразливих пристроїв вбудовані у федеральні мережі, а додаткові екземпляри захищають критичну інфраструктуру в приватному секторі. Оскільки брандмауери регулюють вхідний і вихідний трафік, їх компрометація дозволяє зловмисникам прослуховувати, змінювати дані або відкривати «задні двері», які залишаються навіть після перезавантаження або оновлення програмного забезпечення…

Дослідники з безпеки в Palo Alto Networks приписують цю кампанію китайським операторам; CISA не заперечує цю оцінку. Злочинці використовують складні методи, що дозволяють їм приховувати сліди та зберігати доступ, і подібні атаки були виявлені в деяких агентствах ще в травні. Чиновники чекали з оприлюдненням інформації про порушення, поки Cisco не розробила патчі та рекомендації щодо мінімізації ризиків. Cisco, яка після 30 вересня припиняє

підтримку деяких застарілих моделей обладнання, закликає клієнтів негайно оновити обладнання. Тепер, коли технічні деталі стали публічними, CISA та уряди союзних країн попереджають, що інші шпигунські угруповання та злочинці можуть швидко скопіювати цей метод, підкреслюючи необхідність як для федеральних, так і для приватних організацій без затримки виконати опубліковані заходи щодо мінімізації ризиків…» ***(Joseph Menn. U.S. government scrambles to stop new hacking campaign blamed on China // The Washington Post (https://www.washingtonpost.com/technology/2025/09/25/cisa-federal-hacks-cisco/). 26.09.2025).***

***

«…Компанія Cisco попередила, що до двох мільйонів її маршрутизаторів, комутаторів та іншого обладнання, що працює під управлінням будь-якої підтримуваної версії IOS або IOS XE, містять активно експлуатовану уразливість нульового дня (CVE-2025-20352). Ця помилка, переповнення стека в компоненті Simple Network Management Protocol (SNMP), може бути викликана спеціально створеними пакетами SNMP: зловмисник, який володіє лише рядком спільноти тільки для читання пристрою (або дійсними обліковими даними SNMPv3), може вивести обладнання з ладу, а особа з вищими привілеями може перейти до повного віддаленого виконання коду як root. Команда реагування на інциденти безпеки продуктів Cisco (PSIRT) повідомляє, що вторгнення вже відбулися після викрадення локальних облікових даних адміністраторів. Хоча відкритий доступ до SNMP в Інтернеті вважається неналежною практикою, сканування Shodan показує, що понад два мільйони пристроїв саме так і працюють, надаючи зловмисникам величезну базу цілей. Cisco випустила виправлене програмне забезпечення і закликає клієнтів негайно оновити його; короткострокові заходи щодо зменшення ризику полягають лише в обмеженні доступу до SNMP для довірених користувачів і моніторингу трафіку SNMP, оскільки обхідних шляхів немає. Ця вразливість є однією з 14, виправлених у вересневому пакеті оновлень постачальника, вісім з яких мають високий рівень серйозності від 6,7 до 8,8…» ***(Dan Goodin. As many as 2 million Cisco devices affected by actively exploited 0-day // Condé Nast (https://arstechnica.com/security/2025/09/as-many-as-2-million-cisco-devices-affected-by-actively-exploited-0-day/). 25.09.2025).***

***

«…Дослідники в галузі безпеки виявили серйозну вразливість, названу «UniPwn», у популярних чотириногих і гуманоїдних роботах Unitree (моделі Go2, B2, G1, H1), яка дозволяє зловмисникам отримати повний контроль через Bluetooth Low Energy. Процес налаштування BLE використовує жорстко запрограмований, загальновідомий ключ; зашифрувавши слово «unitree» цим ключем, хакер може ввести шкідливий код (під виглядом SSID або пароля Wi-Fi), який виконується з правами суперкористувача. Заражений робот може автоматично сканувати, компрометувати та поширювати шкідливе програмне забезпечення на інші сусідні пристрої Unitree, утворюючи саморозповсюджувану «ботнет-мережу роботів»…

Окрім віддалених збоїв або перезавантажень, зловмисники можуть імплантувати троянські програми для викрадення даних або блокування оновлень прошивки. Дослідники Андреас Макріс, Віктор Майорал-Вільчес і Кевін Фіністерре також виявили, що гуманоїд G1 від Unitree кожні кілька хвилин непомітно передає аудіо-, відео-, сенсорні та GPS-дані на китайські сервери (43.175.228.18 і 43.175.229.18) через MQTT, фактично перетворюючи робота на прихований пристрій спостереження. Тести показали, що G1 може запускати агенти тестування на проникнення на базі штучного інтелекту, які самостійно сканують мережі, створюють карти поверхонь атак і запускають експлойти, перетворюючи робота з жертви на активного зловмисника.

Unitree не відреагувала на кількамісячні приватні повідомлення, і вразливість залишається невиправленою. З огляду на використання роботів у будинках, лабораторіях і навіть у британській поліції, дослідники попереджають, що скомпрометовані роботи можуть підслуховувати, створювати карти приміщень або слугувати мобільними платформами для кібероперацій. Вони стверджують, що цей інцидент підкреслює загальне ігнорування стандартів безпеки в галузі комерційної робототехніки, і представлять свої висновки — а також заклик до створення надійних систем кібербезпеки — на конференції IEEE Humanoids Conference в Сеулі…» ***(Tibi Puiu. Cybersecurity Experts Say These Humanoid Robots Secretly Send Data to China and Let Hackers Take Over Your Network // zmescience (https://www.zmescience.com/science/news-science/cybersecurity-experts-say-these-humanoid-robots-secretly-send-data-to-china-and-let-hackers-take-over-your-network/). 27.09.2025).***

***

«…Багато серверів Supermicro та материнських плат для центрів обробки даних знаходяться під загрозою, оскільки контролер управління базовою платою (BMC), припаяний до них, містить дві нещодавно виявлені вади прошивки, CVE-2025-7937 та CVE-2025-6198. Дослідники з Binarly виявили ці помилки під час перевірки січневого виправлення Supermicro для попередньої проблеми (CVE-2024-10237) і стверджують, що початкове виправлення було неповним.

Якщо зловмисник спочатку отримає доступ до BMC — що вже можливо завдяки додатковим уразливим місцям епохи 2024 року — нові слабкі місця дозволяють легко обійти перевірку підписів і прошити заражене зображення прошивки. Зловмисний код, захований у прошивці BMC, працює нижче рівня операційної системи, тому жоден звичайний засіб безпеки не може його побачити або видалити, що дає зловмисникам прихований і стійкий плацдарм для маніпулювання живленням, датчиками або навіть віддаленої переінсталяції ОС.

Supermicro заявляє, що усунула недоліки в тестовій версії прошивки і перевіряє більш широке оновлення, але генеральний директор Binarly Алекс Матросов попереджає, що ці помилки «важко» виправити і що повне, надійне виправлення може зайняти час. До того часу тисячі серверів на базі Supermicro залишаються вразливими до невидимих атак з боку кваліфікованих злочинців або державних структур…» ***(Alfonso Maruccia. Supermicro servers hit by critical***

vulnerabilities that allow undetectable malware attacks // TechSpot, Inc. (https://www.techspot.com/news/109608-supermicro-servers-susceptible-flaws-baseboard-management-controller.html). 24.09.2025).

***

«Libraesva усунула вразливість у своїй інтегрованій платформі безпеки електронної пошти, яка була використана зловмисниками.

Ця вразливість, яка відстежується як CVE-2025-59689 (оцінка CVSS 6,1), описується як проблема введення команд, яка може призвести до виконання довільних команд як користувач без привілеїв.

Згідно з повідомленням Libraesva, ця помилка може бути використана через шкідливі електронні листи, що містять спеціально створені стислі вкладення…

CVE спрацьовує з певними форматами архівів, що містять корисні навантаження, що використовують помилку неправильної санітарної обробки вводу для виконання довільних команд оболонки.

Дефект безпеки впливає на версії Libraesva ESG від 4.5 до 5.5, але виправлення були випущені лише для версій ESG 5.x, оскільки версії 4.x більше не випускаються.

Libraesva впровадила патчі як у хмарних, так і в локальних розгортаннях ESG і стверджує, що всі пристрої тепер використовують фіксовану версію програмного забезпечення.

Клієнтам, які використовують локальні версії ESG 4.x, рекомендується якомога швидше вручну оновити систему до виправленої версії 5.x, враховуючи, що вразливість було використано…

Libraesva ESG — це інтегроване рішення, яке захищає поштові служби від фішингу, BEC та складних загроз і підходить для всіх типів організацій, включаючи малий та середній бізнес, а також великі підприємства». ***(Ionut Arghire. Libraesva Email Security Gateway Vulnerability Exploited by Nation-State Hackers // SecurityWeek ® (https://www.securityweek.com/libraesva-email-security-gateway-vulnerability-exploited-by-nation-state-hackers/). 24.09.2025).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Оскільки рівень кіберзагроз продовжує зростати, ISN, світовий лідер в управлінні інформацією підрядників та постачальників, оснащує організації комплексними інструментами та послугами, які допомагають виявляти, оцінювати та пом'якшувати кіберризики, що виникають від сторонніх підрядників та постачальників. Завдяки пропозиції Cyber Secure™ від ISN, клієнти-наймаючий персонал отримує доступ до низки рішень, розроблених для забезпечення безперервності операційної діяльності, дотримання нормативних вимог та ефективного управління ризиками.

«Кіберризики в усьому ланцюжку поставок є актуальною та зростаючою проблемою», – сказав Джо Шльосер, віцепрезидент ISN. «Інтегруючи нагляд за кіберризиками в ISNetworld, клієнти з найму можуть оптимізувати відстеження, покращити дотримання вимог та приймати більш обґрунтовані рішення з більшою ефективністю».

Нещодавні кіберінциденти виявили вразливості критичної інфраструктури, підкреслюючи нагальну потребу в посиленні нагляду, особливо в капіталомістких галузях, де поширений доступ третіх сторін. Інструменти ISN Cyber Secure забезпечують комплексне рішення для управління кіберризиками третіх сторін. Центральним елементом цієї пропозиції є оцінка Cyber 360, яка забезпечує цільові оцінки кібербезпеки для підрядників та відповідає світовим стандартам.

Для подальшого посилення кіберстійкості ISN запровадив функцію сканування порушень у ISNetworld. Ця нова функція розширює можливості платформи щодо постійного моніторингу кіберстану та громадського сприйняття.

Cyber Secure доступний для клієнтів ISN Hiring без додаткової оплати та забезпечує централізований та ефективний контроль кіберризиків…» ***(ISN® Expands Cybersecurity Solutions to Help Organizations Manage Third-Party Cyber Risk // Business Wire, Inc. (https://www.businesswire.com/news/home/20250904987033/en/ISN-Expands-Cybersecurity-Solutions-to-Help-Organizations-Manage-Third-Party-Cyber-Risk). 04.09.2025).***

***

«…Підрядники Космічних сил США розробляють Cyber Resilience On-Orbit (CROO) — інструмент на базі штучного інтелекту, який виявляє кібератаки на супутники шляхом безперервного аналізу поведінки на орбіті та телеметрії, виводячи захист за межі сучасних переважно наземних систем оборони та шифрування каналів зв'язку, які захищають дані під час передачі, але не сам космічний апарат. Під керівництвом Proof Labs спільно з Big Bear AI та Redwire Space Systems, CROO буде пропонуватися у вигляді програмного забезпечення (з можливістю впровадження на борту) і, як заплановано, вийде на ринок наступного року. Проект частково фінансувався грантом від Дослідницької лабораторії ВПС США, а ймовірним замовником вважається Командування космічних систем. Продукт буде продаватися військовим та комерційним операторам… Моделі машинного навчання системи навчаються на високоточній синтетичній телеметрії, згенерованій за допомогою цифрового двійника Redwire і скомпільованій Big Bear, що охоплює швидкість реакційних коліс, положення зоряних трекерів, кути сонячних датчиків тощо, створюючи набір даних FireSat з 1,2 мільйонами рядків, що моделює як нормальну роботу, так і сценарії атак, які Big Bear планує опублікувати на GitHub. Важливо, що CROO призначений для виявлення атак за сигналами поза цільовою підсистемою, щоб протидіяти обману в стилі Stuxnet, порівнюючи фактичну роботу таких компонентів, як реакційні колеса, з даними, що надходять від їхніх датчиків. Ранні модельовані атаки зосереджуються на реакційному колесі та батареї космічного апарата — «серці» супутника — обраних за чіткі телеметричні сигнали, які вони створюють, з

додатковими сценаріями, випробуваними на іншому, нерозкритому супутнику. Представлена на заході Aerospace Corp та Space ISAC, ця ініціатива підкреслює роль цифрових двійників, спільних наборів даних та міжгалузевої співпраці у зміцненні космічних систем проти все більш витончених кіберзагроз…» ***(Shaun Waterman. Space Force Building Tools to Detect Cyberattacks on Satellites // Air & Space Forces Association (https://www.airandspaceforces.com/space-force-tools-to-detect-cyberattacks-satellites/). 11.09.2025).***

***

«…Агентство зв'язку та інформації НАТО вибрало Oracle Cloud Infrastructure (OCI) для модернізації критично важливих IT-систем альянсу, переходячи від локальних систем до гібридної хмарної моделі, про що було оголошено 11 вересня 2025 року. Під керівництвом Thales як головного підрядника та за участю фахівців Oracle Red Reply і Shield Reply, програма використовуватиме розподілену хмару OCI для задоволення суворих вимог безпеки та суверенітету даних у всіх державах-членах, додаючи аналітику на основі штучного інтелекту для швидшого виявлення загроз, високої доступності та доступу з низькою затримкою для операцій у реальному часі. Цей вибір підкреслює переваги суверенної хмари OCI — регіони з повітряним розривом і вдосконалене шифрування — в умовах посилення конкуренції в хмарній сфері та більш широких оборонних зусиль Oracle, включаючи партнерства з метою розширення можливостей штучного інтелекту та глобальної зв'язності. Впровадження буде здійснюватися поетапно, щоб мінімізувати перебої та інтегрувати штучний інтелект для прогнозного технічного обслуговування та кіберстійкості, хоча залишаються виклики щодо об'єднання застарілих систем, забезпечення взаємодії між мережами НАТО та захисту від загроз, що фінансуються державою. У разі успіху ця угода може стати зразком для впровадження хмарних технологій штучного інтелекту в оборонній сфері, прискорити цифрову трансформацію НАТО та закріпити зростаючу роль Oracle в цьому секторі, а перші показники вказують на створення більш гнучкої та безпечної інфраструктури альянсу…» ***(Tim Toole. NATO Selects Oracle Cloud for IT Modernization and Cyber Defense // iEntry, Inc. (https://www.webpronews.com/nato-selects-oracle-cloud-for-it-modernization-and-cyber-defense/). 12.09.2025).***

***

«…Восьмимісячне рандомізоване дослідження, в якому взяли участь 19 500 співробітників медичного центру Каліфорнійського університету в Сан-Дієго (UC San Diego Health), показує, що антифішингові програми, на які покладаються більшість великих організацій — щорічні «аудиторні» модулі та вбудовані уроки після кліка — практично не впливають на реальний ризик. У десяти спеціально розроблених фішингових кампаніях дослідники не виявили значущого зв'язку між нещодавнім проходженням щорічного навчання та схильністю до фішингу, а вбудоване навчання зменшило кількість кліків лише на два процентні пункти. Залученість до уроків на місці була мінімальною: три чверті користувачів витратили на них менше хвилини, а третина одразу закрила

сторінку… З плином місяців сукупна кількість жертв зросла з 10 % до понад 50 %, а ефективність сильно варіювалася залежно від приманки (менше 2 % клікнули на приманку «оновіть свій пароль Outlook», але 31 % повелися на підроблену зміну політики щодо відпусток). Враховуючи статус електронної пошти як головного вектора порушення безпеки, особливо в галузі охорони здоров'я, де в 2023 році було викрадено понад 133 мільйони записів, автори роблять висновок, що сучасне навчання «має невелику практичну цінність», і рекомендують перенаправити ресурси на технічні засоби захисту, такі як обов'язкова багатофакторна автентифікація та менеджери паролів, які перевіряють цілісність домену…» ***(Cybersecurity Training Programs Don't Prevent Employees from Falling for Phishing Scams // University of California (https://today.ucsd.edu/story/cybersecurity-training-programs-dont-prevent-employees-from-falling-for-phishing-scams). 17.09.2025).***

***

«…У сучасному взаємопов'язаному технологічному середовищі управління та захист нелюдських ідентичностей (NHI) має першочергове значення для надійної кібербезпеки. NHI, також відомі як ідентичності машин, — це криптографічні облікові записи, пов'язані з «секретами» (зашифрованими паролями або ключами), які аутентифікують та авторизують автоматизовані процеси в IT-інфраструктурі. Хоча управління цими ідентичностями є надзвичайно важливим для безперебійної роботи, воно є складним, а неправильне управління може призвести до несанкціонованого доступу та порушення безпеки даних.

Саме тут незамінною стає масштабована система управління секретами. Масштабованість є необхідністю, а не просто бажаною властивістю, оскільки вона дозволяє організаціям йти в ногу зі зростанням кількості та складності НІЗ у міру розширення їхніх IT-середовищ. Така система забезпечує гнучкість, дозволяючи організаціям адаптувати ресурси кібербезпеки до мінливих потреб, оптимізувати використання ресурсів, зменшити операційні витрати та забезпечити вищу окупність інвестицій.

Ефективна масштабована система управління секретами має безліч переваг: вона проактивно виявляє та мінімізує ризики безпеки, зменшуючи ймовірність порушень; забезпечує дотримання нормативних вимог завдяки впровадженню політик та аудиторських слідів; підвищує операційну ефективність завдяки автоматизації управління секретами, звільняючи команди безпеки для стратегічних ініціатив; а також покращує прозорість завдяки централізованому перегляду управління доступом, сприяючи кращому управлінню…

Вибір системи управління секретами з урахуванням масштабованості як основного критерію гарантує майбутнє рішення, яке сприяє безперебійній операційній ефективності. Динамічний характер цифрових загроз вимагає такої адаптивної структури, що робить її розуміння та впровадження необхідністю для створення безпечної та стійкої цифрової фортеці.

Наголос на масштабованому управлінні секретами є стратегічною необхідністю, оскільки з розширенням цифрової інфраструктури кількість НІІ та загрози, які вони становлять у разі неналежного управління, зростають експоненціально. Масштабована структура оптимізує управління життєвим циклом

НІІ, зменшує ризики безпеки, демонструє відповідність вимогам та підвищує ефективність організації, дозволяючи їй випереджати зростаючі виклики у сфері кібербезпеки…

Перехід до цієї структури вимагає ретельної оцінки: інвентаризації існуючих НІ, їх секретів і дозволів; розподілу необхідних ресурсів відповідно до організаційних цілей; проведення ретельного аудиту безпеки для усунення прогалин; і, що найважливіше, забезпечення того, щоб обрана структура могла адаптуватися до майбутнього зростання. Цей стратегічний підхід перетворює масштабоване управління секретами на каталізатор підвищення кібербезпеки, пропонуючи такі переваги, як готовність до майбутнього розширення, поліпшене управління ризиками, підвищена операційна ефективність та більш надійне управління і дотримання вимог…

Виклики, пов'язані з управлінням NHIs та секретами, будуть тільки посилюватися з розвитком технологій. Дослідження показують, що організації, які застосовують ефективні практики управління секретами, рідше стикаються з порушеннями безпеки даних і краще дотримуються вимог нормативних документів. Тому впровадження масштабованої системи управління секретами вже зараз є ключовим фактором для створення перспективної стратегії кібербезпеки, що стає обов'язковою умовою для підтримки надійних практик кібербезпеки в умовах постійно мінливого цифрового середовища…» ***(Alison Mack. Building a Scalable Secrets Management Framework // Techstrong Group Inc. (https://securityboulevard.com/2025/09/building-a-scalable-secrets-management-framework/). 20.09.2025).***

***

«Такі галузеві фреймворки, як MITRE ATT&CK та NIST, мають вирішальне значення для команд з кібербезпеки, які оцінюють засоби контролю, виявляють вразливі місця та встановлюють спільну мову між різними дисциплінами. До цих усталених моделей приєдналася нова Insider Threat Matrix™ — відкрита, загальнодоступний фреймворк, призначена виключно для виявлення та запобігання внутрішнім загрозам, розроблена колишніми фахівцями з внутрішніх загроз Джеймсом Вестоном та Джошуа Біманом.

Вестон і Біман створили Insider Threat Matrix™, оскільки вони зрозуміли, що існуючі структури зосереджуються переважно на зовнішніх супротивниках, залишаючи без належної уваги розслідування внутрішніх загроз, які часто є складними, неоднозначними та залежать від міжфункціональної співпраці. Їхньою метою було створити структуру, зосереджену на «людському факторі» та тому, як довіра руйнується зсередини, надаючи кібербезпековим, кадровим, юридичним та комплаєнс-командам послідовну таксономію для класифікації, виявлення та реагування на випадки внутрішніх загроз. Основними користувачами матриці є слідчі, які розслідують внутрішні загрози, та аналітики з питань безпеки, які розбираються у складних внутрішніх подіях, від тонких дій до інцидентів з високими ставками, де наміри можуть бути неясними…

Засновники також розрізняють «внутрішній ризик» та «внутрішню загрозу». «Внутрішній ризик» визначається як ймовірність та потенційний вплив будь-яких

дій або бездіяльності члена «населення» організації (працівників, підрядників тощо), які можуть призвести до шкоди або збитків, включаючи як навмисні, так і ненавмисні дії. «Внутрішня загроза», однак, конкретно стосується члена або групи всередині цієї популяції, які мають намір або можуть заподіяти шкоду або збитки. По суті, всі внутрішні загрози входять до ширшого спектру внутрішнього ризику, але не всі ризики переростають у загрози.

З моменту свого запуску на конференції Black Hat у 2024 році Insider Threat Matrix™ отримала надзвичайно позитивні відгуки, а слідчі та керівники програм високо оцінили її здатність забезпечити так необхідну спільну мову та структуру. Її застосування охоплює інженерію виявлення, розробку процесів розслідування, аудит безпеки та розробку політик. Засновники були особливо здивовані широким інтересом не тільки з боку спеціалізованих команд з боротьби з внутрішніми загрозами, але й з боку аналітиків SOC, фахівців з управління персоналом, а також зацікавлених сторін з юридичної та комплаєнс-сфери, що підкреслює її міжфункціональну цінність…

Для команд з безпеки, які бажають впровадити матрицю, вона розроблена для негайного використання, незалежно від зрілості програми. Нові програми можуть використовувати її для встановлення базових політик та відображення «масових порушень» — незначних, але частих порушень політик, які сигналізують про відхилення в поведінці. Вже встановлені програми можуть використовувати її для виявлення прогалин у контролі, узгодження виявлень для всебічного охоплення, керівництва розробкою правил та забезпечення послідовності розслідувань. Засновники зазначають, що «занадто рано» для впровадження матриці не буває; правильний час настає тоді, коли команда прагне перейти від ситуативних заходів до структурованих, обґрунтованих виявлень, запобіжних заходів та розслідувань. Першим практичним кроком є відображення останніх інцидентів, пов'язаних з інсайдерами, відповідно до категорій матриці, оскільки це часто виявляє очевидні закономірності та прогалини для виявлення та вдосконалення політики». ***(Stephanie Torto and Kasey Olbrych. The Insider Threat Matrix™: A Holistic Approach to Insider Threats // Proofpoint (https://www.proofpoint.com/us/blog/insider-threat-management/insider-threat-matrix-holistic-approach). 26.09.2025).***

***

Питання криптографії

«…Шифрування ніколи не було постійним: римські шифри були розгадані фахівцями з виявлення закономірностей, а машина «Енігма» — командою Тьюринга, а тепер квантові обчислення загрожують криптографічним основам цифрової ери. Квантові комп'ютери, що мають значення для криптографії (CRQC), які очікуються вже в 2030-35 роках, можуть використовувати алгоритми, такі як алгоритми Шора і Гровера, для зламу широко використовуваних схем, таких як RSA і криптографія на еліптичних кривих, що дозволить супротивникам підробляти підписи, відкривати «безпечні» канали і розшифровувати дані ретроактивно. Тому національні держави вже застосовують

стратегію «збирай зараз, розшифровуй пізніше», накопичуючи зашифровані скарби на той день, коли квантові машини досягнуть зрілості…

Особливо вразливими є фармацевтичні та біомедичні організації. Їхні записи клінічних випробувань, запатентовані формули, протоколи виробництва, набори даних геноміки та інформація про здоров'я пацієнтів повинні залишатися конфіденційними протягом десятиліть — саме протягом цього періоду, за прогнозами, з'являться CRQC. Десятирічні випробування або рецепт вакцини вартістю в мільярди доларів, розроблений сьогодні, можуть бути розшифровані завтра, що спричинить порушення нормативних вимог, втрату інтелектуальної власності, шкоду репутації та навіть загрозу національній безпеці в галузі охорони здоров'я. Велика мережа контрактних дослідницьких організацій, регуляторних органів та академічних партнерів у цьому секторі ще більше розширює площу атаки.

Однак перехід на постквантову криптографію (PQC) займе роки. Ключі стають більшими, застарілі системи можуть заклинити, а мільйони цифрових сертифікатів необхідно буде замінити за стислими циклами оновлення задовго до того, як NIST остаточно затвердить всі стандарти PQC. Кваліфікованих криптографів не вистачає, а управління, тіньові IT-системи та вразливість ланцюгів постачання додають складності…

Тому підготовка до квантової ери повинна розпочатися вже зараз. Правління компаній повинні зробити PQC стратегічним пріоритетом, провести інвентаризацію та класифікацію довготривалих даних, автоматизувати управління сертифікатами, апробувати алгоритми PQC та створити гнучкі процеси для відстеження змін стандартів. Якщо розглядати квантову стійкість як програмну зміну, а не як суто технічне оновлення, це дозволить захистити інтелектуальну власність, безпеку пацієнтів та довіру громадськості, а також гарантувати, що медичні досягнення майбутнього не будуть зведені нанівець квантовими комп'ютерами майбутнього…» ***(Nalneesh Gaur, Michael Elmore. Why pharma and life sciences must act now on the quantum threat // World Economic Forum (https://www.weforum.org/stories/2025/09/pharma-life-sciences-quantum-threat-cybersecurity/). 25.09.2025).***

***