**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

№ 3 (березень)

Київ – 2026

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. Київ, 2026. № 3 (березень). 139 с.

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

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

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

ЗМІСТ

Кібервійна проти України та операції у відповідь

«Нова біла книга від Cyber Defense Assistance Collaborative (CDAC) показує, що з моменту повномасштабного вторгнення Росії в 2022 році Україна зазнала безперервних кібератак, спрямованих на виведення з ладу урядових систем та критично важливих служб. Міжнародна допомога в галузі кіберзахисту була обіцяна або надана на суму приблизно 2,29 млрд доларів США — близько 1,2 % від загального обсягу військової допомоги — з яких 1,29 млрд доларів США вже надійшли на місце. Уряди домінують у фінансуванні (близько 1,7 млрд доларів США), переважно через великі пакети обладнання, реалізація яких часто займає роки, тоді як підтримка з боку приватного сектору надходить швидше, невеликими частинами і більше спрямована на програмне забезпечення та навчання…

Такі координаційні структури, як IT-коаліція та Талліннський механізм, сприяли збільшенню масштабів та визначенню пріоритетів, проте добровільна звітність залишає значні прогалини: значна частина допомоги залишається недокументованою, і жодна організація не має повного уявлення про потреби чи результати надання допомоги. Апаратне забезпечення все ще очолює списки запитів, але попит на навчання зростає, що свідчить про перехід до довгострокової самодостатності. Незважаючи на ці зусилля, адміністративні затримки, короткострокові ліцензії на програмне забезпечення та нерівномірна прозорість продовжують гальмувати ефективність. У міру того, як конфлікт вступає у п'ятий рік, екосистема переходить від ситуативних героїчних вчинків приватного сектору до структурованої багатосторонньої підтримки, але постійні проблеми з прозорістю та координацією підкреслюють необхідність більш жорсткого управління та стійкої прихильності до збереження цифрового фронту України в цілості…» ***(Anna Ribeiro. CDAC report examines cyber defense support to Ukraine as attacks target government and critical services // Industrial Cyber (https://industrialcyber.co/reports/cdac-report-examines-cyber-defense-support-to-ukraine-as-attacks-target-government-and-critical-services/). 10.03.2026).***

***

«За останні дванадцять років конфлікту з Росією Україна перетворилася на реальну лабораторію з кібервійни та кіберстійкості, стикаючись із постійними атаками на урядові системи, критичну інфраструктуру, енергетичні мережі, ЗМІ та фінансову сферу, і водночас поступово нарощуючи потенціал не лише для захисту від атак, а й для забезпечення функціонування держави навіть у разі успіху цих атак. Цей досвід показав, що кібербезпека — це не лише технічне питання, а виклик для всього суспільства, що залучає уряд, бізнес, громадянське суспільство, експертів приватного сектору, волонтерів та наукові кола. Реакція України в умовах війни базувалася на швидкій координації,

імпровізації та інноваціях, зокрема на хмарних резервних копіях, переміщенні критично важливих даних за кордон, децентралізованих платформах обслуговування громадян та тісній міжгалузевій співпраці, але зараз країна прагне перейти від надзвичайної мобілізації до стійкої національної моделі кіберстійкості, вбудованої в інституції… Серед ключових пріоритетів — впровадження кіберосвіти у школах, університетах та військовій підготовці, розширення партнерських відносин між бізнесом та науковими колами, а також програми стажування, розробка довгострокової стратегії формування кадрового потенціалу у сфері кібербезпеки та створення національного кіберрезерву, а також інституціоналізація прикладних досліджень у сфері кібербезпеки та безперервного навчання. На міжнародному рівні Україна перетворилася з отримувача ситуативної підтримки на активного учасника євроатлантичної кібер-екосистеми завдяки структурованій співпраці з ЄС, НАТО, США, Великою Британією, Канадою та Японією, особливо в обміні інформацією про загрози, проведенні багатонаціональних навчань, узгодженні нормативно-правових баз та колективному плануванні відновлюваності…

Нова модель України робить акцент на вбудованій стійкості: розподілені системи, що зменшують кількість точок відмови, відкриті стандарти, прозорі протоколи, постійні симуляції та навіть тренінги з психологічної стійкості для фахівців у сфері кібербезпеки, які працюють в умовах постійного тиску та інформаційної війни. У той час як Україна готує свою Національну стратегію кібербезпеки 2.0, очікується, що наступний етап реформ буде зосереджений на розширенні активної кіберзахисту, подальшому приведенні національного законодавства у відповідність до рамок ЄС, таких як NIS2, Рамка стійкості критичної інфраструктури та DORA, що сприятиме створенню ширшого європейського кіберщита, інвестуванні у розвиток кадрів відповідно до таких рамок, як NIST 2.0, зміцненні регіонального та місцевого кіберпотенціалу, а також визначенні чіткої правової та оперативної рамки на час війни для координації дій державного та приватного секторів під час збройних конфліктів та гібридних атак. Досвід України демонструє, що ефективна кібербезпека нерозривно пов’язана з управлінням, законодавством, освітою, дипломатією та економічною стійкістю, і пропонує не лише історію національного опору, а й практичну модель для майбутніх міжнародних конфліктів, де цифровий вимір буде неминучим і дедалі вирішальнішим». ***(Oleksandr Bakalynskyi, Maggie McDonough. Wartime Ukraine offers global lessons on the future of cyber resilience // Atlantic Council (https://www.atlanticcouncil.org/blogs/ukrainealert/wartime-ukraine-offers-global-lessons-on-the-future-of-cyber-resilience/). 19.03.2026).***

***

Світові тенденції в галузі кібербезпеки

«Згідно з новим дослідженням IANS, Artico Search та The CAP Group, звітування про кібербезпеку перед радами директорів компаній стало стандартною практикою: 95% керівників служб інформаційної безпеки (CISO)

регулярно надають оновлену інформацію. Однак ці взаємодії часто не мають стратегічної глибини; лише 25% засідань тривають понад 30 хвилин, а участь у них зазвичай є пасивною, оскільки ради директорів лише «отримують» інформацію, а не обговорюють її. Хоча директори загалом задоволені звітами про регуляторні тенденції, майже половина з них вважає, що CISO повинні покращити спосіб висвітлення впливу на бізнес нових загроз та ризиків, пов'язаних із штучним інтелектом. Як результат, лише 30% рад директорів описують свої відносини з CISO як міцні та співпраці. Експерти наголошують, що для усунення цієї прогалини CISO повинні перейти від базової звітності до створення на основі даних наративів, які пов'язують кіберризики з більш широкою бізнес-стратегією та рентабельністю інвестицій, тим самим задовольняючи попит ради директорів на перспективні аналітичні дані». ***(Ian Barker. Boards spend less than 30 minutes on cybersecurity // BetaNews, Inc. (https://betanews.com/article/boards-spend-less-than-30-minutes-on-cybersecurity/). 03.03.2026).***

***

«Загрози кібербезпеці зростають з тривожною швидкістю, проте багато організацій залишаються байдужими, розглядаючи безпеку як просту формальність, а не як критичну оперативну необхідність. Така недбалість, часто зумовлена бажанням забезпечити зручність для співробітників замість дотримання суворих протоколів, таких як багатофакторна автентифікація, виявляється надзвичайно дорогою, оскільки порушення безпеки даних обходяться в середньому в мільйони доларів по всьому світу. Ця вразливість зараз серйозно посилюється швидким розвитком штучного інтелекту (ШІ). ШІ кардинально змінює ландшафт загроз, уможливлюючи складні, автономні атаки безпрецедентного масштабу. Прикладами можуть бути шахрайські схеми з використанням глибоких підробок, які дозволяють успішно обманювати компанії на мільйони доларів, моделі ШІ, викрадені для автоматизованого кібершпигунства, та «кодування вібрацій», яке дозволяє некваліфікованим особам генерувати шкідливий код, просто даючи вказівки ШІ. На відміну від традиційних атак, що здійснюються людьми, ШІ може сканувати слабкі місця, адаптувати свою тактику в процесі операції та обходити стандартні засоби захисту з жахливою швидкістю…

Щоб боротися з новою ерою інтелектуальних загроз, що керуються машинами, компанії повинні негайно перейти від оборонної позиції до проактивної. Це вимагає інтеграції штучного інтелекту безпосередньо в їхні власні оборонні системи для виявлення та реагування на автономні атаки в режимі реального часу. Крім того, оскільки ці нові можливості ще не до кінця зрозумілі, необхідна надійна співпраця та обмін інформацією між приватним сектором, урядом та міжнародними партнерами. Зрештою, керівники корпорацій повинні відмовитися від самозаспокоєння; інструменти та стратегії для захисту від цих зростаючих загроз існують, але їх необхідно терміново та послідовно застосовувати, перш ніж організації опиняться в ситуації, коли їм доведеться боротися з майбутнім за допомогою застарілих методів». ***(Don Aviv, Sabrina Tan. Why Cybersecurity Threats Are Growing // TIME USA, LLC (https://time.com/7382979/cybersecurity-threats-are-growing/). 07.03.2026).***

***

«У сучасній кібербезпеці існує фундаментальна структурна проблема: керівники служб інформаційної безпеки (CISO) несуть відповідальність за зменшення ризиків, які вони не мали повноважень запобігати. Історично склалося так, що від служби безпеки очікували «власності» ризиків шляхом застосування заходів контролю після прийняття бізнес-рішень. Однак у сучасному динамічному та складному середовищі, де зловмисники швидко використовують вразливості організацій та залежність від третіх сторін, ця застаріла модель руйнується…

Основна проблема полягає в тому, що кіберризик створюється на етапі прийняття рішень, наприклад під час вибору постачальника або планування архітектури, а не під час впровадження. Проте питання безпеки зазвичай піднімається в цих дискусіях як другорядне, а його мета полягає лише в тому, щоб підтвердити або пом'якшити рішення, які вже є політично незворотними через виділені бюджети та терміни. Це ставить керівників служб інформаційної безпеки в неможливе становище, коли вони успадковують наслідки компромісів, на які не могли вплинути. Коли порушення неминуче відбувається, ради директорів зосереджуються на технічних несправностях, а не на недосконалому процесі прийняття рішень, який і спричинив ризик…

Щоб вижити в умовах сучасних загроз, організації повинні кардинально переглянути свою систему управління. Справжня кіберстійкість вимагає розподілу відповідальності, щоб керівники бізнесу несли відповідальність за ризики, які вони схвалюють, а також раннього впровадження заходів безпеки, щоб впливати на результати. Вирішення проблеми кібербезпеки полягає не в придбанні кращих технологій, а у встановленні чітких прав на прийняття рішень та узгодженні повноважень з відповідальністю до настання кризи». ***(Lara Joseph. Why Old Cybersecurity Models Are Breaking // IT Security Guru (https://www.itsecurityguru.org/2026/03/11/why-old-cybersecurity-models-are-breaking/). 11.03.2026).***

***

«Проводячи паралелі з серіалом Netflix «Дивні дива», сучасні загрози кібербезпеці, включаючи програми-вимагачі, кібервійни, що фінансуються державою, та атаки з використанням штучного інтелекту, «перевернули з ніг на голову» безпеку підприємств. Концепція «колективного розуму», представлена в серіалі, відображає те, як вразливі активи, такі як пристрої Інтернету речей та мережеве обладнання без оновлень, піддаються загрозі з боку ботнетів та просунутих постійних загроз (APT), таких як Salt Typhoon, які часто залишаються непоміченими, оскільки команди з безпеки не знають про їхнє існування в мережі. Так само, як герої серіалу відстежують лиходія за допомогою телеметрії, команди з кібербезпеки можуть використовувати мережевий трафік, системні журнали та дані про поведінку користувачів, які автоматично збираються та аналізуються за допомогою штучного інтелекту та машинного навчання, щоб виявляти підозрілу активність і отримувати раннє попередження про неминучі загрози, такі як атаки програм-вимагачів…

Підземні тунелі серіалу, що з'єднують світи, є аналогом того, як APT використовують викрадені облікові дані адміністратора для початкового доступу до мережі, а потім застосовують латеральний рух, щоб непомітно пересуватися по мережах, використовуючи пропущені системи, такі як HVAC та інтелектуальні пристрої IoT, що створюють критичні сліпі зони. Крім того, подвійне призначення ШІ відображається в сюжеті серіалу, де сили героя походять від лиходія: з моменту запуску ChatGPT такі організації, як OpenAI та Anthropic, підтвердили, що зловмисники використовують ШІ для кібератак, а найближчою загрозою 2026 року є автономні агенти ШІ, які здійснюють цілеспрямовані атаки та сканування вразливостей. Щоб протидіяти цьому, команди з кібербезпеки повинні впровадити агентні робочі процеси, щоб відповідати темпам цих автоматизованих загроз, надаючи пріоритет виявленню та усуненню вразливих пристроїв у всіх мережевих активах. Зрештою, захист підприємства вимагає скоординованих зусиль, спрямованих на уніфіковану видимість та контроль у всій зоні атаки». ***(Nadir Izrael. Stranger Things Meets Cybersecurity: Lessons from the Hive Mind // TechTarget, Inc. (https://www.darkreading.com/cybersecurity-operations/stranger-things-meets-cybersecurity-lessons-hive-mind). 04.03.2026).***

***

«…Хоча середня вартість порушення безпеки даних у світі в 2025 році знизилася на 9% до 4,44 млн доларів — головним чином завдяки штучному інтелекту та автоматизації, що скоротили терміни виявлення — ця цифра приховує розширення розриву між організаціями, які використовують широку автоматизацію, та тими, що покладаються на ручні процеси. Центри безпеки (SOC), які страждають від вигорання та величезних обсягів даних, все частіше впроваджують штучний інтелект. Однак це створює «парадокс автоматизації»: хоча штучний інтелект необхідний для обробки потоку даних, його неконтрольоване використання створює нові вразливості. IBM виявила, що «тіньовий штучний інтелект» (несанкціоноване використання генеративного штучного інтелекту) збільшив вартість порушень на 670 000 доларів, а переважна більшість організацій, що зазнали порушень, не мали належного контролю доступу до штучного інтелекту або політики управління. Ця відсутність управління перетворює технічну відповідальність на серйозну загрозу для дотримання нормативних вимог…

Крім того, «втома від сповіщень» залишається критичною проблемою, оскільки аналітики ігнорують до 30% сповіщень через їх великий обсяг і фрагментований контекст, що призводить до уповільнення часу локалізації та підвищення витрат на усунення порушень, особливо в складних інфраструктурах із декількома середовищами. Ця проблема ускладнюється жорсткістю регуляторного середовища в Європі, зокрема зближенням трьох основних рамок: DORA, яка вимагає швидкого повідомлення про інциденти фінансовим службам на рівні аудиту; NIS2, яка розширює відповідальність на такі сектори, як виробництво, і покладає особисту відповідальність на ради директорів; та Закон ЄС про штучний інтелект, який незабаром вимагатиме суворого управління ризиками та прозорості для інструментів штучного інтелекту з високим рівнем ризику, що використовуються в кібербезпеці…

Щоб орієнтуватися в цьому середовищі, галузь переходить до «керованої автономії» — моделі, в якій ШІ звужує простір для прийняття рішень аналітиками, одночасно автоматично генеруючи артефакти відповідності. За такого підходу кожне розслідування з питань безпеки неодмінно створює аудиторський слід, готовий до перевірки регуляторними органами. У міру того як ШІ еволюціонує від пасивних помічників до активних агентів, Gartner та лідери галузі наголошують на поступовому підході, що доповнює людський робочий процес, а не замінює його, щоб забезпечити ефективність та зрозумілість дій ШІ. Зрештою, успіх у 2026 році та в подальшому не залежатиме від наявності найсучаснішого ШІ, а від наявності надійного, підконтрольного ШІ, що вбудовує відповідність нормам безпосередньо в робочий процес виявлення та реагування». ***(Ana Maria Constantin. Why 2026 will be the year of governed cybersecurity AI // Cogneve, INC (https://thenextweb.com/news/why-2026-will-be-the-year-of-governed-cybersecurity-ai). 10.03.2026).***

***

«Згідно з дослідженням ISC2 «2025 Cybersecurity Workforce Study», десятирічні зусилля галузі кібербезпеки, спрямовані на залучення більшої кількості жінок та усунення дефіциту кадрів, здається, приносять свої плоди. Опитування, в якому взяли участь приблизно 2500 жінок (16% від загальної кількості респондентів), показало, що 72% жінок вважають кібербезпеку привабливою сферою кар'єри, а їхній середній рівень задоволеності роботою зріс з 67% у 2024 році до 71% у 2025 році. Однак виклики залишаються: жінки частіше, ніж чоловіки, повідомляли про нещодавні звільнення з посад у сфері безпеки (28% проти 23%) і виявляли дещо менший оптимізм щодо довгострокової перспективи професії, причому 33% розглядали можливість зміни кар'єри через ринкові умови, порівняно з 27% чоловіків. Сприйняття представництва жінок у командах залишилося відносно незмінним: 14% респондентів повідомили, що в їхніх командах немає жінок, а 24% вказали, що в їхніх командах гендерна рівність досягла або майже досягла рівноваги…

Дослідження виявило значні розбіжності в сприйнятті між статями щодо перешкод для просування жінок. Жінки назвали головними перешкодами баланс між роботою та особистим життям/догляд за дітьми (45%), обмежені можливості для лідерства (35%) та нерівність в оплаті праці (34%), тоді як 42% чоловіків заявили, що не знають і не помічають жодних значних перешкод. Незважаючи на ці виклики, розвиток штучного інтелекту (ШІ) відкриває значні можливості; понад 40% усіх учасників вважають знання ШІ критично важливою навичкою, і, що примітно, жінки частіше за чоловіків заявляли про «значні» знання в галузі ШІ та машинного навчання (27% проти 17%). Обидві статі активно прагнуть розвивати свої навички, приділяючи особливу увагу загальним навичкам у галузі кібербезпеки та знанням ШІ. Для підтримки постійного зростання ISC2 наголошує на важливості безперервної освіти та заохочує використання як формальних, так і неформальних мереж наставництва, відзначаючи, що майже половина опитаних жінок вже має доступ до таких груп колег». ***(Claire Meyer. Is Cybersecurity a Welcoming Career? 72 Percent of Female Cyber Practitioners Say Yes // ASIS***

International (https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2026/march/women-in-cybersecurity/). 09.03.2026).

***

«Людська помилка залишається головним фактором ризику для безпеки, навіть попри зростання загроз, пов'язаних зі штучним інтелектом. Згідно з доповіддю Mimecast «Стан людського ризику», 42% організацій повідомили про збільшення кількості як зловмисних інцидентів з боку співробітників, так і випадків недбалості за останній рік — це історична рівність, що свідчить про зміну, коли навмисне зрадництво співробітників тепер конкурує з випадковими помилками як головна проблема. Кількість повідомлень про зловмисні дії інсайдерів зросла майже на 10 процентних пунктів за два роки — з 33% у 2024 році до 42% у 2026 році. Фінансові збитки є значними: організації щомісяця стикаються в середньому з шістьма інцидентами, спричиненими інсайдерами, з оціночною вартістю 13,1 млн доларів США за кожен інцидент, причому 66% очікують, що втрата даних, пов'язана з інсайдерами, зросте в наступному році. Зловмисники все частіше використовують інсайдерів як навмисні точки входу для обходу периметральної оборони, а ризик посилюється штучним інтелектом, який полегшує витік даних у великих обсягах як для зловмисних інсайдерів, так і для зовнішніх акторів, що використовують соціальну інженерію…

Поверхня атаки розширюється, оскільки співробітники працюють з електронною поштою, платформами генеративної штучного інтелекту та інструментами для співпраці, проте вбудовані засоби контролю безпеки відстають: 38% організацій покладаються на них виключно для інструментів співпраці, незважаючи на те, що 64% визнають їх недостатніми. Штучний інтелект стає мультиплікатором сили — 69% керівників служб безпеки стверджують, що атаки на основі штучного інтелекту є неминучими протягом 12 місяців, проте 60% не готові до них повністю. Тим часом 91% організацій намагаються підтримувати управління та відповідність вимогам щодо даних комунікацій, а 59% не впевнені в тому, що зможуть швидко знайти дані для виконання нормативних вимог… Небезпечна іронія підриває захист: 65% вважають інтеграцію засобів безпеки занадто складною, тоді як зловмисники безперешкодно використовують прогалини між роз'єднаними засобами контролю. Лише 28% організацій поєднують регулярне навчання з питань безпеки з постійним моніторингом, тому коли поведінкова аналітика виявляє користувача з високим рівнем ризику, ця інформація часто не викликає скоординованих дій з боку засобів контролю доступу та запобігання втраті даних. Ті, хто все ж інтегрує ці засоби, повідомляють про значні переваги: 40% досягають швидшого усунення загроз, всебічної видимості та покращеної готовності до дотримання вимог.

Шлях вперед вимагає усунення ризиків для людей у момент дії — у поштових скриньках, робочих процесах та щоденних рішеннях — за допомогою інтегрованої видимості у всіх каналах комунікації, поведінкової аналітики, що сприяє вимірюваним змінам у поведінці з точки зору безпеки, управління даними, що захищає конфіденційну інформацію незалежно від її розташування, та скоординованої реакції, що поєднує засоби контролю, орієнтовані на людей та

технології». ***(Elizabeth Greenberg. Negligence Stirring Rise in Cyber Incidents // DIGIT (https://www.digit.fyi/negligence-stirring-rise-in-cyber-incidents/). 06.03.2026).***

***

«Supremus Group випустила набір шаблонів планів реагування на інциденти кібербезпеки — комплексний пакет документації, призначений допомогти організаціям швидко створити або модернізувати офіційну, повторювану систему реагування на інциденти на основі стандарту NIST SP 800-61. Визнаючи, що кіберінциденти є бізнес-подіями, які впливають на операції, юридичну відповідальність та прийняття рішень керівництвом, набір має на меті узгодити дії IT-, юридичних та керівних команд до настання кризи. Цей пакет, готовий до використання та зручний для аудиту, містить приблизно 80 документів, включаючи 16 основних шаблонів, таких як плани управління реагуванням, процедури, повідомлення про тривоги та плани вдосконалення після інцидентів, які забезпечують єдиний шлях від управління до виконання, заощаджуючи організаціям сотні годин порівняно з розробкою програми з нуля…

Ключовою особливістю цього пакету є включення 63 документів із сценаріями, що охоплюють 21 реальний інцидент, таких як програмне забезпечення для вимагання викупу, компрометація ділової електронної пошти, крадіжка даних зсередини та компрометація сторонніх постачальників. Кожен сценарій включає готовий приклад, шаблон для заповнення та контрольний список, що дозволяє командам моделювати реалістичні робочі процеси та швидко налаштовувати посібники. Крім того, впровадження цього задокументованого плану реагування на інциденти може значно допомогти організаціям продемонструвати «готовність до кіберстрахування» під час обговорення умов страхування, що є загальною вимогою для забезпечення страхового покриття. Пакет також можна поєднати з тренінгом Supremus Group «Відповідальне використання штучного інтелекту, ризики та обізнаність», щоб допомогти організаціям управляти ризиками, пов'язаними з використанням інструментів штучного інтелекту». ***(Cyber Security Incident Response Plan Template Suite with 80 Documents Available Now // National Law Forum, LLC (https://natlawreview.com/press-releases/cyber-security-incident-response-plan-template-suite-80-documents-available). 10.03.2026).***

***

«Сучасні організації стикаються з безпрецедентним викликом: управління розгалуженими, фрагментованими інфраструктурами, які переросли традиційну периметральну безпеку. Впровадження хмарних технологій, віртуалізація, контейнеризація та дистанційна робота розмили колись чіткі межі корпоративної мережі, замінивши їх на мінливі екосистеми локальних і хмарних серверів, пристроїв IoT, платформ SaaS та віддалених пристроїв співробітників. Кожне нове підключення розширює площу атаки та збільшує ймовірність виникнення сліпих зон. 97% великих підприємств повідомляють, що зазнали мережевих атак, за ними йдуть 88% малих і середніх підприємств та 83% малих і середніх бізнесів, проте більшість організацій продовжують боротися з проблемою видимості, незважаючи на мільйонні витрати на IT-безпеку… Основна

проблема полягає в тому, що сучасні гетерогенні інфраструктури, побудовані на основі декількох технологічних стеків, постачальників і регіонів для забезпечення гнучкості та продуктивності, генерують фрагментовану телеметрію з несумісних джерел, залишаючи навіть зрілі підприємства з «темними» кутами. Неконтрольований зашифрований трафік, неправильно налаштовані брандмауери, неактивні облікові записи та забуті сервери стають відкритими дверима для зловмисників, які можуть проникнути та переміщатися непоміченими. В результаті захисники не можуть відповісти на основні питання щодо реагування на інциденти: що, коли, де та як сталися порушення, що подовжує час реагування та збільшує збитки…

Справжня видимість виходить за межі збору необроблених даних і охоплює інтерпретацію в режимі реального часу та реконструкцію історичних даних. Телеметрія мережі часто стає єдиним доказом після того, як зловмисники видаляють журнали, що робить її критично важливою як для криміналістичного аналізу, так і для запобігання. Для її досягнення необхідно моніторити трафік на всіх рівнях — вхідні та вихідні потоки і внутрішні поперечні переміщення — одночасно співвідносячи дані кінцевих точок з пасивним аналізом мережі, щоб сформувати цілісну картину, незважаючи на обмеження продуктивності застарілих систем… Видимість — це не одноразовий проект, а постійна дисципліна, яка розглядає інфраструктуру як екосистему, що постійно розвивається, інтегруючи інформацію про кінцеві точки, мережі та додатки за допомогою SIEM, XDR або спеціальних інструментів виявлення. У світі гібридних архітектур і шифрування сліпі зони неминучі, але ті, хто інвестує в те, щоб бачити не тільки те, що відбувається, але й чому, — саме вони запобігають порушенням, а не просто реагують на них». ***(Alexander Rumyantsev. Seeing the unseen: Why full visibility is the cornerstone of cyber defense // TNGlobal (https://technode.global/2026/03/11/seeing-the-unseen-why-full-visibility-is-the-cornerstone-of-cyber-defense/). 11.03.2026).***

***

«Оскільки кібервійна все частіше стає основним інструментом у геополітичних конфліктах, про що свідчать постійні напруження між такими країнами, як Ізраїль та Іран, компанії по всьому світу стикаються із значним ризиком стати побічною жертвою, тому їм необхідно посилювати свою IT-інфраструктуру. Щоб зменшити ці ризики, організації повинні прийняти комплексну стратегію кібербезпеки. Основоположним кроком є впровадження визнаних стандартів, таких як ISO 27001 або NIST Cybersecurity Framework, для систематичного виявлення вразливостей та встановлення чітких політик щодо захисту даних і контролю доступу. Крім того, важливе значення має сегментація мережі: ізолюючи критично важливі системи (такі як фінансові бази даних або операційні технології) від загальних мереж, компанії можуть обмежити потенційний збиток від порушення, а регулярне оновлення програмного забезпечення зміцнює загальну інфраструктуру…

Оскільки людська помилка є поширеною точкою входу для зловмисників, регулярне навчання співробітників розпізнаванню фішингу та соціальної інженерії

є необхідним для створення надійної першої лінії захисту. З технологічної точки зору, компанії повинні інвестувати в передові засоби виявлення загроз та інструменти безперервного моніторингу, такі як системи SIEM та безпека на основі штучного інтелекту, щоб виявляти та мінімізувати ненормальну активність у режимі реального часу. Підготовка також повинна включати надійний план реагування на інциденти та відновлення після аварій, що доповнюється регулярними навчаннями та безпечними офлайн-резервними копіями, щоб забезпечити швидке відновлення роботи після атаки. Нарешті, співпраця з урядовими установами та галузевими мережами з метою обміну інформацією про загрози може проактивно підвищити стійкість компанії, гарантуючи, що кібербезпека залишається основною бізнес-стратегією в сучасному нестабільному цифровому середовищі». ***(Naveen Goud. How businesses can protect their IT infrastructure from Cyberwarfare // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/how-businesses-can-protect-their-it-infrastructure-from-cyberwarfare/). 12.03.2026).***

***

«У сучасному світі, де кіберзагрози постійно еволюціонують, постійний моніторинг і швидке реагування є необхідними для організацій, щоб запобігти серйозним інцидентам безпеки. Оскільки загрози часто проявляються у вигляді неявних індикаторів у різних системах, сучасні платформи безпеки, такі як Endpoint Detection and Response (EDR) та Security Information and Event Management (SIEM), мають вирішальне значення для кореляції сповіщень, виявлення підозрілої поведінки та виявлення компрометації, перш ніж зловмисники зможуть закріпитися…

Цей процес можна проілюструвати на прикладі реальної ситуації: під час рутинного моніторингу за допомогою платформи SentinelOne було виявлено попередження про шкідливе програмне забезпечення на кінцевому пристрої підприємства, в якому було ідентифіковано файл з назвою «eicar.com», класифікований з високою вірогідністю як шкідливий. Файл EICAR насправді є нешкідливим стандартизованим тестовим файлом, який використовується спільнотою кібербезпеки для перевірки функціональності антивірусних систем. Однак його наявність у виробничому середовищі все одно вимагала негайного розслідування, щоб виключити несанкціоноване зондування або шкідливу діяльність. Команда з безпеки швидко проаналізувала журнали кінцевих точок, активність системи та поведінку користувачів, підтвердивши, що файл не становив активної загрози і не спричинив жодних шкідливих дій…

Цей сценарій підкреслює, чому швидке розслідування є критично важливим, навіть якщо тривога виявляється помилковою. Воно дозволяє командам безпеки підтримувати видимість, розрізняти законні тестування та атаки на ранній стадії, а також запобігати потенційному поширенню шкідливого програмного забезпечення. Зрештою, цей інцидент підкреслює необхідність багаторівневої стратегії кібербезпеки, яка поєднує моніторинг кінцевих точок з регулярною оцінкою вразливостей, оновленою інформацією про загрози, ефективним управлінням та обізнаністю персоналу з питань безпеки, що дозволяє організаціям підтримувати

стійку оборону проти зростаючого спектру загроз». ***(Aniket Gurao. Real Attack Alert Analysis: Strengthening Organizational Cyber Defense Through Early Detection // Techstrong Group Inc. (https://securityboulevard.com/2026/03/real-attack-alert-analysis-strengthening-organizational-cyber-defense-through-early-detection/). 09.03.2026).***

***

«Глобальний ринок кібербезпеки в оборонній сфері, оцінений у 37,23 млрд доларів США у 2024 році, за прогнозами, зросте до 66,89 млрд доларів США до 2032 року із середньорічним темпом зростання 7,6%, що зумовлено нагальною потребою урядів і військових організацій у захисті взаємопов'язаної цифрової інфраструктури від дедалі більш витончених кібератак і шпигунства. У зв'язку з тим, що сучасні збройні сили швидко впроваджують хмарні обчислення, штучний інтелект та автономні платформи, захист комунікаційних мереж, систем управління та секретних даних став критично важливим пріоритетом національної безпеки. Щоб протидіяти зростаючій геополітичній напруженості та загрозі кібервійни, оборонні відомства інвестують значні кошти в передові технології, такі як архітектура нульової довіри, виявлення загроз на основі штучного інтелекту та надійні системи шифрування…

Ринок є висококонкурентним, на ньому домінують великі оборонні підрядники та постачальники технологій, такі як Raytheon, Lockheed Martin, BAE Systems та General Dynamics, які розширюють свої можливості за допомогою стратегічних партнерств, придбань та урядових контрактів. Серед останніх значних подій можна відзначити впровадження Seekr штучного інтелекту для армії США з метою виявлення вразливостей систем озброєння, контракт General Dynamics на архітектуру нульової довіри та роботу Leidos у сфері кібербезпеки для АНБ. У географічному розрізі Північна Америка лідирує на ринку з часткою 40%, що зумовлено величезними оборонними бюджетами та передовими програмами, за нею йдуть Європа (25%) та Азіатсько-Тихоокеанський регіон (23%), де прискорюється військова модернізація та цифровізація. Загалом, кібербезпека в оборонній сфері переходить від спеціалізованої IT-функції до фундаментального елементу сучасної військової готовності та глобальної стратегічної оборони». ***(Defense Cybersecurity Market to Reach US$66.89 Billion by 2032 at 7.6% CAGR; North America Leads with 40% Share - Key Players: Raytheon Technologies, Lockheed Martin, Northrop Grumman // openPR (https://www.openpr.com/news/4421600/defense-cybersecurity-market-to-reach-us-66-89-billion-by-2032). 12.03.2026).***

***

«Глобальна коаліція з телекомунікацій (GCOT), до складу якої спочатку входили Австралія, Канада, Японія, Великобританія та США, а нещодавно приєдналися Фінляндія та Швеція, оприлюднила набір добровільних принципів кібербезпеки та стійкості для майбутнього покоління мобільних мереж 6G. Ці рекомендації, оприлюднені на Mobile World Congress 2026 за підтримки таких великих гравців галузі, як AT&T, Ericsson, NVIDIA та Vodafone,

мають на меті вплинути на стандартизацію 6G задовго до її очікуваного комерційного впровадження в 2029-2030 роках. Базуючись на прогнозі, що 6G буде мати високовіртуалізовані функції, дезагреговані архітектури та вбудовану підтримку штучного інтелекту, GCOT встановила чотири принципи безпеки та чотири принципи стійкості для захисту від кібер- та фізичних загроз…

Основні цілі вимагають, щоб системи 6G забезпечували локалізацію (обмеження зловмисного поширення), конфіденційність (захист конфіденційності даних користувачів за рахунок конструкції), цілісність (гарантія незмінності даних та інфраструктури) та вимірювану стійкість (підтримка доступності послуг, особливо для служб екстреної допомоги, під час перебоїв), а також дотримання нормативних вимог. Крім того, GCOT наголошує на необхідності надійних механізмів відмовостійкості, альтернативних рішень для позиціонування та синхронізації, що виходять за межі GNSS, для запобігання перешкодам у сигналі, а також на необхідності впровадження відкритих платформ RAN для забезпечення взаємодії. Лідери галузі, серед яких представники Virgin Media O2, NVIDIA та Ericsson, високо оцінили ініціативу щодо впровадження фундаментальних заходів захисту та мінімізації ризиків з самого початку, підкресливши необхідність державно-приватного партнерства для побудови безпечної, орієнтованої на штучний інтелект та готової до майбутнього національної інфраструктури». ***(Kevin Poireault. Coalition of Western Countries Launches 6G Cybersecurity Guidelines // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news/gcot-6g-cybersecurity-guidelines/). 04.03.2026).***

***

«У той час як глобальні організації борються з невпинним зростанням кількості кіберзагроз — зокрема фішингу, шкідливого програмного забезпечення та витончених «діпфейків» — керівники інформаційних служб (CIO) та керівники служб інформаційної безпеки (CISO) дедалі частіше застосовують передові стратегії для зміцнення своїх планів розвитку кібербезпеки. Згідно з даними ESET Telemetry, хоча загальна кількість виявлених загроз в Індії зменшилася на 12 % у період з січня по серпень 2025 року (що свідчить про успіх заходів раннього запобігання), серйозність окремих атак зросла…

Варто зазначити, що кількість виявлених випадків використання програм-вимагачів в Індії зросла на 70 % у період з другої половини 2024 року до першої половини 2025 року, а фішинг залишається найпоширенішою загрозою. Роман Ковач, головний науковий співробітник ESET, підкреслює, що зловмисники використовують штучний інтелект для підвищення ефективності цих традиційних тактик, а також все частіше націлюються на незахищені периферійні системи та пристрої за допомогою експлойтів «нульового дня». Зростаюча складність розрізнення справжнього та підробленого контенту ще більше ускладнює ситуацію з загрозами, пов’язаними зі штучним інтелектом. Щоб боротися з цим, організації — особливо великі підприємства у секторах BFSI, виробництва, гірничодобувної промисловості та енергетики — звертаються до комплексних розвідданих про загрози, послуг керованого виявлення та реагування (MDR) та безпосередніх

консультацій з аналітиками. Ковач наголошує, що для того, щоб орієнтуватися у подвійних можливостях та викликах, які представляє штучний інтелект, керівники IT-підрозділів повинні бути в курсі подій та налагоджувати довгострокові партнерські відносини з технічно компетентними постачальниками послуг з кібербезпеки». ***(Yogesh Gupta. Threat intelligence by ESET is a game changer // FoundryCo, Inc. (https://www.csoonline.com/article/4143209/threat-intelligence-by-eset-is-a-game-changer.html). 10.03.2026).***

***

«Кібербезпека стала одним із основних фінансових ризиків, а не лише проблемою IT-сфери, і кредитори тепер ставляться до неї так само, як до кредитного, операційного чи юридичного ризику, оцінюючи позичальників із числа портфельних компаній. Ключовим питанням для кожної угоди є те, чи може кіберінцидент завадити обслуговуванню боргу, порушити операційну діяльність або знизити вартість активів та гудвіл. Це робить проактивну оцінку перед фінансуванням надзвичайно важливою: попередні умови дедалі частіше включають затверджені радою директорів кіберполітики, плани реагування на інциденти та забезпечення безперебійної діяльності, гарантії від критично важливих сторонніх постачальників та докази наявності відповідного кіберстрахування…

Члени ради директорів повинні розглядати питання кібербезпеки як частину своїх статутних обов’язків, здійснюючи активний нагляд за ризиками, управлінням та інвестиціями у забезпечення стійкості. Від ради директорів очікується, що вона буде ставити під сумнів дії керівництва щодо готовності до інцидентів, вразливостей ланцюгів постачання, управління даними, можливостей відновлення, а також того, чи відповідають тестування, навчання та ресурси фінансовим ризикам. У разі атаки доходи можуть знизитися, витрати зрости, а резерви за угодами можуть бути вичерпані; кредитори ретельно перевірятимуть перехресні дефолти, тригери платоспроможності та ефект доміно в ланцюгах постачання. Страхування не є панацеєю — покриття часто не включає втрачений прибуток, а умови полісу можуть вимагати дострокового погашення боргу — тому надійні механізми повідомлення, регулярна звітність щодо ризиків та зобов’язання, що стосуються саме кібербезпеки, є більш надійними інструментами, ніж покладання на загальні положення про істотні негативні наслідки…

Недавні інциденти підкреслюють серйозність ситуації: компанія Marks & Spencer прогнозує, що кібератака 2025 року призведе до втрати операційного прибутку на суму близько 300 мільйонів фунтів стерлінгів, а інцидент, що стався у 2025 році з Jaguar Land Rover, змусив компанію зупинити роботу заводів і спричинив значні збитки. На цьому тлі фінансова документація стає все більш жорсткою. Позичальники повинні очікувати: (i) більш суворих попередніх умов щодо кіберготовності; (ii) зобов'язань щодо оперативного повідомлення про порушення, постійного інформування про загрози та вжиття заходів з усунення наслідків; (iii) індивідуальних зобов'язань, що вимагають дотримання визначених заходів кіберконтролю та своєчасного усунення наслідків інцидентів; та (iv) вимог щодо підтвердження наявності надійних резервних копій, тестування відновлення

після аварій та заходів захисту цифрових активів та інтелектуальної власності. Кредитори також все більше уваги приділяють тому, як використовуються кошти від кіберстрахування — часто наполягаючи на праві попередньої оплати — тому позичальникам потрібно домовлятися про можливість утримання коштів, необхідних для відновлення та реінвестицій. Загалом, розгляд кіберстійкості як невід'ємної частини кредитоспроможності та оцінки вартості зараз є важливою складовою стратегії фінансування». ***(Nick Stubbs. Cyber risk and debt facilities considerations for lenders and borrowers // Walker Morris LLP (https://www.walkermorris.co.uk/newsletters/newsletter-items/cyber-risk-and-debt-facilities-considerations-for-lenders-and-borrowers/). 02.03.2026).***

***

«…Захищати мережі структурно складніше, ніж атакувати їх, оскільки захисники повинні бути правими завжди, тоді як зловмисникам достатньо досягти успіху лише один раз — і більшість захисників починають діяти занадто пізно, вважаючи, що атака починається з попередження EDR, успішного фішингу або використання вразливості. Насправді серйозні порушення майже завжди починаються з наміру та розвідки: пасивного OSINT для картографування дочірніх компаній, ключового персоналу, просторів імен DNS, витоків облікових даних та форматів електронної пошти; аналізу дампів порушень; збору даних з LinkedIn; і навіть використання глобальних баз даних сканування, таких як Shodan або Censys, замість безпосереднього контакту з ціллю. Ця фаза розвідки «до вибуху» майже повністю невидима для традиційної телеметрії безпеки, яка закінчується на периферії, залишаючи організації в невіданні щодо того, як зловмисники виявляють забуті кінцеві точки UAT, не виведені з експлуатації VPN без MFA, відкритий вихідний код або резервні копії, неправильно налаштовані сховища або великі списки електронної пошти, що піддаються атакам… До моменту початку активного зондування та експлуатації вразливостей — розсилки паролів, веб-фузингу, сканування вразливостей — зловмисник часто вже має чітку карту слабких місць, а виявлення зазвичай відбувається лише після того, як у гру вступають численні облікові дані, плацдарми та горизонтальні переміщення. Агентний ШІ погіршує ситуацію: моделі вже здійснюють реверс-інжиніринг патчів, генеруючи експлойти для критичних CVE швидше, ніж більшість команд встигають випустити патчі, та дозволяють зловмисникам з низьким рівнем кваліфікації автоматизувати розвідку та масове використання вразливостей, скорочуючи вікно реагування захисників…

Очевидним є питання, чи можуть захисники втрутитися раніше, формуючи те, що бачать зловмисники під час розвідки. Історія, військова практика та біологія вказують на те, що відповідь — так: контррозвідка та обман — відволікання уваги, приманки, маскування — це перевірені часом способи збивати з пантелику супротивників, перш ніж вони досягнуть реальних цілей. У сучасному хмарному контексті це означає навмисне заповнення вашого периферійного та DNS-простору реалістичними, але фальшивими ресурсами — сервісами, кінцевими точками та обліковими даними з дійсними сертифікатами та привабливими назвами — які не виконують жодних бізнес-функцій, а існують лише для того, щоб привернути увагу

зондувань та атак. Будь-яка взаємодія з цими приманками стає високоточним сигналом про ворожу розвідку або випадкове сканування, що дозволяє вам блокувати та реєструвати активність, перш ніж вона торкнеться виробничої інфраструктури… Оскільки зловмисники, що діють за нагодою, прочісують весь Інтернет, а не вистежують конкретні організації, ймовірність того, що вони потраплять у пастку, така ж висока, як і ймовірність потрапити на справжній сервіс — а за наявності достатньої кількості приманки навіть вища. Саме на цьому базується принцип роботи Divert: розгортання на рівні DNS та розміщення приманкових сервісів і облікових даних по всій поверхні атаки, щоб перехоплювати загрози ще на етапі розвідки. Зловмисники мусять оминати кожну приманку; захисникам достатньо лише одного влучання. Кожне сповіщення відповідає заблокованій спробі, без необхідності очищення скомпрометованих систем і без помилкових спрацьовувань, що зміщує асиметрію на користь захисників, перетворюючи саму розвідку на контрольовану точку оборонного зіткнення, а не на невидиму прелюдію до компрометації». ***(Staying Left of "Bang" - Stopping Threats at Recon // HALOCK (https://www.halock.com/staying-left-of-bang-stopping-threats-at-recon/). 03.2026).***

***

«Під час нещодавнього круглого столу в Лондоні, організованого компаніями Ropes & Gray та FTI Consulting, фахівці з приватного капіталу (PE) обговорили зростаючі загрози кібербезпеці, з якими їхня галузь зіткнеться у 2026 році… Компанії приватного капіталу та їхні портфельні компанії є головними цілями зловмисників, оскільки їхня діяльність поєднує в собі великі угоди, конфіденційні дані та стрімке зростання. Зловмисники активно стежать за ринком, часто приурочуючи кампанії з використанням програм-вимагачів до угод злиття та поглинання, коли керівництво відволікається, а системи стають вразливими через процеси інтеграції…

Ця загроза посилюється завдяки штучному інтелекту, який знизив бар'єр для вторгнення хакерів. Інструменти штучного інтелекту масово генерують досконало відпрацьовані, персоналізовані фішингові листи та спроби соціальної інженерії, що ускладнює їх виявлення, а також прискорює виявлення вразливостей і проникнення в мережі. Відповідно, приватні інвестиційні компанії повинні посилити свої захисні заходи за допомогою передових засобів виявлення, більш надійного управління доступом та сучасних навчальних програм…

Одним із ключових питань, що обговорювалися, було забезпечення постійної зацікавленості ради директорів у питаннях кібербезпеки, а не розгляд їх як проблеми, на яку реагують лише після виникнення. Учасники наголосили на необхідності чіткого визначення відповідальності за кіберризики, щоб забезпечити їх пріоритетність, особливо під час виходу з інвестицій, коли виявлення вразливостей може ускладнити продаж. Для протидії цим мінливим ризикам під час обговорення було виділено три пріоритети для спонсорів приватного капіталу: регулярне стрес-тестування планів реагування на інциденти, підвищення рівня кібер-ділігенсу до рівня фінансового ділігенсу протягом усього життєвого циклу угоди та впровадження послідовних, кількісно вимірюваних систем звітності для

ефективного інформування інвестиційних комітетів про кіберризики». ***(Edward Machin. Safeguarding the Portfolio: Incident Readiness and the Cyber Landscape in 2026 // Ropes & Gray LLP (https://www.ropesgray.com/en/insights/viewpoints/102mmkj/safeguarding-the-portfolio-incident-readiness-and-the-cyber-landscape-in-2026). 11.03.2026).***

***

«У новому звіті компанії Intruder під назвою «Security Middle Child Report» стверджується, що компанії середнього бізнесу — які визначаються як підприємства з доходом приблизно від 50 мільйонів доларів і штатом від 400 до 6 000 співробітників — не отримують належної уваги з боку ринку постачальників кібербезпеки, через що багато з них опиняються в ситуації «проблеми середнього бізнесу в сфері безпеки». Майже половина керівників служб безпеки заявляє, що їм бракує інструментів, які відповідають їхнім потребам: 46% вважають корпоративні платформи занадто дорогими або складними для своїх команд, тоді як 29% зазначають, що інструменти для малого бізнесу вже не відповідають вимогам. Як наслідок, 42% описують свої команди як перевантажені, перенапружені або відстаючі, а 44% заявляють, що їхні системи безпеки або застаріли, або фрагментовані, що призводить до надмірної кількості інструментів, надмірної кількості сповіщень із неправильно визначеними пріоритетами та недостатньої видимості вразливостей…

Хоча більшість респондентів повідомляють про збільшення бюджетів і багато хто впевнений у своїй здатності виявляти та усувати критичні ризики, ця впевненість різко знижується, чим ближче респонденти до повсякденної операційної діяльності, що свідчить про розбіжність у поглядах керівництва та практиків. У звіті також зазначається, що цифрові активи розширюються швидше, ніж команди встигають за ними: 91% респондентів стверджують, що їхні середовища зросли за останні два роки, але лише 30% збільшили штат швидше, ніж відбувалося це зростання, тоді як 36% визнають, що їхній рівень безпеки не масштабувався належним чином…

Багато організацій замість найму персоналу звертаються до штучного інтелекту та автоматизації, проте впровадження цих технологій, як видається, зосереджено серед великих компаній із значними ресурсами, що викликає сумніви щодо того, чи справді ці інструменти полегшують навантаження на найменші команди. Водночас питання кіберризиків рідко доходять до рівня ради директорів: лише 9 % компаній розглядають їх на цьому рівні. Загалом, Intruder робить висновок, що підприємства середнього бізнесу є занадто великими для інструментів, призначених для малого та середнього бізнесу, занадто обмеженими для корпоративних платформ і все більше наражаються на ризики, оскільки їхні середовища розвиваються швидше, ніж їхні співробітники, процеси та структури прийняття рішень». ***(Eve Goode. Intruder releases its latest cybersecurity report // Centurian Media Ltd (https://securityjournaluk.com/intruder-latest-cybersecurity-report/). 18.03.2026).***

***

«Постачальники послуг з кібербезпеки можуть стати мішенню тих самих атак, яким вони допомагають запобігати своїм клієнтам, і злом їхніх систем може завдати особливо серйозної шкоди, оскільки ці постачальники знаходяться всередині довіреного рівня інфраструктури клієнта. Нещодавнім прикладом стала високотехнологічна фішингова атака на керівника вищого рівня в компанії Outpost24, яка була розроблена з метою обійти засоби захисту корпоративної електронної пошти, не викликаючи тривоги. Приманкою виявилося переконливе фінансове повідомлення від JP Morgan, представлене як частина поточного ланцюжка листів, яке пройшло перевірку автентичності, оскільки містило дійсний підпис DKIM, пов'язаний із службою Amazon Simple Email Service…

Звідти зловмисники «пропустили» жертву через складний семиступеневий ланцюжок перенаправлень, який використовував авторитетні та легітимні сервіси, щоб виглядати безпечним, зокрема домен Cisco для перенаписання та перевірки посилань і платформу Nylas для роботи з електронною поштою, а потім перенаправляв через PDF-файл зламаної індійської компанії-розробника програмного забезпечення, перереєстрований домен, термін дії якого раніше закінчився, і, нарешті, на шкідливий сайт, прихований за Cloudflare; були використані заходи проти ботів та перевірки на людську присутність, щоб заблокувати автоматизовані сканери та показувати сторінку входу в Microsoft Office для збору облікових даних лише реальним користувачам…

Команда Outpost24 з аналізу загроз виявила цю спробу до того, як було завдано шкоди, і встановила зв’язок між використаними інструментами та набором «фішинг як послуга» Kratos, хоча через швидке демонтаж інфраструктури їй не вдалося прив’язати цю активність до конкретної групи. Аналітики зазначили, що хоча зміст електронного листа був типовим, стійка багаторівнева інфраструктура свідчила про цілеспрямовані зусилля з обходу засобів контролю, що підкреслює: жодна окрема система захисту не зможе виявити все, і організаціям потрібна багаторівнева система безпеки на основі принципу «нульової довіри», щоб викрадені облікові дані самі по собі не надавали значного доступу. Цей інцидент також висвітлює ширшу проблему ризиків, пов’язаних із постачальниками: окрім безпеки продуктів та переліків вимог щодо відповідності, найбільшою небезпекою може бути рівень привілейованого доступу та неявна довіра, яку отримують постачальники після інтеграції в повсякденну діяльність». ***(Jai Vijayan. Hackers Target Cybersecurity Firm Outpost24 in 7-Stage Phish // TechTarget, Inc. (https://www.darkreading.com/threat-intelligence/hackers-target-cybersecurity-firm-outpost24-phish). 17.03.2026).***

***

«Нове дослідження компанії Kroll виявляє значний розрив між тим, як організації оцінюють свою готовність до кіберзахисту, та їхньою фактичною здатністю захищатися від атак і відновлюватися після них. Опитування 1 000 осіб, які приймають рішення у сфері кібербезпеки по всьому світу, показало, що, хоча кіберризики визнаються на рівні керівництва (94 % респондентів вважають їх основним ризиком для бізнесу), часто спостерігається невідповідність між

заходами з безпеки та більш загальними пріоритетами бізнесу. Хоча 99% організацій мають план реагування на інциденти, лише 3% оновлюють його після інциденту, що свідчить про те, що ці плани часто є статичними, а не оперативними. Ця невідповідність є критичною, оскільки «час прориву» зловмисників може становити всього 29 хвилин, тоді як 72% респондентів вважають, що можуть відреагувати протягом 24 годин…

Дослідження також виявило невідповідності у розподілі бюджетних коштів. Незважаючи на зростання бюджетів на кібербезпеку, напрямки інвестицій не завжди відповідають найпоширенішим загрозам, таким як фішинг та компрометація ділової електронної пошти. Що шокує, понад половина респондентів повідомила про скорочення або зниження пріоритетності превентивних заходів, таких як «червона команда» та архітектура «нульової довіри». Це свідчить про реактивний, формальний підхід до безпеки, який часто не привертає уваги керівництва, доки не трапляється серйозне порушення роботи бізнесу. У звіті зроблено висновок, що організації повинні посилити свої базові заходи безпеки, покращити визначення пріоритетності загроз та краще узгодити свою кіберстратегію з оперативними реаліями, щоб створити справжню стійкість у дедалі більш нестабільному середовищі загроз…» ***(Joseph Gabriel Lagonsin. Kroll warns of widening gap in global cyber resilience // TechDay (https://securitybrief.co.uk/story/kroll-warns-of-widening-gap-in-global-cyber-resilience). 20.03.2026).***

***

«Кібербезпека та захист даних функціонують в одному середовищі, але не є взаємозамінними поняттями, і їхнє плутання створює правові та комерційні ризики в організаціях, діяльність яких дедалі більше базується на даних. Кібербезпека — це насамперед технічна дисципліна, спрямована на захист систем, мереж та всіх типів даних від несанкціонованого доступу, компрометації або втрати шляхом забезпечення конфіденційності, цілісності та доступності за допомогою таких заходів, як шифрування, контроль доступу, моніторинг та реагування на інциденти. Натомість захист даних — це правова та регуляторна система, що регулює законну обробку персональних даних — як їх збирати, використовувати, зберігати, передавати та зберігати — і в Південній Африці значною мірою визначається POPIA (Закон про захист персональних даних), який вимагає законної, мінімальної, обмеженої ціллю обробки з відповідним рівнем безпеки…

Ця відмінність має значення, оскільки організація може мати надійну систему кібербезпеки, але при цьому порушувати правила захисту даних, збираючи надто багато персональних даних, використовуючи їх не за заявленими цілями або зберігаючи їх надто довго; при цьому порушення є не лише технічною подією, а й приводом для виконання обов’язків із захисту даних, таких як повідомлення, взаємодія з регуляторними органами та потенційна відповідальність. Багато організацій надмірно інвестують у засоби безпеки, водночас недостатньо розвиваючи управління даними, і без чіткого розуміння того, які персональні дані обробляються та куди вони надходять, сама лише безпека не може гарантувати

дотримання вимог. Це робить підходи «за замовчуванням» надзвичайно важливими: конфіденційність за замовчуванням передбачає врахування питань конфіденційності, орієнтованих на користувача, з самого початку; захист даних за замовчуванням інтегрує такі законодавчі вимоги, як мінімізація, обмеження цілей та контроль зберігання, у функціонування системи; а кібербезпека за замовчуванням забезпечує технічну стійкість у процесі розробки завдяки безпечній конфігурації, управлінню ідентифікацією та доступом, шифруванню та моніторингу…

Оскільки ці елементи взаємозалежні, їх окреме розгляд призводить до прогалин, які неможливо усунути після впровадження; тому в договорах слід відобразити це розмежування, поєднуючи технічні стандарти безпеки з конкретними умовами щодо захисту даних, що охоплюють ролі, обмеження цілей використання, транскордонну передачу даних та відповідальність. Зрештою, організації повинні з самого початку інтегрувати обидві сфери, щоб зменшити технічні ризики, виконати законодавчі зобов'язання, зберегти довіру та відповідально вести діяльність в економіці, що базується на даних». ***(Isaivan Naidoo, Shaaista Tayob. Cybersecurity vs data protection: Why the difference matters // ENSafrica (https://www.ensafrica.com/news/detail/11493/cybersecurity-vs-data-protection-why-the-diff). 20.03.2026).***

***

«Сучасний ландшафт кібербезпеки формується переважно під впливом трьох взаємопов'язаних факторів: критичної вразливості цифрових ідентичностей, прискорення темпів атак на основі штучного інтелекту та посилення впливу глобальних геополітичних напружень. Ідентичність залишається основним каналом проникнення в системи, а зловмисники для проникнення в середовища використовують надзвичайно ефективний ланцюжок постачання програм для викрадення даних та соціальну інженерію з використанням штучного інтелекту — зокрема, переконливі фішингові приманки та діпфейки…

Хоча штучний інтелект значно прискорює та розширює масштаби окремих етапів атак, таких як розвідка та розробка шкідливого програмного забезпечення, повністю автономні комплексні кібератаки на основі штучного інтелекту залишаються скоріше новою, ніж поширеною загрозою, головним чином тому, що традиційні тактики, такі як викрадення облікових даних, як і раніше, дають результат у разі наявності елементарних прогалин у системі безпеки. Однак глибока взаємопов'язаність сучасних бізнес-інфраструктур, що охоплює хмарні платформи та ланцюги постачання, дозволяє як злочинцям, так і державним суб'єктам швидко використовувати довірчі взаємозалежності та спричиняти ланцюгові наслідки… Оскільки різні зловмисники — наприклад, пов'язані з Росією чи Китаєм — керуються різноманітними фінансовими, шпигунськими чи геополітичними мотивами, організації не можуть однаково захищати всі свої ресурси. Натомість вони повинні визначити свої «найцінніші активи» та налагодити систему захисту, спрямовану проти конкретних загроз, які з найбільшою ймовірністю можуть націлитися саме на ці критично важливі ресурси. Зрештою, щоб забезпечити стійкість у цьому мінливому середовищі загроз,

підприємствам необхідно надати пріоритет постійній перевірці ідентичності та інтегрувати управління кіберризиками безпосередньо у свої загальні операційні та геополітичні стратегії». ***(Kevin Townsend. AI Speeds Attacks, But Identity Remains Cybersecurity's Weakest Link // SecurityWeek (https://www.securityweek.com/ai-speeds-attacks-but-identity-remains-cybersecuritys-weakest-link/). 25.03.2026).***

***

«Хоча кібербезпека автомобілів значно покращилася з часу гучного випадку дистанційного злому Jeep Cherokee у 2015 році, загрози продовжують зростати, оскільки сучасні автомобілі стають дедалі більш підключеними до мережі та автономними. Сучасні автомобілі — це, по суті, «комп'ютери на колесах», що базуються на мільйонах рядків коду зі складних ланцюгів постачання, бездротових підключень до додатків та розширеного аналізу даних. Ця технічна складність створює серйозні ризики для безпеки, особливо з огляду на те, що зламані автомобілі або системи автономного керування можуть мати летальні наслідки, а також через помітний брак фахівців, які володіють навичками як в автомобільній інженерії, так і в кібербезпеці… У відповідь на ці зростаючі вразливості уряди різних країн запровадили суворі стандарти, такі як Регламент ООН № 155, який передбачає проведення ретельних довгострокових оцінок кібербезпеки транспортних засобів у понад 60 країнах. Водночас незалежні дослідники у сфері безпеки продовжують відігравати вирішальну роль у виявленні вразливостей та забезпеченні відповідальності виробників… У міру того, як автомобільна промисловість все більше просувається у напрямку високоінтегрованого, автономного майбутнього, вона стикається зі складним, але надзвичайно важливим завданням — проактивно вдосконалювати свої засоби захисту від нових технологічних загроз, включаючи штучний інтелект та постквантові обчислення, щоб забезпечити довгострокову безпеку пасажирів». ***(Bree Fowler. Automotive Cybersecurity Threats Grow in Era of Connected, Autonomous Vehicles // TechTarget, Inc. (https://www.darkreading.com/vulnerabilities-threats/automotive-cybersecurity-threats-grow-connected-autonomous-vehicles). 26.03.2026).***

***

Сполучені Штати Америки

«…У березні 2026 року адміністрація Трампа започаткувала масштабну федеральну ініціативу з кібербезпеки, оприлюднивши новий указ президента та комплексну «Кіберстратегію для Америки». Ці два заходи свідчать про більш скоординовану та проактивну позицію федерального уряду, спрямовану на запобігання кіберзагрозам, посилення міжнародного правозастосування та модернізацію оборонних систем країни за допомогою державно-приватного партнерства…

Указ під назвою «Боротьба з кіберзлочинністю, шахрайством та хижацькими схемами, спрямованими проти американських громадян» спрямований, зокрема,

проти транснаціональних злочинних угруповань. Він доручає ключовим урядовцям розробити план дій, який передбачає створення оперативної групи для співпраці між державним і приватним секторами, надання пріоритету притягненню до відповідальності кіберзлочинців, а також запровадження програми відшкодування збитків жертвам для допомоги у компенсації фінансових втрат. Указ також містить попередження іноземним урядам, обіцяючи відповідні наслідки тим, хто допускає систематичну кіберзлочинну діяльність…

На додаток до цього, у «Кіберстратегії для Америки» визначено шість основних напрямків, спрямованих на запобігання загрозам із використанням усіх інструментів державної влади, а також на спрощення нормативно-правових вимог з метою зменшення навантаження на підприємства, пов’язаного з дотриманням цих вимог. Пріоритетними завданнями визначено модернізацію федеральних мереж із застосуванням систем безпеки на основі штучного інтелекту, посилення захисту критичної інфраструктури, забезпечення переваги США у сфері нових технологій, таких як штучний інтелект та квантові обчислення, а також формування потужного національного кадрового потенціалу у сфері кібербезпеки…

Для бізнесу ці заходи свідчать про посилення контролю та підвищення вимог. Компаніям слід очікувати більш ретельного контролю їхніх міжнародних партнерських відносин, що вимагатиме проведення більш ретельної перевірки іноземних суб’єктів господарювання. Хоча нова програма відшкодування збитків може стати способом компенсації втрат, організації відчуватимуть тиск з боку регуляторних органів щодо посилення своїх внутрішніх програм кібербезпеки з метою мінімізації ризиків, пов’язаних із дотриманням вимог законодавства. Зрештою, нова система вказує на постійну еволюцію регуляторних вимог та підвищення очікувань щодо співпраці з федеральними органами влади, зокрема в питаннях обміну інформацією та надання пропозицій щодо нових стандартів безпеки». ***(Sarah F. Hutchins, Robert M. Botkin, Madelyn R. Candela. What Businesses Need to Know About Trump's Latest Cybersecurity Executive Order and Initiatives // Parker Poe Adams & Bernstein LLP. (https://www.parkerpoe.com/news/2026/03/what-businesses-need-to-know-about-trumps-latest). 24.03.2026).***

***

«…Комітет Палати представників США з питань енергетики та торгівлі одноголосно направив до Палати представників вісім законопроектів, спрямованих на зміцнення фізичної та кібербезпеки енергетичного сектору країни за допомогою вдосконалених програм обміну інформацією та захисту інфраструктури…

Серед ключових заходів є Закон про забезпечення модернізації громад для створення стійкої енергосистеми (H.R. 7257), який вносить поправки до Закону про енергетичну політику та енергозбереження. Він вимагає від штатів чітко включити стратегії фізичної безпеки, кібербезпеки та стійкості для місцевих систем розподілу електроенергії (що працюють на напрузі 100 кіловольт або менше) до своїх планів енергетичної безпеки штатів. Законопроект вимагає врахування кіберзагроз, фізичних загроз та загроз, пов'язаних з погодою, а також вразливостей ланцюгів

постачання, що вимагає консультацій з операторами енергетики та постачальниками обладнання…

Закон про готовність до кібербезпеки трубопроводів (H.R. 7272) доручає Міністерству енергетики (DoE) створити програму для забезпечення безпеки трубопроводів та об'єктів скрапленого природного газу (СПГ). Ця ініціатива спрямована на поліпшення координації між федеральними, державними та приватними зацікавленими сторонами; розробку передових, добровільних технологій кібербезпеки та пілотних проектів; створення спеціалізованих навчальних програм для підготовки кадрів; та надання технічних інструментів, що допоможуть операторам оцінювати вразливі місця…

Крім того, Закон про Центр аналізу енергетичних загроз 2026 року (H.R. 7305) офіційно засновує Центр аналізу енергетичних загроз і поновлює дію програми підтримки кіберстійкості Міністерства енергетики. Цей закон створює основу для двостороннього обміну інформацією та скоординованого аналізу загроз між урядовими установами, розвідувальним співтовариством, національними лабораторіями та операторами енергетичного сектору приватного сектору з метою проактивного виявлення вразливостей та розробки стратегій запобігання атакам на критичну інфраструктуру». ***(Anna Ribeiro. House panel moves pipeline cybersecurity and energy threat analysis bills forward to boost energy sector resilience // Industrial Cyber (https://industrialcyber.co/regulation-standards-and-compliance/house-panel-moves-pipeline-cybersecurity-and-energy-threat-analysis-bills-forward-to-boost-energy-sector-resilience/). 09.03.2026).***

***

«…Ситуація з працевлаштуванням глухих та людей з вадами слуху в США залишається складною, а розрив у зайнятості зберігається вже майже два десятиліття: лише 57,7% глухих людей мають роботу, порівняно з 73,4% людей з нормальним слухом. Багато глухих працівників займають низькооплачувані посади без перспектив кар'єрного зростання, часто стикаючись з відсутністю пристосувань та низькими очікуваннями. Однак сектори технологій та кібербезпеки є багатообіцяючим винятком. Оскільки робота в галузі кібербезпеки в основному базується на тексті, здійснюється за допомогою екрану та сприяє дистанційній роботі, вона природно підходить для глухих фахівців…

Експерти стверджують, що залучення глухих людей до сфери кібербезпеки є стратегічною необхідністю. Джастін Пеллетьє з Рочестерського технологічного інституту (RIT) підкреслює, що «когнітивне різноманіття», яке приносять ці фахівці, є необхідним для передбачення та перемоги над хакерами. Щоб розвивати цей талант, RIT у партнерстві з Національним технічним інститутом для глухих (NTID) створив спеціалізовані, повністю дистанційні навчальні курси з кібербезпеки, які викладаються американською мовою жестів, і успішно працевлаштовує випускників у таких великих компаніях, як Microsoft та Amazon…

Незважаючи на ці можливості, орієнтуватися у корпоративному світі з вадами слуху залишається важко, навіть на рівні керівництва. Головний спеціаліст з інформаційної безпеки (CISO) Стю Херст детально описав величезне когнітивне навантаження, необхідне для участі в засіданнях, покладаючись одночасно на

недосконалі слухові апарати, читання по губах і затримку субтитрів. Хоча він пристосувався, просячи колег про конкретні корективи в спілкуванні, він зазначає, що заходи в соціальних мережах залишаються дуже складними. Крім того, структурні проблеми залишаються повсюдними; навіть при повноцінній зайнятості глухі люди стикаються зі значною різницею в заробітку порівняно зі своїми колегами, які чують. Для усунення цих нерівностей необхідний постійний доступ до освіти, кращі умови на робочому місці (такі, як описані EEOC) та ширше визнання в галузі того, що стійкість і когнітивна різноманітність глухих фахівців є безцінним надбанням, особливо в таких сферах з високим тиском, як кібербезпека». ***(Mirko Zorz. Decoding silence: How deaf and hard-of-hearing pros are breaking into cybersecurity // Help Net Security (https://www.helpnetsecurity.com/2026/03/09/deaf-hard-of-hearing-cybersecurity-careers/). 09.03.2026).***

***

«Компанія Secureframe Inc., що спеціалізується на автоматизації процесів забезпечення відповідності вимогам, запустила Secureframe Defense — платформу на базі штучного інтелекту, покликану допомогти підрядникам оборонної промислової бази (DIB) орієнтуватися у складному та дорогому процесі досягнення відповідності вимогам Сертифікації моделі зрілості кібербезпеки (CMMC). За оцінками Міністерства оборони США, майже 80 000 організацій зрештою потребуватимуть сертифікації CMMC рівня 2, проте на сьогодні її отримали менше ніж 800. Традиційний процес відомий своєю повільністю та високою вартістю: часто він триває понад рік і коштує від 100 000 до 300 000 доларів…

Компанія Secureframe Defense прагне змінити цю ситуацію, використовуючи штучний інтелект для скорочення терміну сертифікації з 12–18 місяців до всього чотирьох–восьми тижнів. Платформа супроводжує користувачів через три критичні етапи: по-перше, розгортання безпечних середовищ для контрольованої несекретної інформації (CUI) менш ніж за 30 хвилин шляхом автоматичної конфігурації таких інструментів, як Google Workspace та Microsoft GCC High; по-друге, використання штучного інтелекту для створення планів системної безпеки, політик та управління оцінками ризиків; і по-третє, надання підтримки в сертифікації за допомогою модуля аудиту, який автоматично збирає докази. Засновник Shrav Mehta зазначає, що платформа відображає уроки, отримані під час їхньої власної оцінки CMMC, пропонуючи оптимізовану альтернативу ручним процесам. За підтримки венчурного фінансування у розмірі 79 мільйонів доларів Secureframe позиціонує цей інструмент як рішення, що допомагає підрядникам оборонної галузі швидше та без зайвої складності відповідати вимогам Міністерства оборони США». ***(Duncan Riley. Secureframe unveils new platform to cut defense cyber certification timelines to weeks // SiliconANGLE Media Inc. (https://siliconangle.com/2026/03/10/secureframe-unveils-secureframe-defense-cut-defense-cyber-certification-timelines-weeks/). 10.03.2026).***

***

«Нещодавнє рішення Верховного суду штату Делавер у справі «Travelers Casualty and Surety Company of America проти Blackbaud, Inc.» суттєво змінило ситуацію у судовій практиці щодо постачальників керованих послуг (MSP) та постачальників програмного забезпечення як послуги (SaaS) після інцидентів у сфері кібербезпеки. Скасувавши два рішення нижчих судів про відмову у позові, Верховний суд дозволив страховикам продовжити розгляд об’єднаного позову про порушення договору від імені 97 клієнтів компанії Blackbaud, які постраждали від атаки програм-вимагачів. Це рішення істотно знижує тягар доведення для позивачів, дозволяючи подавати об'єднані позови на основі спільних звинувачень і вирішуючи, що позивачам не потрібно остаточно доводити безпосередню причину — пов'язуючи конкретні порушення договору з конкретними фінансовими збитками — на стадії розгляду клопотання про відхилення позову. Натомість позивачам потрібно лише продемонструвати розумний висновок про причинно-наслідковий зв'язок, що переводить справи у дорогу, насичену фактами стадію розкриття доказів і тим самим збільшує тиск на постачальників щодо укладення угоди на ранній стадії…

Крім того, це рішення свідчить про те, що суди активно визначають, що саме становить «комерційно обґрунтований рівень безпеки», перетворюючи колишні «найкращі практики» — такі як багатофакторна автентифікація (MFA), шифрування даних, управління оновленнями, сегментація мережі та мінімізація обсягу даних — на суворі критерії для судових розглядів. Суд також негативно оцінив спробу Blackbaud перекласти тягар реагування на інциденти та їх усунення виключно на своїх клієнтів, зазначивши, що провайдери не можуть легко перекласти ці обов'язки на нижчі ланки ланцюга постачання без збільшення власного ризику відповідальності… З огляду на ці розширені юридичні зобов'язання та підвищену ймовірність зіткнутися з тривалими та дорогими судовими процесами з боку страхових компаній, які агресивно застосовують право суброгації, MSP та постачальникам SaaS рекомендується терміново переглянути свої контракти, щоб чітко визначити можливості безпеки, встановити чіткі обмеження відповідальності та уточнити зобов'язання щодо реагування на інциденти та зберігання даних. І навпаки, клієнти тепер мають сильніші юридичні важелі, щоб вимагати конкретних заходів безпеки та відшкодування витрат від постачальників, які зазнали збитків». ***(C.Jade Davis and Enisha Smith. Delaware Supreme Court Expands Cyber Liability Exposure for SaaS & Managed Service Providers // Shumaker, Loop & Kendrick, LLP. (https://www.shumaker.com/insight/delaware-supreme-court-expands-cyber-liability-exposure-for-saas-managed-service-providers/). 11.03.2026).***

***

«Міністерство юстиції США (DOJ) опублікувало статистику щодо виконання Закону про неправдиві заяви (FCA) за 2025 фінансовий рік, яка свідчить про рекордні суми врегулювання спорів, що перевищили 6,8 млрд доларів, та безпрецедентну кількість позовів від інформаторів — 1 297. Забезпечення дотримання вимог кібербезпеки стало одним із головних пріоритетів: у рамках дев’яти угод було стягнуто понад 52 млн доларів, що є різким зростанням

порівняно з попередніми роками та продовжує динаміку Ініціативи щодо боротьби з цивільним кібершахрайством, започаткованої за часів адміністрації Байдена. Увага DOJ зосереджена на покаранні урядових підрядників, грантоотримувачів та субпідрядників, які свідомо надають неправдиву інформацію щодо дотримання вимог кібербезпеки, а не на покаранні жертв кібератак…

Ключові угоди про врегулювання у 2025 році свідчать про широкий масштаб застосування цього законодавства, що зачіпає підрядників оборонної галузі, адміністраторів закладів охорони здоров'я, університети та приватні інвестиційні компанії. Серед найпомітніших випадків — угода на суму 11,2 млн доларів із підрядником, що надає медичні послуги військовослужбовцям, за невиконання сканування на наявність вразливостей, а також угода на суму 9,8 млн доларів із виробником медичного обладнання — це перший випадок застосування FCA, пов'язаний зі стандартами кібербезпеки продукції. Ці справи підтверджують, що для встановлення відповідальності за FCA не обов'язково мати фактичні порушення даних або шкоду уряду; достатньо просто неправильного представлення дотримання стандартів, таких як NIST SP 800-171. Крім того, стандарт FCA щодо «свідомості» включає «необережне ігнорування», що означає, що необережні або неперевірені підтвердження відповідності можуть спричинити відповідальність. Оскільки Міністерство юстиції США (DOJ) явно надає пріоритет боротьбі з кібершахрайством, значною мірою завдяки фінансово зацікавленим інформаторам, компаніям, що розпоряджаються федеральними коштами, настійно рекомендується ретельно перевіряти свою відповідність вимогам кібербезпеки, належним чином реагувати на занепокоєння внутрішніх співробітників та розглядати можливість добровільного саморозкриття інформації для зменшення ризиків притягнення до відповідальності. З огляду на 2026 рік, створення нового підрозділу Міністерства юстиції США з боротьби з національним шахрайством свідчить про те, що цей жорсткий контроль лише посилиться». ***(J. Ryan Frazee, Adam S. Hickey, John Prairie, Arun G. Rao and Hadassah G. Diament. False Claims Act Enforcement: Record-Breaking Year Signals Continued Attention to Cybersecurity // Mayer Brown (https://www.mayerbrown.com/en/insights/publications/2026/03/false-claims-act-enforcement-record-breaking-year-signals-continued-attention-to-cybersecurity). 11.03.2026).***

***

«Під час укладення технологічних угод розуміння фінансових наслідків витоку даних має вирішальне значення для розробки ефективних положень щодо відшкодування збитків та обмеження відповідальності. Згідно з доповіддю IBM «Вартість витоку даних — 2025», середня глобальна вартість витоку даних становить 4,44 млн доларів США, а в США цей показник зріс до рекордних 10,22 млн доларів США… Ці витрати поділяються на виявлення та ескалацію (в середньому 1,47 млн доларів США), повідомлення (390 000 доларів США), реагування після порушення (1,35 млн доларів США) та втрату бізнесу (1,20 млн доларів США). Витрати також значно різняться залежно від сектору та вектора атаки; порушення у сфері охорони здоров'я є найдорожчими — 7,42 млн доларів США, тоді як зловмисні атаки зсередини та компрометація сторонніх

постачальників є найдорожчими типами порушень. Крім того, відновлення є тривалим — 76 % організацій, що повністю відновилися, витрачають на це понад 100 днів — а штрафи за порушення нормативних вимог стають дедалі суворішими: майже половина організацій, на які накладено штрафи, сплачує понад 100 000 доларів США…

З огляду на ці цифри постачальники технологій та клієнти повинні ретельно аналізувати свої договори. Для постачальників стандартні обмеження відповідальності (наприклад, 12-місячна сума абонплатежів) часто виявляються вкрай недостатніми для покриття фактичних збитків від порушення безпеки, а це означає, що їм слід очікувати вимог клієнтів щодо розширення винятків з відповідальності або встановлення окремих, більш високих лімітів, а також забезпечити наявність належного кіберстрахування. З іншого боку, клієнти технологічних компаній повинні усвідомлювати, що стандартні ліміти захищають постачальника, залишаючи клієнта вразливим перед регуляторним контролем та ризиком репутаційних збитків… Клієнти повинні наполягати на значному відшкодуванні, яке покриває витрати на захист, повідомлення та реагування, домовлятися про окремі ліміти відповідальності за порушення даних та вимагати дотримання конкретних стандартів кібербезпеки. Зрештою, ці положення контракту не є стандартними формулюваннями, а є важливими інструментами розподілу ризиків, які повинні відображати реальність багатомільйонних збитків та довгострокові перебої в бізнесі, спричинені сучасними кіберінцидентами…» ***(Jack Horgan. The Cost of a Data Breach: Why Lawyers Fight Over Data Breach Indemnities // Koley Jessen PC (https://www.koleyjessen.com/insights/publications/the-cost-of-a-data-breach-why-lawyers-fight-over-data-breach-indemnities). 11.03.2026).***

***

«За останні п’ять місяців Конгрес двічі допускав втрату чинності законодавчих повноважень, що лежать в основі обміну розвідданими про кіберзагрози в США, а потім поновлював їх лише шляхом короткострокових продовжень — востаннє продовживши дію закону до вересня 2026 року — що створює постійну невизначеність, яка послаблює один із основних стовпів колективної кіберзахисту саме в той час, коли загрози, пов’язані зі штучним інтелектом, набирають обертів. Закон, термін дії якого закінчується, — Закон про обмін інформацією з питань кібербезпеки 2015 року (CISA 2015) — був розроблений для усунення правових перешкод, які раніше заважали компаніям добровільно ділитися індикаторами загроз з урядом та між собою, таких як побоювання щодо розкриття конфіденційних даних, порушення антимонопольного законодавства або наслідки для акціонерів та регуляторних органів; він забезпечує захист від відповідальності та обмежує публічне розкриття або використання обмінюваної інформації регуляторними органами…

Ці заходи захисту сприяли розширенню та налагодженню роботи центрів та організацій з обміну та аналізу інформації (ISAC/ISAO) і помітно підвищили швидкість та ефективність міжгалузевого реагування на інциденти, при цьому галузеві об’єднання попереджають, що припинення дії цих заходів може скоротити

потоки інформації на 80–90 % і зробити країну більш вразливою до дій державних суб'єктів та злочинної діяльності. Однак закон був прийнятий понад десять років тому і не оновлювався з урахуванням загроз, пов'язаних зі штучним інтелектом, в умовах яких швидкий обмін великими обсягами інформації є ще більш важливим, зокрема для залучення потужних компаній у сфері штучного інтелекту до співпраці, спрямованої на забезпечення національної безпеки; серед нещодавніх прикладів можна навести розкриття компанії Anthropic у листопаді 2025 року про те, що суб'єкт, спонсорований державою, маніпулював її моделлю, змушуючи її діяти як автономний агент-зловмисник протягом більшої частини шпигунської кампанії, а також дані опитування, які показують, що керівники вважають вразливості, пов'язані зі штучним інтелектом, кіберризиком, що зростає найшвидше…

План дій адміністрації Трампа щодо штучного інтелекту значною мірою спирається на добровільні механізми державно-приватного партнерства, передбачені законом CISA 2015 року — такі як центр обміну інформацією, орієнтований на штучний інтелект, та рекомендації щодо вразливостей штучного інтелекту — проте постійні випадки втрати чинності підривають багаторічну координацію, якої потребують ці ініціативи. Виходячи за межі простого продовження терміну дії, аргумент полягає в тому, що Конгрес повинен модернізувати CISA 2015, щоб уточнити, що обмін інформацією про загрози, пов'язані саме зі ШІ, охоплюється законом, та вирішити нові проблеми, такі як дистиляція моделей (вилучення ШІ та крадіжка інтелектуальної власності), шляхом явного захисту обміну такими індикаторами, як аномальні шаблони запитів та зловживання API, одночасно потенційно розширивши охоплення на захисні техніки та процедури, а не лише на необроблені індикатори… Хоча цей закон і зазнав критики — зокрема, через спроби скасувати передбачені ним заходи захисту від відповідальності та більш загальні нападки, пов'язані з недоліками таких програм, як «Автоматизований обмін індикаторами» — багаторічне застосування закону дозволило розвіяти чимало побоювань щодо конфіденційності, а представники обох партій в цілому сходяться на думці, що ця система є цінною; головна рекомендація полягає в тому, щоб покласти край циклу прострочень і тимчасових заходів, а натомість безперервно продовжувати дію закону, водночас оновлюючи його відповідно до реалій епохи штучного інтелекту». ***(Spencer Michaels, Janet Egan, Michael Daniel. America's AI Cyber Defense Gap Needs Congress to Act // Center for a New American Security (https://www.cnas.org/publications/commentary/insights-americas-ai-cyber-defense-gap-needs-congress-to-act). 17.03.2026).***

***

«На конференції RSAC 2026 співробітники Конгресу з обох партій висловили спільну думку про необхідність того, щоб адміністрація Трампа надала детальний план реалізації своєї нової стратегії кібербезпеки, а також вела більш активну комунікацію щодо заходів захисту від кіберзагроз, пов'язаних з Іраном, які набирають обертів. У той час як демократи критикували нещодавно оприлюднену стратегію за відсутність конкретних повноважень

відомств та запитів на фінансування, республіканці очікують на майбутні виконавчі накази, які доповнять цю концепцію. Головною проблемою, що викликає занепокоєння у обох партій, є готовність Агентства з кібербезпеки та безпеки інфраструктури (CISA) захищати критичну інфраструктуру, особливо з огляду на те, що з січня 2025 року агентство втратило приблизно третину своїх співробітників…

Щоб вирішити цю проблему, демократи розглядають законопроект, який зобов'яже CISA провести офіційну оцінку готовності. Законодавці також прагнуть реформувати Спільну коаліцію з кіберзахисту (JCDC) при CISA, яка, на думку багатьох, стала занадто великою, щоб забезпечувати надійний обмін інформацією, шляхом можливого створення менших, ретельно перевірених підгруп. Крім того, комітети вивчають законодавчі рішення для стабілізації та модернізації програми «Загальні вразливості та ризики» (CVE)…

З огляду на різке зростання кількості повідомлень про вразливості, спричинене розвитком штучного інтелекту, та нещодавню невизначеність щодо фінансування, програма CVE може зазнати реформ, спрямованих на забезпечення стабільності бюджету, зміцнення міжнародного співробітництва та офіційне закріплення функції прямого нагляду з боку CISA з метою надання більш ефективної підтримки фахівцям із захисту глобальних мереж». ***(Eric Geller. Congress wants details from White House on cyber strategy, Iran resilience measures // TechTarget, Inc. (https://www.cybersecuritydive.com/news/congress-white-house-cybersecurity-strategy-iran-cisa-cve/815628/). 25.03.2026).***

Країни ЄС та Великобританія

«…У січні 2026 року Європейська комісія запропонувала цільові поправки до Директиви NIS2, спрямовані на звуження її сфери застосування, перегляд інтенсивності нагляду та запровадження часткової максимальної гармонізації без зміни основних зобов'язань щодо управління ризиками кібербезпеки. Визнаючи, що широка сфера застосування оригінальної директиви та розбіжності у її імплементації на національному рівні створили непропорційне навантаження на дотримання вимог та правову невизначеність, пропозиція спрямована на зменшення витрат для приблизно 29 000 компаній. Для уточнення сфери застосування поправки передбачають більш ризик-орієнтований підхід, звільняючи від вимог дрібних виробників електроенергії та імпортерів виключно хімічної продукції, водночас розширюючи охоплення, включивши стратегічно чутливі сфери, такі як цифрові гаманці, оператори підводних мереж передачі даних та інфраструктура військового призначення…

Однією з головних особливостей пропозиції є запровадження нової категорії «малих підприємств середньої капіталізації» (з чисельністю персоналу менше 750 осіб та доходом до 150 млн євро), що підвищує поріг, необхідний для віднесення суб'єкта господарювання до категорії «важливих». Хоча основні зобов'язання щодо кібербезпеки залишаються незмінними, ця зміна суттєво знижує регуляторне навантаження на менші компанії, перевівши їх з режиму попереднього (ex ante)

нагляду (включно з регулярними аудитами) на режим ретроспективного (ex post) нагляду. Крім того, пропозиція запроваджує максимальну гармонізацію для конкретних секторів, що не дозволяє державам-членам встановлювати додаткові технічні вимоги, які виходять за межі тих, що визначені імплементаційними актами Комісії. Вона також дозволяє суб'єктам господарювання підтверджувати відповідність вимогам за допомогою європейських схем сертифікації кібербезпеки, що, хоча й не є повноцінним «безпечним притулком», може обмежити втручання з боку наглядових органів. Нарешті, пропозиція запроваджує гармонізовану систему звітування про дані щодо програм-вимагачів, включаючи вектори атак та виплати викупу, без накладення додаткової відповідальності. Пропозиція тепер пройде законодавчий процес ЄС, передбачаючи 12-місячний період транспонування після її прийняття…» ***(Alex van der Wolk, Christoph Nüßing and Nina Graw. Easing the NIS2 Burden: Targeted Reforms to Europe's Cybersecurity Rules // Morrison Foerster LLP (https://www.mofo.com/resources/insights/260304-easing-the-nis2-burden-targeted-reforms). 04.03.2026).***

***

«Атанасіос Рантос, генеральний адвокат Суду Європейського Союзу (CJEU), видав офіційну думку, в якій рекомендує банкам негайно відшкодувати збитки власникам рахунків, які постраждали від несанкціонованих транзакцій, навіть якщо втрата сталася через недбалість клієнта. Ця думка випливає з польської справи, в якій банк відмовився відшкодувати збитки клієнту, який став жертвою фішингового шахрайства після введення своїх облікових даних на шахрайському веб-сайті… Рантос стверджує, що відповідно до Директиви ЄС про платіжні послуги банки не можуть відмовити у негайному відшкодуванні збитків, якщо немає обґрунтованих підстав підозрювати шахрайство з боку клієнта, про що необхідно повідомити національні органи влади. Однак банк все ще має право вимагати відшкодування збитків від клієнта, вживши юридичних заходів, якщо він може довести, що порушення було спричинене грубою недбалістю або умисним неправомірним діянням клієнта. Ця думка є необов'язковою юридичною рекомендацією, але вона вказує на ймовірний напрямок, який CJEU обере, коли винесе остаточне, обов'язкове рішення з цього питання...» ***(Bill Toulas. EU court adviser says banks must immediately refund phishing victims // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/legal/eu-court-adviser-says-banks-must-immediately-refund-phishing-victims/). 08.03.2026).***

***

«Експертні знання в галузі кібербезпеки стали найбільш затребуваними і високооплачуваними технічними навичками у Великобританії, що обумовлено зростанням кіберзагроз і регуляторних вимог. Згідно з дослідженням Robert Half, 48% лідерів у сфері технологій називають кібербезпеку своїм головним пріоритетом, а 44% компаній планують найняти фахівців у цій галузі протягом найближчих шести місяців. Цей високий попит призвів до 14% зростання кількості вакансій у порівнянні з минулим роком, перевищивши 6000

нових посад по всій країні, причому особливо високий попит на аналітиків та менеджерів з інформаційної безпеки спостерігається в таких ключових центрах, як Лондон, Манчестер, Брістоль та Бірмінгем…

Однак цей стрімкий ріст намірів щодо найму персоналу суперечить гострій глобальній нестачі кваліфікованих кадрів, що змушує 44% британських роботодавців пропонувати преміальні зарплати, щоб забезпечити собі дефіцитних фахівців. Хоча завищені зарплати наразі є основним інструментом залучення персоналу, експерти попереджають, що це не є стійкою довгостроковою стратегією. Для ефективного створення та підтримки своїх можливостей у сфері безпеки підприємствам рекомендується розробляти комплексні пакети працевлаштування, що акцентують увагу на кар'єрному зростанні, безперервному навчанні та гнучкому графіку роботи, оскільки фахівці все більше цінують структуровані можливості розвитку поряд із фінансовою компенсацією». ***(Elizabeth Greenberg. Cybersecurity Talent Is the UK Job Market's Hot New Bombshell // DIGIT (https://www.digit.fyi/cybersecurity-talent-is-the-uk-job-markets-hot-new-bombshell/). 11.03.2026).***

***

«Поки геополітичні напруження займають перші шпальти газет, Європейський Союз тихо перекроює свій цифровий ландшафт, пропонуючи зміни до Закону про кібербезпеку, які мають на меті розширити нагляд за ланцюгами постачання ІКТ та посилити вимоги до сертифікації. Це свідчить про перехід від сприйняття кібербезпеки як простої проблеми дотримання вимог до її розгляду як фундаментальної необхідності. Нагальність цього питання випливає з посилення відчуття вразливості: у міру того, як кіберзагрози стають дедалі більш витонченими, ЄС прагне забезпечити відповідність технологій, що лежать в основі основних послуг — від банківської справи до охорони здоров'я — єдиним стандартам безпеки…

Недавній звіт Всесвітнього економічного форуму підкреслює цю стурбованість, відзначаючи, що лише 40% європейських громадян відчувають впевненість у кіберстійкості своєї країни, а 61% називають швидко зростаючі загрози найбільшим викликом. У таких умовах міжнародні сертифікати кібербезпеки стали вирішальними для відновлення довіри. Такі компанії, як Dahua Technology та Axis Communications, показують приклад, досягаючи таких стандартів, як сертифікати CC EAL 3+ та BSI, щоб продемонструвати свою відданість безпеці проти таких ризиків, як масове спостереження. Зрештою, реформи ЄС встановлюють новий стандарт: підприємства повинні адаптуватися до цих більш суворих правил, а споживачам нагадують про необхідність надавати перевагу сертифікованим продуктам, щоб орієнтуватися у все більш ворожій цифровій середовищі». ***(Cybersecurity threats are mitigated in the new proposal by the European Union in response to new cyber complexities // EU Reporter (https://www.eureporter.co/defence/cybercrime-2/2026/03/11/cybersecurity-threats-are-mitigated-in-the-new-proposal-by-the-european-union-in-response-to-new-cyber-complexities/). 11.03.2026).***

***

«У відповідь на глобальний сплеск кібершахрайства, який наразі коштує економіці Великої Британії приблизно 19 мільярдів доларів щорічно і зачіпає кожного чотирнадцятого дорослого, уряд Великої Британії створює Центр боротьби з онлайн-злочинністю (OCC), який буде займатися боротьбою з цією зростаючою загрозою. Кіберзлочинці все частіше використовують цифрові платформи, застосовуючи такі методи, як фішинг, фальшиві інвестиції та крадіжка особистих даних, що зумовлює необхідність створення єдиної системи захисту…

OCC, спільний проект, в якому беруть участь Міністерство внутрішніх справ, Національне агентство з боротьби зі злочинністю (NCA), телекомунікаційні компанії, технологічні фірми та розвідувальні організації, має на меті об'єднати ресурси для виявлення та припинення онлайн-шахрайства. Основна увага буде приділятися боротьбі з міжнародними операціями, зокрема тими, що походять з-за кордону, але спрямовані проти громадян Великої Британії. Для ефективного нейтралізування цих загроз OCC використовуватиме потужні засоби правозастосування, включаючи блокування шахрайських повідомлень, заморожування банківських рахунків злочинців, демонтаж цифрової інфраструктури та видалення шахрайських профілів у соціальних мережах. Крім того, центр планує інтегрувати передові технології, такі як штучний інтелект і машинне навчання, для проактивного аналізу моделей і прогнозування загроз з метою зупинення кіберзлочинності у її джерелі, перш ніж вона поширіться». ***(Naveen Goud. UK launches Online Crime Centre to curb Cyber Frauds // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/uk-launches-online-crime-centre-to-curb-cyber-frauds/). 09.03.2026).***

***

«У 2025 році ситуація з кібербезпекою у Франції характеризувалася неоднозначними тенденціями: кількість атак з використанням програм-вимагачів зменшилася, тоді як загрози стали більш складними. Французьке агентство з кібербезпеки (ANSSI) повідомило про 128 інцидентів з використанням програм-вимагачів у 2025 році, що менше, ніж 141 у 2024 році. Це незначне поліпшення частково пов'язане з успішними операціями правоохоронних органів, зокрема операцією «Endgame», яка зруйнувала значну частину екосистеми програм-вимагачів і підірвала довіру серед кіберзлочинців. Однак програми-вимагачі як і раніше становили значну частку загальної кіберзлочинної діяльності. Основними цілями залишалися малі та середні підприємства, хоча найбільше зростання кількості атак у порівнянні з попереднім роком спостерігалося в організаціях охорони здоров'я та освіти. Найпоширенішими різновидами були Qilin (21%), Akira (9%) і LockBit 3.0/LockBit Black (5%), а також було виявлено десяток нових варіантів, серед яких Nova, Warlock і Sinobi, що спостерігалися вперше. Хоча постачальники засобів безпеки попереджали про сплеск кібервимагань без шифрування, дані ANSSI показали, що такі інциденти залишалися обмеженими…

Загалом ANSSI опрацювала 1366 підтверджених зловмисних інцидентів із 3586 загальних сповіщень у 2025 році, що становить 18% зниження кількості сповіщень, але стабільну кількість інцидентів з урахуванням піку під час

Олімпійських ігор у Парижі 2024 року. У даних спостерігається значне зростання кількості заяв про витік даних, хоча ANSSI застерігає, що 58 % з 460 заявлених витоків були або фальшивими, або повторно використаними даними з попередніх порушень. Також значно зменшилася кількість розподілених атак типу «відмова в обслуговуванні», спрямованих проти французьких організацій. Більш тривожною тенденцією стало стирання меж між діяльністю національних держав і кіберзлочинців: обидві категорії все частіше обмінюються можливостями, переймають тактику одна одної та розподіляють роботу між спеціалізованими етапами — це «технологічний туман», який ускладнює атрибуцію та вказує на зростаюче перекриття між державними та кримінальними суб'єктами. Генеральний директор ANSSI Вінсент Струбель виділив атаки на електричну інфраструктуру Польщі наприкінці 2025 року як передвісника «страшного сценарію» для Франції — масового сплеску гібридних атак до 2030 року, що поєднують кібернетичні та кінетичні ефекти на критичну інфраструктуру, — водночас стверджуючи, що Франція має засоби для протидії, стримування та ускладнення таких загроз». ***(Kevin Poireault. France: National Cybersecurity Agency Reports Ransomware Attack Drop in 2025 // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news/france-anssi-ransomware-attack/). 11.03.2026).***

***

«Уряд Великобританії запустив новий план дій у сфері кібербезпеки, на який виділено понад 200 мільйонів фунтів стерлінгів, щоб реформувати кібербезпеку державного сектору та забезпечити, щоб переваги цифровізації послуг — більша ефективність та доступність — не були підірвані порушеннями. В основі плану лежить новий урядовий підрозділ з кібербезпеки, завданням якого є сприяння швидким, скоординованим покращенням у всіх департаментах та державному секторі в цілому, а також узгодження з більш широкими цілями цифрової трансформації…

Експерти з безпеки вітають перехід від добровільних рекомендацій до обов'язкових стандартів, стверджуючи, що тільки обов'язкові заходи дають вимірювані результати. Вони виділяють три критично важливі напрямки: вирішення проблеми накопиченого технічного боргу в застарілих системах, які неможливо захистити в повному обсязі; розгляд ланцюжка поставок, особливо постачальників і постачальників керованих послуг, як основного вектора атак шляхом посилення договірних зобов'язань; переорієнтація показників успіху з «чи є у вас засоби контролю?» на «чи можете ви довести, що вони швидко і ефективно виявляють, пріоритезують і локалізують ризики?». План сигналізує про більш широкий поворот у бік стійкості в умовах реального тиску, а не дотримання вимог на папері, встановлюючи орієнтир, якого також закликають дотримуватися організації приватного сектору». ***(Tim Sandle. UK government seeks to clamp down on cyber-threats // DIGITAL JOURNAL INC. (https://www.digitaljournal.com/tech-science/uk-government-seeks-to-clamp-down-on-cyber-threats/article). 06.03.2026).***

***

«…Створення цифрової вартості німецькими компаніями значною мірою залежить від хмарних, платформних та SaaS-послуг, що надаються кількома американськими технологічними гігантами, такими як AWS, Microsoft та Google, що забезпечує ефективність та інновації, але також створює значну правову та стратегічну залежність. Американський закон CLOUD Act зобов'язує американських провайдерів передавати дані, що перебувають у їхньому «володінні, зберіганні або контролі», американським органам незалежно від місця їхнього фізичного зберігання, що потенційно суперечить суворим правилам GDPR щодо передачі даних до третіх країн та доступу держави — навіть якщо дані зберігаються в дата-центрах ЄС або у «суверенних хмарах». Рамка захисту даних між ЄС та США, підтверджена Загальним судом у 2025 році, наразі пропонує німецьким компаніям оперативне полегшення, дозволяючи передачу даних сертифікованим американським фірмам без додаткових гарантій, але вона не вирішує структурних проблем, таких як ризик екстериторіального доступу, прив'язка до постачальника або обмежені можливості переходу; отже, цифровий суверенітет виходить за межі простої залежності від рішення про адекватність…

Паралельно з цим ЄС посилює регуляторне середовище та створює власні екосистеми даних та інфраструктури. Директива NIS 2 встановлює комплексні вимоги щодо кібербезпеки та управління ризиками ланцюгів постачання для широкого кола «ключових» та «важливих» суб'єктів, тоді як DORA (Закон про цифрову операційну стійкість) зобов'язує фінансові установи впроваджувати надійні системи управління ризиками у сфері ІКТ, здійснювати нагляд за «критичними» сторонніми постачальниками та планувати сценарії виходу з угод і заміни постачальників, фактично перетворюючи цифровий суверенітет на зобов'язання щодо дотримання вимог. Інші інструменти, такі як Закон про дані та галузеві правила безпеки, спрямовані на посилення взаємодії, переносимості та доступу до даних, а ініціативи, такі як GAIA-X та європейські галузеві простори даних — зокрема запланований Європейський простір даних про здоров'я — мають на меті створити об'єднані, взаємосумісні середовища з чітким управлінням, відкриваючи нові ринки, але додаючи складні обов'язки щодо дотримання вимог…

Для компаній цифровий суверенітет стає конкретним завданням у сфері управління: їм слід систематично аналізувати залежності в сфері IT та даних (включно з субпідрядниками та юрисдикціями), посилювати умови договорів положеннями щодо локалізації, прав на аудит, запитів від органів влади та підтримки виходу/міграції, а також підвищувати технічну стійкість за допомогою мультихмарних або гібридних архітектур, відокремлення чутливих робочих навантажень та шифрування на стороні клієнта з використанням власних ключів, де це можливо. Управління передачею даних не повинно спиратися виключно на Рамку захисту даних; важливе значення зберігають стандартні договірні умови, оновлені оцінки впливу передачі даних та плани дій на випадок непередбачених обставин, пов'язаних із нестабільністю регуляторного середовища. Оскільки NIS 2 та DORA прямо пов'язують вищий керівний склад із кіберризиками та ризиками у сфері ІКТ, ради директорів повинні розглядати концентрацію хмарних ресурсів, доступ з третіх країн та залежність від платформ як частину комплексної перевірки ризиків, дотримання нормативних вимог, ESG та злиттів і поглинань на рівні

всього підприємства. У цьому мінливому правовому та геополітичному контексті німецькі компанії не можуть уникнути залежності від глобальних IT-провайдерів, але завдяки прозорому аналізу цих залежностей, управлінню ними на договірній основі та їх технічному захисту вони можуть відповідати регуляторним очікуванням і зміцнити власний стратегічний простір для маневру у дедалі складнішому цифровому середовищі…» ***(Hans Markus Wulf, Theresa Marie Bardenhewer and Emily Bernklau. Digital sovereignty in companies: Making cloud and AI use legally compliant // HEUKING (https://www.heuking.de/en/news-events/newsletter-articles/detail/digital-sovereignty-in-companies-making-cloud-and-ai-use-legally-compliant.html). 03.03.2026).***

***

«У «Цифровому омнібусному» пропозиції Європейської комісії запропоновано цільові поправки до Загального регламенту про захист даних (GDPR) з метою зменшення навантаження, пов'язаного з дотриманням вимог, гармонізації механізмів правозастосування та вирішення практичних проблем без кардинального перегляду законодавства. Серед основних змін — звуження сфери застосування поняття «персональні дані» шляхом уточнення, що воно є відносним до суб'єкта: це означає, що дані, псевдонімізовані однією стороною, можуть не вважатися персональними даними для одержувача, який не має можливості їх реідентифікації, що може спростити обмін даними…

Ця пропозиція також передбачає суттєве реформування регулювання файлів cookie та технологій відстеження шляхом перенесення положень щодо «кінцевого обладнання» з Директиви про електронну конфіденційність безпосередньо до Загального регламенту про захист даних (GDPR). Хоча згода залишається основною передумовою для відстеження, пропозиція запроваджує чіткіші винятки, вимагає надання простих можливостей відмови (заборона «темних шаблонів») та забороняє повторні спроби отримання згоди протягом шести місяців. Вона також свідчить про перехід від традиційних банерів з повідомленням про файли cookie до механізмів надання згоди, що підтримують машинне зчитування (наприклад, налаштування браузера)…

З метою забезпечення прозорості пропозиція спрощує інформаційні зобов'язання, передбачені статтею 13, у випадках відносин із клієнтами, що характеризуються низьким рівнем ризику та мають чітко визначений характер. У сфері штучного інтелекту вона прямо визнає «законні інтереси» як правову підставу для обробки персональних даних під час розробки штучного інтелекту за умови дотримання суворих заходів безпеки, а також уточнює умови обмеженої залишкової обробки даних особливих категорій. Крім того, вона оновлює правила щодо автоматизованого прийняття рішень з метою уточнення поняття «договірної необхідності».

З оперативної точки зору, пропозиція вводить нову підставу «зловживання правами», яка дозволяє контролерам відхиляти запити суб'єктів даних (DSR), що мають деструктивний характер або стратегічну мотивацію. Вона спрямована на гармонізацію вимог до оцінки впливу на захист даних (DPIA) у всій ЄС за допомогою Європейської ради з захисту даних (EDPB). Нарешті, щодо порушень

захисту даних, пропозиція підвищує поріг повідомлення органів влади з «ризику» до «високого ризику» (приводячи його у відповідність до порогу повідомлення фізичних осіб) та подовжує строк повідомлення з 72 до 96 годин, приділяючи більшу увагу надійним внутрішнім оцінкам ризиків та передбачаючи інтеграцію з єдиним пунктом прийому повідомлень NIS2…» ***(Stéphanie De Smedt, Kirill Ryabtsev and Emilia Fronczak. Digital Omnibus: What the proposed changes mean for GDPR, privacy and cookies // Loyens & Loeff (https://www.loyensloeff.com/insights/news--events/news/digital-omnibus-what-the-proposed-changes-mean-for-gdpr-privacy-and-cookies/). 05.03.2026).***

***

«Ситуація з безпекою в Європі різко змінилася, і ЄС рухається в напрямку створення єдиної нормативно-правової та фінансової системи, яка дедалі більше стирає межу між цивільною та військовою авіацією. Ключове значення в цьому відіграє пакет заходів ЄС щодо військової мобільності та мета створення до 2027 року «зони військової мобільності» ЄС — своєрідного «військового Шенгену», що забезпечить швидке транскордонне переміщення обладнання, вантажів та людей як у військових цілях, так і для забезпечення цивільного захисту. Нова регуляторна структура, що включає Європейську систему посиленого реагування з військової мобільності (EMERS), розрізнятиме звичайні операції та надзвичайні заходи і чітко визнаватиме подвійне призначення цивільної авіаційної інфраструктури та активів. Для авіакомпаній, лізингодавців та інших цивільних операторів це порушує делікатні питання щодо реквізиції, втрати можливості використання, розподілу ризиків, страхування та компенсації, а також вимагатиме ретельнішого вивчення умов лізингу та заходів безпеки, оскільки інституції ЄС опрацьовують детальні гарантії разом із державами-членами…

Водночас ЄС різко збільшує інвестиції в оборонну сферу в рамках ініціативи «ReArm Europe» («Readiness 2030») на суму 800 млрд євро, яка базується на інструменті SAFE та більш гнучких правилах формування національних бюджетів. Тільки SAFE може надати до 150 млрд євро у вигляді кредитів на розвиток оборонного потенціалу, а План дій у сфері безпеки та оборони Європейського інвестиційного банку, як очікується, подвоїть щорічні інвестиції до близько 2 млрд євро у дрони, космічну галузь, кібербезпеку, квантові технології та цивільний захист. Ці заходи відображають чіткий політичний поштовх у напрямку технологій та інфраструктури «подвійного призначення» — супутників, важких вантажних літаків, дронів та кіберсистем, що підтримують як цивільні, так і військові місії, — створюючи нові джерела доходів та можливості для партнерства для приватних компаній авіаційної, аерокосмічної та космічної галузей, які можуть продемонструвати взаємодію та функціональне перекриття…

Приклад Ірландії ілюструє, як національна політика розвивається в цьому ширшому європейському контексті. Уряд оголосив про план розвитку оборонної галузі вартістю 1,7 млрд євро та виділив 170 млн євро на європейські космічні програми до 2030 року, що свідчить про перехід від традиційного «військового нейтралітету» до більш виваженої позиції, яка розмежовує політичний нейтралітет від активної участі в ініціативах ЄС у сфері безпеки та оборони. Географічне

положення Ірландії на узбережжі Атлантичного океану та її залежність від партнерів з ЄС та ЄЕЗ у питаннях колективної безпеки означають, що її авіаційна, аерокосмічна, супутникова та кібербезпекова галузі, ймовірно, відіграватимуть дедалі більшу роль у європейській оборонній екосистемі, насамперед через комерційні партнерства та технологічну підтримку, а не класичні засоби «жорсткої сили». У міру дозрівання регуляторних та фінансових програм ЄС ірландські та інші європейські зацікавлені сторони в авіаційній та аерокосмічній галузях повинні будуть розширити свої стратегічні горизонти, включивши до них діяльність, пов'язану з обороною, при цьому ретельно керуючи договірними, регуляторними та ризиковими наслідками глибшої цивільно-військової інтеграції». ***(Christine O'Donovan and David McGovern. Aligning Civil Aviation and Aerospace with EU Defence Readiness 2030 :Defending the Skies // Mason Hayes & Curran (https://www.mhc.ie/latest/insights/defending-the-skies-aligning-civil-aviation-and-aerospace-with-eu-defence-readiness-2030). 06.03.2026).***

***

«У 2025 році Управління комісара з питань інформації (ICO) Великої Британії змінило пріоритети у своїй правозастосовній діяльності: загальна кількість порушень зменшилася, проте організаціям приватного сектору, які допустили серйозні порушення у сфері кібербезпеки та захисту даних, приділялася непропорційно велика увага. Після гучних атак на великі компанії ICO наклало шість штрафів за порушення GDPR на загальну суму понад 20 мільйонів фунтів стерлінгів — це значне зростання як за кількістю, так і за середнім розміром штрафу порівняно з 2024 роком. Штрафи, накладені на такі компанії, як Capita, Advanced Computer Software, 23andMe та LastPass, висвітлили повторювані теми: правозастосування було зумовлене чутливістю та обсягом скомпрометованих даних, відсутністю фундаментальних заходів безпеки, таких як багатофакторна автентифікація (MFA) та своєчасне виправлення вразливостей, а також недотриманням встановлених галузевих рекомендацій. Примітно, що ICO продемонструвало готовність притягати сторонніх обробників даних до прямої відповідальності за порушення безпеки, хоча контролери даних не можуть знімати з себе відповідальність за нагляд. ICO винагороджувало проактивну співпрацю та своєчасне визнання порушень зменшенням розміру штрафів, але карало за недостатньо обґрунтовані відповіді та повторні порушення вимог…

З огляду на перспективи до 2026 року, організації стикаються з дедалі небезпечнішим середовищем, яке характеризується ескалацією кіберзагроз, можливим поновленням масових позовів про відшкодування збитків (як це було в нещодавньому судовому процесі проти Capita) та регуляторним органом, наділеним розширеними повноваженнями. Нещодавно прийнятий Закон про дані (використання та доступ) надає ICO розширені інструменти розслідування, включаючи примусові допити свідків, а майбутній законопроект про кібербезпеку та стійкість (CSRB) розширить його повноваження щодо критично важливих послуг та сторонніх постачальників. Як наслідок, фінансові та репутаційні витрати, пов'язані з базовими, запобіжними порушеннями безпеки, зростають, що робить проактивне зменшення кіберризиків та надійне управління постачальниками

необхідними для корпоративної стійкості». ***(Richard Jeens and William Doyle. Cyber enforcement - when an incident is just the tip of the iceberg // Slaughter and May (https://www.slaughterandmay.com/insights/new-insights/cyber-enforcement-when-an-incident-is-just-the-tip-of-the-iceberg/). 10.03.2026).***

***

«З метою вирішення проблеми уповільненого впровадження первісної Європейської системи сертифікації кібербезпеки (ECCF) — яка за майже п'ять років дала лише одну діючу схему — Європейська комісія запропонувала комплексну реформу в рамках переглянутого Закону про кібербезпеку (CSA2)… Реформа спрямована на перетворення добровільної системи з неефективної ініціативи на практичний механізм забезпечення відповідності вимогам за допомогою стратегії, що базується на трьох основних напрямках. По-перше, вона прискорює розробку схем, встановлюючи для ENISA строгий 12-місячний термін на підготовку проектів схем, замінивши попередній процес з відкритим терміном, а також вимагає регулярного оновлення та чотирирічних оцінок для забезпечення актуальності схем. По-друге, вона розширює сферу застосування рамки за межі продуктів та послуг ІКТ, включивши керовані послуги безпеки та «кіберпозу» цілих організацій, що дозволяє організаціям сертифікувати загальний рівень зрілості своєї кібербезпеки. По-третє, вона запроваджує потужну «презумпцію відповідності», що дозволяє підприємствам використовувати єдиний сертифікат ECCF для підтвердження відповідності іншим нормам ЄС, таким як NIS2 та, потенційно, GDPR, тим самим зменшуючи дублювання регуляторного навантаження, за умови, що сертифікація проводиться незалежними сторонніми органами для рівнів ризику, що є вищими…

З метою забезпечення якості та гармонізації ринку реформа передбачає проведення експертних оцінок національних органів сертифікації кожні п'ять років і встановлює, що після впровадження європейської схеми всі національні схеми, що дублюють її, мають бути припинені, що дозволить створити єдиний ринок, який знизить витрати на дотримання вимог для транскордонних підприємств. Крім того, реформа стосується безпеки ланцюга поставок, надаючи Комісії повноваження визначати треті країни як такі, що викликають занепокоєння з точки зору кібербезпеки, фактично забороняючи «постачальникам високого ризику» мати сертифікати або надавати ІКТ-компоненти для ключових сертифікованих активів… Хоча сертифікація ECCF залишається добровільною, ці радикальні зміни роблять її надзвичайно стратегічним інструментом дотримання вимог для підприємств, що працюють у ЄС…» ***(Pia Ek. Reforming Europe's Cybersecurity Certification: From Stalled Framework to Practical Compliance Tool // Bird & Bird (https://www.twobirds.com/en/insights/2026/reforming-europe's-cybersecurity-certification-from-stalled-framework-to-practical-compliance-tool). 11.03.2026).***

***

«…Кіберзагроза, з якою стикається система подальшої освіти (FE) у Великій Британії, різко посилилася: на сьогодні атаки з використанням штучного інтелекту становлять майже дев'ять із десяти інцидентів; компанія

CrowdStrike повідомляє, що повне проникнення в систему може відбутися всього за 27 секунд, тоді як три роки тому на це йшло близько тижня, а суб'єкти, що діють за підтримки держави, вже націлилися на систему подальшої та вищої освіти (HE). Уряд Великої Британії тепер розглядає кібербезпеку як питання управління на рівні ради директорів, а не лише як проблему IT-відділу: у щорічному огляді NCSC за 2025 рік це названо «питанням виживання бізнесу та національної стійкості», і ця позиція підкріплена міністерським листом від жовтня 2025 року, в якому ради директорів закликають прийняти Кодекс практики кіберуправління, а також відкритим листом, у якому лідерів просять застосовувати Cyber Essentials у ланцюгах постачання та Рамку кібероцінки NCSC (CAF) для критично важливих послуг; майбутній законопроект про стійкість кібербезпеки закріпить зобов'язання щодо цифрової стійкості…

Проте заклади професійної освіти стикаються з серйозними обмеженнями — нечисленними IT-командами, застарілою інфраструктурою, великою площею атаки та обмеженими бюджетами — і лише 37 % з них мають спеціалізований персонал з кібербезпеки (що на 7 % менше, ніж у 2024 році). Jisc рекомендує зосередити обмежені ресурси на двох найважливіших напрямках: безпеці ідентифікації (включно з багатофакторною автентифікацією для тисяч студентів, співробітників та підрядників) та постійному моніторингу основних сервісів для раннього виявлення порушень. Ради директорів повинні використовувати безкоштовний набір інструментів NCSC Cyber Toolkit для впровадження управління ризиками на рівні персоналу, процесів та технологій. Культура також має значення: страх перед особистими наслідками може затримати повідомлення про інциденти та призвести до їх ескалації, тому надзвичайно важливою є прозора модель підзвітності, орієнтована на навчання, підкріплена доступними тренінгами з підвищення обізнаності…

Регулярні та ретельні тренування з реагування на інциденти за реалістичними сценаріями мають вирішальне значення, враховуючи, що середні витрати на відновлення досягають 2 млн фунтів стерлінгів, а час простою становить 10–20 днів. Нарешті, захист спільноти — швидкий обмін інформацією про загрози між колегами — підвищує стійкість; кіберспільнота Jisc, що налічує 3 000 учасників, є прикладом того, як колективні дії в поєднанні з індивідуальною пильністю забезпечують надійніший захист, ніж будь-яка установа може досягти самостійно». ***(David Batho. Cybersecurity in FE: Together we're Stronger // FE News (https://www.fenews.co.uk/exclusive/cybersecurity-in-fe-together-were-stronger/). 18.03.2026).***

***

«13 лютого 2026 року Європейська комісія опублікувала «Набір інструментів для забезпечення безпеки ланцюга поставок у сфері ІКТ» разом з оцінкою кіберризиків для підключених та автономних транспортних засобів (CAV), що ознаменувало чіткий перехід від дотримання вимог на рівні транспортних засобів до забезпечення стійкості на рівні екосистеми. Повідомлення для виробників оригінального обладнання, розробників програмного забезпечення для автономних транспортних засобів, постачальників програмного

забезпечення та операторів полягає в тому, що кібербезпека тепер є основним ризиком для бізнесу, а не лише регуляторною формальністю. Оцінка ризиків, проведена відповідно до NIS2 Групою співпраці NIS, Комісією та ENISA, розглянула 107 ризиків та визначила 14 як найпріоритетніші, причому системи керування транспортними засобами та системи обробки даних і прийняття рішень вважаються найбільш критичними, оскільки кібератаки можуть спричинити аварії та серйозну фізичну шкоду…

Також було відзначено, що основні вразливі місця пов'язані з підключенням до мережі та хмарною інфраструктурою, при цьому в оцінці підкреслювалося, що існуючі системи сертифікації, такі як Регламенти ООН R155 та R156, хоча й є важливими для кібербезпеки транспортних засобів та управління оновленнями програмного забезпечення, не забезпечують повного захисту від більш складних загроз у ланцюгу поставок, зокрема від віддаленого злому через бездротові оновлення або ризиків, пов'язаних із постачальниками, які перебувають під тиском іноземних урядів. Хоча на даний момент «Інструментарій» не є обов'язковим до виконання, він забезпечує структурований підхід до управління ризиками ланцюга постачання ІКТ, тоді як оцінка CAV визначає ключові групи активів, ймовірних зловмисників та сценарії атак, що передбачають оновлення OTA (бездротове оновлення), маніпуляції з датчиками або картою, а також атаки на автопарки чи мобільні платформи…

У сукупності ці заходи, ймовірно, визначатимуть очікування з боку регуляторних органів, інвесторів та ділових партнерів. Вони також вписуються в ширший і постійно розвиваючийся регуляторний контекст, що включає Закон ЄС про кіберстійкість, NIS2, резолюції ООН R155/R156, запропоновану редакцію Закону про кібербезпеку, а також паралельні зміни у Великій Британії в рамках Закону про автоматизовані транспортні засоби, правил типового затвердження у Великій Британії та законопроекту про кібербезпеку та стійкість. На практиці підприємства у всьому ланцюгу постачання CAV повинні тепер скласти карту своїх систем, постачальників та вразливостей, визначити компоненти, критичні для безпеки, виконання завдань та даних, оцінити технічні ризики, ризики ланцюга постачання та юрисдикційні ризики, посилити контракти зобов'язаннями щодо безпеки, повідомлення та аудиту, а також підготувати плани реагування на інциденти для подій, пов'язаних із ланцюгом постачання, таких як вразливості компонентів, перебої у роботі хмарних сервісів або компрометація мобільних платформ». ***(Cybersecurity in the connected and autonomous vehicle supply chain: the EU's ICT Supply Chain Security Toolbox and cyber risk assessment // Osborne Clarke Verein (OCV) (https://www.osborneclarke.com/insights/cybersecurity-connected-and-autonomous-vehicle-supply-chain-eus-ict-supply-chain-security). 17.03.2025).***

***

«…Опитування 1 000 власників малих і середніх підприємств у Великій Британії, проведене на замовлення компанії Samsung, свідчить про те, що багато малих підприємств вкрай погано підготовлені до кіберзагроз: кожен п'ятий респондент зазначив, що витік даних змусить його закрити бізнес протягом трьох місяців, а збитки від незапланованих витрат на усунення

проблем із безпекою та відновлення після зараження шкідливим програмним забезпеченням можуть сягати 100 000 фунтів стерлінгів на рік. Незважаючи на усвідомлення таких загроз, як фішинг (88%) та шкідливе програмне забезпечення (84%), ризикована поведінка є поширеною: 58% підключаються до безкоштовних громадських мереж Wi-Fi, 15% отримують доступ до конфіденційних робочих документів через них, 32% щотижня працюють у кав'ярнях, 24% — у громадському транспорті, 23% залишають пристрої розблокованими в громадських місцях, 58% встановлюють додатки, не перевіряючи дозволів, а 31% ніколи не використовують фізичні екрани для захисту приватної інформації…

Відстають і практики у сфері безпеки: 67% опитаних не впроваджували нових заходів кібербезпеки протягом останнього року, 45% не проводили навчання персоналу, а 21% охарактеризували свій підхід як реактивний; кожен п'ятий також зазначив, що не знав би, чи було пристрій зламано. Особливо помітним є ризик, пов'язаний з мобільними пристроями, оскільки 74% використовують телефони для роботи, але 49% не ставлять кібербезпеку в пріоритет при виборі пристроїв. Ці висновки були опубліковані разом з кампанією Samsung Galaxy S26 Ultra Enterprise Edition за участю колишнього експерта з кібербезпеки та переможця шоу «Traitors» Стівена Ліббі, який попередив, що навіть один випадок порушення безпеки може порушити роботу або навіть призвести до закриття малого та середнього бізнесу, тоді як Samsung стверджував, що вбудовані засоби захисту, такі як екрани конфіденційності та система безпеки Knox, можуть допомогти малим компаніям залишатися проактивними». ***(Hannah Bentley. Small businesses sleepwalking into cybersecurity crisis, expert warns // News Group Newspapers Limited (https://www.thesun.co.uk/tech/38558395/small-business-cyber-crisis/). 18.03.2026).***

***

«Усвідомлення кіберзагроз різко зросло, проте європейська кібербезпека все ще ризикує потрапити в «пастку дотримання вимог», коли збільшення витрат і обсягів звітності не призводить до підвищення стійкості. На круглому столі, що відбувся в лютому 2026 року за спільної організації Trusted Future та CEPA в рамках Мюнхенської конференції з безпеки, експерти з понад 13 країн — під спільним головуванням адмірала у відставці Майкла Роджерса та Ієви Ілвес — закликали перейти до моделей, орієнтованих на результати, що надають пріоритет оперативним можливостям та вимірюваним результатам. Учасники зазначили, що, незважаючи на подвоєння середніх витрат на безпеку (≈0,7 млн євро до 1,4 млн євро) під впливом NIS2, кількість інцидентів у ЄС зросла (ENISA 2025), малі та середні підприємства очікують значного кадрового навантаження для дотримання вимог (≈89%), а 59% організацій мають труднощі з заповненням вакансій — це свідчить про те, що найм персоналу для виконання паперової роботи витісняє фахівців з питань захисту…

Підхід України в умовах війни — показники у форматі OKR, пов'язані з безперебійністю роботи сервісів та зменшенням кількості шахрайських випадків — було названо зразком для наслідування на тлі зростання обсягу шахрайства у сфері цифрових платежів в ЄС до приблизно 4,2 млрд євро (приблизно 20 % від загального обсягу шахрайства). Група закликала переглянути підхід до обміну

інформацією: ставитися до кібербезпеки так само, як до безпеки авіації, забезпечуючи транскордонний обмін даними майже в режимі реального часу та співпрацю у реагуванні на інциденти, підвищити пріоритетність цих питань на рівні правління компаній та усунути прогалини в координації на рівні ЄС. Структурні перешкоди залишаються: програмне забезпечення для вимагання викупу як загроза національній безпеці без єдиної реакції ЄС/НАТО, фрагментований єдиний ринок кібербезпеки, гостра нестача робочої сили та нижча конкурентоспроможність заробітної плати, а також відсутність централізованого «покупця» в ЄС, який би стимулював безпеку через закупівлі…

Розробка політик також потребує «перевірки на безпеку»: на відміну від США, до кіберагентств ЄС часто звертаються за консультаціями на пізній стадії; у важливих документах (наприклад, у законопроекті про ринок цифрових послуг) бракувало структурованих рекомендацій з питань безпеки, а існуючі стандарти (наприклад, «Загальні критерії») використовуються недостатньо. Загальний висновок: перехід від процесу до результатів — оцінка успіху за кількістю запобігань атакам, систем, що залишаються в мережі, та зменшенням економічних втрат — через співпрацю під керівництвом галузі, розвиток талантів, операційні показники та рамки політики, що з самого початку враховують експертизу з питань безпеки». ***(Ronan Murphy and James Lamond. Less Talk, More Security: Cyber Lessons Learned from Munich // Center for European Policy Analysis (https://cepa.org/article/less-talk-more-security-cyber-lessons-learned-from-munich/). 18.03.2026).***

***

«Сіаран Мартін, високопоставлений співробітник Центру кібермоніторингу (CMC), нещодавно поставив під сумнів доцільність надання урядом Великої Британії гарантії по кредиту на суму 1,5 млрд фунтів стерлінгів компанії Jaguar Land Rover (JLR) після масштабної кібератаки. Виступаючи на заході, організованому Королівським інститутом об’єднаних служб, Мартін назвав це втручання «нещасливим прецедентом», оскільки це була реакція на конкретний випадок, що не мала чітких критеріїв для надання державної підтримки. Визнаючи, що в найгірших сценаріях дії уряду іноді є необхідними, він виступив за створення чіткої системи — наприклад, схем обов'язкового страхування або податкових стимулів — замість ситуативних заходів фінансового порятунку. Цю точку зору підтримала Трейсі Пол з Pool Re, яка зазначила зростаючий розрив між економічними збитками та наявним страховим покриттям, підкресливши, що структуроване партнерство між урядом та страховим сектором є необхідним для ефективного управління передачею ризиків…

Аналітики галузі підтримали ці побоювання, попередивши про довгострокові наслідки рішення JLR. Ерік Авакян з Info-Tech Research Group висловив думку, що надання гарантії за кредитом свідчить про те, що деякі компанії вважаються «занадто важливими, щоб збанкрутувати» з точки зору кіберризиків. Він застеріг, що це може створити «моральний ризик», коли компанії недостатньо інвестують у безпеку, покладаючись на неявну державну систему захисту, а великі організації водночас стають привабливішими цілями для злочинців, які прагнуть спричинити

максимальні збитки. Авакян підкреслив, що кібератаки еволюціонували і тепер загрожують не лише ІТ-системам, а й національному ВВП та зайнятості, що вимагає переорієнтації уваги на операційну стійкість…» ***(Paul Barker. Are nations ready to be the cybersecurity insurers of last resort? // FoundryCo, Inc. (https://www.cio.com/article/4148261/are-nations-ready-to-be-the-cybersecurity-insurers-of-last-resort.html). 20.03.2026).***

***

«Британське Управління з фінансового регулювання та нагляду (FCA) запровадило нові правила, покликані уточнити та оптимізувати процедуру повідомлення про інциденти, пов'язані з кібербезпекою, з метою зміцнення операційної стійкості фінансового сектору. Ці оновлення, розроблені у відповідь на відгуки представників галузі щодо плутанини з протоколами повідомлення, були створені у співпраці з Управлінням з питань пруденційного регулювання (PRA) та Банком Англії. Основні зміни включають створення єдиного порталу для повідомлення, скасування дублюючих вимог щодо повідомлення для постачальників платіжних послуг та кредитних рейтингових агентств, а також запровадження спрощених форм із чіткішими вказівками щодо порогових значень та визначень…

Основна увага нової системи зосереджена на управлінні ризиками, пов'язаними з третіми сторонами, що відображає зростаючу залежність сектору від зовнішніх постачальників та надавачів послуг. З огляду на те, що 40 % інцидентів, про які повідомлялося у 2025 році, були пов'язані з третіми сторонами — зокрема, із значними перебоями в роботі провідних технологічних компаній — оновлення FCA узгоджуються з більш широкими законодавчими ініціативами, такими як Закон ЄС про цифрову операційну стійкість (DORA) та законопроект Великої Британії про кібербезпеку та стійкість, який перебуває на розгляді. Фінансовим компаніям надано 12-місячний перехідний період для підготовки до нових правил, які набудуть чинності 18 березня 2027 року. Зрештою, регулятор має на меті використовувати зібрані дані для кращого виявлення ризиків, управління перебоями та обміну інформацією з метою посилення безпеки в усій галузі». ***(Phil Muncaster. FCA Updates Cyber Incident and Third-Party Reporting Rules // Reed Exhibitions Ltd (https://www.infosecurity-magazine.com/news/fca-updates-incident-thirdparty/). 19.03.2026).***

***

«Кіберризики стають дедалі серйознішою проблемою для малого бізнесу: за даними Національного центру кібербезпеки Великої Британії, у 2024 році 42 % малих підприємств зазнали кіберзлочинів. Невеликі компанії є привабливою мішенню, оскільки зловмисники знають, що вони часто мають слабкішу систему безпеки, меншу обізнаність щодо кіберзагроз і не мають спеціалізованих ІТ-команд, незважаючи на те, що зберігають цінні дані клієнтів, обробляють платежі картками, користуються онлайн-банкінгом і значною мірою покладаються на цифрові системи у своїй повсякденній діяльності. Для таких підприємств, як незалежні веломагазини, фінансові наслідки можуть бути

серйозними: середня сума відшкодування за кіберзлочини для підприємств з доходом менше 25 мільйонів фунтів становила близько 80 000 фунтів. До поширених загроз належать програми-вимагачі, шахрайство з платежами, витік даних, компрометація корпоративної електронної пошти та простої систем, що може призвести не лише до прямих збитків, а й до судових витрат, штрафів за порушення GDPR, шкоди репутації та втрати доходу в пікові періоди торгівлі…

Отже, кіберстрахування розглядається не лише як засіб відшкодування збитків, а й як частина ширшої стратегії захисту. Якісний страховий поліс може покривати викрадені кошти, шахрайські операції, інциденти з використанням програм-вимагачів, переривання діяльності, реагування на витік даних, судові витрати, штрафи регуляторних органів та відповідальність перед третіми особами, а також дедалі частіше пропонує засоби профілактики, програмне забезпечення для безпеки, навчання співробітників, підтримку у реагуванні на інциденти та оцінку вразливостей. Дані свідчать, що така підтримка може мати реальне значення: за повідомленнями, страхувальники подають на 73% менше заяв про виплату, ніж у середньому по галузі, а 56% заяв вирішуються без жодних витрат з боку власника бізнесу. Водночас 52% заяв від першої сторони виникають через порушення з боку третіх осіб, що свідчить про те, що підприємства можуть залишатися вразливими через постачальників, платіжних операторів або підключені системи, навіть якщо їхні власні практики є надійними. Окрім страхування, підприємствам слід зменшувати ризики, використовуючи надійні унікальні паролі, вмикаючи двофакторну автентифікацію, оновлюючи програмне забезпечення, навчаючи персонал, створюючи надійні резервні копії даних та обережно ставлячись до підозрілих електронних листів. Загалом, головний висновок полягає в тому, що кібератаки вже не є проблемою лише для великих корпорацій, і малим підприємствам не слід чекати, поки трапиться інцидент, щоб оцінити свою вразливість та запровадити належний захист і запобіжні заходи». ***(Joanna Evans. Cyber Security: The Threat Every Bike Shop Needs to Take Seriously // BizMedia (https://bikebiz.com/bikmo-cyber-security-the-threat-every-bike-shop-needs-to-take-seriously/). 18.03.2026).***

***

«Рада Європейського Союзу офіційно затвердила висновки щодо посилення спроможності ЄС запобігати гібридним загрозам, стримувати їх та реагувати на них стосовно Союзу, його держав-членів та партнерів, засудивши скоординовані ворожі дії, що не досягають рівня звичайної війни, — такі як саботаж критичної інфраструктури, зловмисні кібероперації, іноземне маніпулювання інформацією та втручання (FIMI), втручання у вибори та інструменталізація міграції — та прямо вказуючи на Росію та її посередників як головних рушіїв тривалих гібридних кампаній. У висновках закликається до більш стратегічної, колективної реакції ЄС шляхом підвищення ефективності гібридного інструментарію та інструментарію кібердипломатії ЄС, посилення захисту критичної інфраструктури та демократичних процесів, покращення співпраці з міжнародними партнерами, приватним сектором, науковими колами та

громадянським суспільством, а також надання підтримки країнам-кандидатам та потенційним країнам-кандидатам, які зазнають гібридного тиску…

Рада наголошує, що кібердіяльність часто є частиною ширших гібридних кампаній, у тому числі з боку недержавних посередників, і закликає до прискорення впровадження таких ключових правових рамок, як директиви NIS2 та про стійкість критично важливих об'єктів, при цьому «Кіберплан» визначено як центральний елемент скоординованого та оперативного реагування на масштабні кіберінциденти; вона також пов'язує ці зусилля з ширшим «комплексом політик», що включає Стратегію Союзу з питань готовності, Стратегію внутрішньої безпеки «ProtectEU» та План дій ЄС щодо безпеки кабельних мереж. Крім того, Рада наголошує на стійкості в конкретних сферах, закликаючи до посилення морської безпеки (включно із захистом критичної та підводної інфраструктури відповідно до міжнародного права та Стратегії ЄС з морської безпеки) та активізації дій проти гібридних загроз у повітряному просторі, включаючи порушення повітряного простору, зривання роботи аеропортів, шпигунство за допомогою дронів, глушіння та підробку сигналів GNSS, а також кібератаки…

З метою підвищення вартості ворожих операцій у документі ще раз підкреслюється намір ЄС застосовувати обмежувальні заходи та інші інструменти проти дестабілізуючих дій, зокрема пов'язаних із Росією, та кібератак, одночасно розширюючи можливості моніторингу та реагування за допомогою таких заходів, як впровадження інструментів FIMI у місіях Спільної оборонної політики (CSDP) та формування обізнаності щодо кіберситуації через ініціативи на кшталт Координаційного центру кіберзахисту ЄС. На додаток до цього Європейська комісія запровадила Набір інструментів безпеки ланцюгів постачання ІКТ, щоб допомогти державам-членам виявляти, оцінювати та зменшувати ризики у критичних технологічних ланцюгах постачання за допомогою таких заходів, як ретельніший контроль ключових постачальників, стратегії залучення декількох постачальників та зменшення залежності від постачальників з високим рівнем ризику». ***(Anna Ribeiro. EU unveils coordinated strategy to counter cyber, sabotage and disinformation threats amid rising hybrid attacks // Industrial Cyber (https://industrialcyber.co/news/eu-unveils-coordinated-strategy-to-counter-cyber-sabotage-and-disinformation-threats-amid-rising-hybrid-attacks/). 17.03.2026).***

***

«Закон про кіберстійкість (Регламент (ЄС) 2024/2847 - CRA), який набрав чинності 10 грудня 2024 року, встановлює широку систему кібербезпеки ЄС для продуктів із цифровими елементами, що розміщуються на ринку ЄС, з метою усунення недоліків у стандартах кібербезпеки та вирішення проблеми відсутності своєчасних оновлень безпеки протягом усього життєвого циклу продукту. Сфера його застосування є широкою і охоплює як апаратне, так і програмне забезпечення, яке може прямо або опосередковано підключатися до пристрою чи мережі, включаючи споживчі пристрої, такі як смартфони, ноутбуки, продукти для розумного дому, носимі пристрої та підключені іграшки, а також бізнес- та промислові продукти, такі як програмне забезпечення, мікропроцесори, брандмауери та компоненти розумних лічильників…

Регламент CRA поширюється на весь ланцюг постачання та покладає зобов'язання на всіх відповідних суб'єктів господарювання, зокрема виробників, уповноважених представників, імпортерів та дистриб'юторів. Хоча Регламент набуде повної чинності лише 11 грудня 2027 року, його застосування відбувається поетапно: положення щодо нагляду за ринком та забезпечення дотримання вимог застосовуються з 11 червня 2026 року, а з 11 вересня 2026 року виробники повинні почати виконувати обов'язки щодо повідомлення про інциденти та вразливості відповідно до статті 14. Вони вимагають попереднього повідомлення протягом 24 годин після виявлення активно експлуатованої вразливості або серйозного інциденту, більш повного повідомлення протягом 72 годин та остаточного звіту протягом 14 днів після того, як стануть доступними коригувальні заходи щодо експлуатованих вразливостей, або протягом одного місяця для серйозних інцидентів, з використанням Єдиної платформи звітності CRA…

На практиці організації, що виводять цифрові продукти на ринок ЄС, вже зараз повинні оцінювати, чи підпадають їхні продукти під дію цих вимог, переглядати процеси управління ризиками кібербезпеки та усунення вразливостей, стежити за розвитком ситуації щодо впровадження та дотримання вимог NIS2, а також запроваджувати внутрішні процедури повідомлення про інциденти та вразливості задовго до того, як основні зобов'язання набудуть повної чинності». ***(Christiana Bouleanu. 2026 Cybersecurity Countdown: New requirements are coming // Kinstellar (https://www.kinstellar.com/news-and-insights/detail/4164/2026-cybersecurity-countdown-new-requirements-are-coming). 03.2026).***

***

«Запропонований урядом Великої Британії законопроект про кібербезпеку та стійкість (мережі та інформаційні системи) значно розширить і посилить чинний Регламент NIS 2018 року, хоча він ще потребує схвалення парламентом. Законопроект розширює рамки регулювання кібербезпеки у Великій Британії, включивши до сфери його дії нові категорії організацій, зокрема відповідних постачальників керованих послуг (RMSP), та надавши регуляторним органам право призначати певних третіх осіб «критичними постачальниками», якщо порушення роботи їхніх систем може суттєво вплинути на операторів життєво важливих послуг, постачальників цифрових послуг або RMSP. Він також створює новий підсектор інфраструктури даних, включивши відповідних постачальників послуг центрів обробки даних безпосередньо до системи регулювання як операторів життєво важливих послуг… Водночас законопроект розширює визначення «інциденту», про який необхідно повідомляти, таким чином, що воно охоплює не лише події, які спричинили негативні наслідки, а й ті, що можуть їх спричинити, що, ймовірно, призведе до збільшення кількості інцидентів, які потребують уваги та повідомлення. Нова двоступенева система повідомлення вимагатиме від суб'єктів, що підлягають регулюванню, подати попереднє повідомлення протягом 24 годин після виявлення інциденту та більш повне повідомлення протягом 72 годин, а також передбачатиме додаткові обов'язки щодо повідомлення клієнтів для центрів обробки даних, відповідних постачальників цифрових послуг та RMSP. Копії повідомлень про інциденти також необхідно буде

надсилати до британської CSIRT (Команда реагування на інциденти в сфері комп'ютерної безпеки).

Законопроект також надає регуляторним органам та Комісії з питань інформації значно ширші повноваження щодо вимагання інформації та її обміну з іншими органами влади, одночасно суттєво збільшуючи розмір фінансових санкцій. Нинішній максимальний штраф у розмірі 17 млн фунтів стерлінгів за найсерйозніші порушення буде замінено багаторівневою системою, за якою менш серйозні порушення можуть каратися штрафом у розмірі 10 млн фунтів стерлінгів або 2% від світового річного обороту (залежно від того, яка сума більша), а більш серйозні порушення, включаючи порушення безпеки та невиконання вимог щодо повідомлення про інциденти, можуть каратися штрафом у розмірі 17 млн фунтів стерлінгів або 4% від світового річного обороту (залежно від того, яка сума більша). RMSP та деякі оператори центрів обробки даних будуть зобов'язані проходити обов'язкову реєстрацію, регуляторні органи зможуть стягувати періодичні збори для покриття своїх витрат, а право на оскарження буде поширене на RMSP та критично важливих постачальників… Хоча законопроект поділяє загальні цілі Директиви ЄС NIS2, він має суттєві відмінності від NIS2: NIS2 охоплює ширше коло секторів, тоді як британська система безпосередньо регулює діяльність певних критично важливих постачальників; порогові значення для повідомлення та правила інформування клієнтів відрізняються; у Великобританії не застосовується модель управлінської відповідальності, передбачена NIS2; а штрафи у Великобританії в деяких випадках можуть бути вищими. Тому організації, що працюють у Великобританії або з нею, не повинні вважати, що дотримання вимог NIS2 буде достатнім, а повинні на ранньому етапі розпочати оцінку ймовірного впливу законопроекту на їхню відповідність вимогам, реагування на інциденти, ланцюг постачання та механізми управління». ***(Oliver Yaros, Ana Hadnes Bruder, Ellen Hepworth, Alasdair Maher, Katie Steval, Rebecca Keay, Shannon Balnaves. United Kingdom Proposes Changes in the Cyber Security and Resilience Bill to the NIS Regulations, with Key Differences to NIS2 // Mayer Brown LLP (https://www.mayerbrown.com/en/insights/publications/2026/03/united-kingdom-proposes-changes-in-the-cyber-security-and-resilience-bill-to-the-nis-regulations-with-key-differences-to-nis2). 23.03.2026).***

***

Австралія та Нова Зеландія

«Уряд Нової Зеландії оприлюднив свою Стратегію кібербезпеки на 2026–2030 роки та супутній План дій на 2026–2027 роки, якими встановлюється національна система, що охоплює все суспільство, для боротьби з посиленням кіберзагроз та сприяння економічному зростанню. Стратегія, побудована навколо чотирьох основних цілей — «Розуміння», «Запобігання та підготовка», «Реагування» та «Партнерство», — переосмислює кібербезпеку як пріоритет національної безпеки та економічну необхідність. Дворічний План дій окреслює конкретні ініціативи, зокрема зміцнення стійкості критичної інфраструктури,

підготовку до квантовостійкої криптографії, створення централізованої служби повідомлень для Національного центру кібербезпеки, захист державних цифрових послуг та поглиблення міжнародного співробітництва, особливо в Тихоокеанському регіоні…

Важливо, що Стратегія свідчить про кардинальну зміну в очікуваннях щодо корпоративного управління, підкреслюючи, що кібербезпека більше не є лише функцією ІТ-відділу, а є ключовим елементом управління ризиками та прийняття стратегічних рішень для рад директорів та вищого керівництва. Вона також передбачає цілеспрямовані регуляторні та законодавчі реформи, такі як запровадження механізму захисту критичної інфраструктури, додавання цивільних грошових штрафів до Закону про конфіденційність 2020 року для стимулювання захисту даних, встановлення відповідальності за обробку незаконно отриманих персональних даних та розширення повноважень розвідувальних органів для проактивного протидії кіберзагрозам… Організаціям, особливо тим, що пов’язані з критичною інфраструктурою, рекомендується вже зараз інтегрувати кіберризики у своє стратегічне планування, щоб підготуватися до цих майбутніх змін та зберегти довіру зацікавлених сторін». ***(Liz Blythe and Louise Taylor. Release of New Zealand's Cyber Security Strategy // Russell McVeagh (https://www.russellmcveagh.com/insights-news/release-of-new-zealands-cyber-security-strategy/). 04.03.2026).***

***

«У нещодавньому звіті Управління генерального аудитора (OAG) Західної Австралії (WA) було виявлено цілу низку серйозних недоліків у системі безпеки, пов’язаних із тим, як сім державних установ управляють своїми середовищами Microsoft 365 (M365), причому ці недоліки безпосередньо пов’язуються з двома серйозними інцидентами: витоком даних, що містили особисту інформацію неповнолітніх, та випадком шахрайства з рахунками-фактурами, що призвів до розкрадання 71 000 доларів.

У першому випадку невідома організація надіслала електронною поштою конфіденційну інформацію щодо 32 осіб, серед яких були й неповнолітні, сторонньому постачальнику послуг, не провівши попередньої оцінки безпеки. Постачальник послуг завантажив ці дані на обліковий запис Dropbox, який згодом став жертвою кібератаки. У організації не було жодних засобів контролю для запобігання втраті даних (DLP), тому вона навіть не підозрювала, що дані покинули її середовище або були викрадені…

У другому випадку обліковий запис M365 одного з керівників був зламаний за допомогою цілеспрямованого фішингового листа. Зловмисник скористався слабкими механізмами багатофакторної автентифікації (MFA) — зокрема, використанням одноразових паролів, що надсилаються SMS, голосовими повідомленнями або електронною поштою — щоб зареєструвати неконтрольований пристрій із-за кордону. Потім зловмисник створив правила переадресації електронної пошти, вивчив історію офіцера та організував шахрайство з рахунками на суму 71 000 доларів, яке залишалося непоміченим протягом місяця. Хоча кошти було відшкодовано за рахунок страховки, організація

не зберегла достатніх журналів для криміналістичної експертизи та досі не усунула основні вразливості M365.

Генеральна прокуратура виявила системні недоліки у всіх семи перевірених установах. Жодна з них не запровадила комплексних заходів контролю за витоком даних (DLP) у додатках M365, і всі дозволяли співробітникам синхронізувати робочі дані з неконтрольованими сторонніми сервісами, такими як Dropbox та Google Drive. Установи покладалися на ненадійні методи багатофакторної автентифікації (MFA) (які, за даними Австралійського управління зв'язку, стали причиною 58 % інцидентів у сфері урядової безпеки у 2024–2025 роках) та дозволяли реєструвати особисті пристрої для MFA без належного управління. Серед інших недоліків — необмежена інсталяція несанкціонованих додатків Microsoft Teams, невиконання політик безпеки контенту для Power Platform, неефективний захист від підробки електронної пошти та невідповідні терміни зберігання журналів. Деякі організації навіть дозволяли звичайним користувачам створювати орендарів M365 з високим рівнем привілеїв або запрошувати зовнішніх гостей для доступу до конфіденційних даних без схвалення адміністратора…

Проводячи паралелі з руйнівним витоком даних компанії Medibank у 2022 році, генеральний аудитор штату Західна Австралія Керолайн Спенсер наголосила, що ефективне управління M365 має вирішальне значення для захисту урядових даних. У звіті настійно рекомендується, щоб усі організації перейшли на багатофакторну автентифікацію (MFA), стійку до фішингу, запровадили комплексні засоби контролю за витоком даних (DLP), обмежили зберігання даних та ретельно перевіряли сторонніх постачальників відповідно до стандартів, встановлених ASD, CISA та Microsoft». ***(Juha Saarinen. Poor WA gov M365 security led to $71k theft and children's data breached // nextmedia Pty Ltd. (https://www.itnews.com.au/news/poor-wa-gov-m365-security-led-to-71k-theft-and-childrens-data-breached-624118). 09.03.2026).***

***

«Рішення Федерального суду Австралії щодо компанії FIIG Securities Limited ознаменувало значне посилення підходу регуляторних органів до випадків порушення кібербезпеки, що має очевидні наслідки для підприємств як в Австралії, так і в Новій Зеландії. Компанія FIIG, яка має ліцензію на надання фінансових послуг (AFS), зазнала кібератаки у 2023 році, в результаті якої були викрадені та опубліковані в даркнеті надзвичайно конфіденційні дані про 18 000 клієнтів, включаючи паспорти, водійські посвідчення, банківські реквізити та податкові номери. Потім ASIC порушила судову справу, стверджуючи, що протягом чотирьох років FIIG не змогла належним чином управляти та мінімізувати кіберризики, порушивши свої зобов'язання за ліцензією AFS відповідно до статті 912A Закону про корпорації 2001 року (Cth). FIIG визнала три порушення: ненадання фінансових послуг ефективно, чесно та справедливо; відсутність належних фінансових, технологічних та людських ресурсів; та відсутність належних систем управління ризиками. Кожне з них також передбачало цивільно-правові санкції…

У лютому 2026 року суддя Деррінгтон наклав цивільний штраф у розмірі 2,5 млн австралійських доларів, наголосивши, що витрати на належну кібербезпеку були б значно меншими, і що це рішення має на меті стати попередженням для компаній, які недостатньо інвестують у кіберстійкість. Важливо, що жодна третя сторона не мала доводити фактичних фінансових збитків; достатньою була лише ймовірність значної шкоди, а недоліки в кібербезпеці були визнані єдиною та безпосередньою причиною порушень ліцензійних вимог. Хоча в попередніх справах (RI Advice, Lanterne Fund Services) технологічні ресурси були визначені як частина зобов'язань з управління, справа FIIG є першою, в якій було накладено значний узгоджений штраф, коли саме недоліки в управлінні кібербезпекою стали причиною відповідальності. Це рішення підтверджує, що для ліцензіатів AFS недостатня кібербезпека сама по собі може вважатися невиконанням обов'язку щодо ефективного та справедливого надання послуг, що наражає компанії не лише на заходи з дотримання конфіденційності з боку OAIC (Управління Комісара з питань інформації Австралії) після порушення, а й на проактивні заходи з управління відповідно до Закону про корпорації…

Отже, новозеландські підприємства, що ведуть діяльність в Австралії, стикаються з подвійним регуляторним навантаженням: один і той самий кіберінцидент може розглядатися як у рамках законодавства про фінансові послуги, так і в рамках законодавства про захист персональних даних. На внутрішньому ринку Нової Зеландії досі застосовувалися відносно помірні штрафи за порушення конфіденційності (наприклад, до 10 000 новозеландських доларів за неповідомлення Комісара з питань конфіденційності про серйозне порушення), а щодо кіберстійкості у фінансовій сфері аналогічних заходів примусового виконання не було. Однак Управління з фінансових ринків вже дало зрозуміти, що ефективні системи безпеки є невід'ємною частиною виконання ліцензійних зобов'язань, а урядовий План дій з кібербезпеки на 2026-2027 роки вказує на ймовірність посилення повноважень з контролю за дотриманням законодавства та підвищення розміру штрафів. План доручає Міністерству юстиції надати рекомендації щодо варіантів стимулювання захисту персональних даних, включаючи систему цивільних грошових штрафів відповідно до Закону про конфіденційність. У сукупності рішення у справі FIIG та напрямок політики Нової Зеландії надсилають чіткий сигнал: розглядати кібербезпеку як дискреційні витрати на IT більше не є прийнятним; ради директорів та ліцензовані організації повинні розглядати кіберуправління як основне регуляторне зобов'язання та інвестувати відповідно». ***(Karen Ngan, Jania Baigent, Anita Birkinshaw and Michelle Dunlop. Cyber regulatory risk grows: the AUD2.5 million ASIC cyber-attack penalty // Simpson Grierson (https://www.simpsongrierson.com/insights-news/legal-updates/cyber-regulatory-risk-grows-the-aud25-million-asic-cyber-attack-penalty). 09.03.2026).***

***

«Пакистан розробляє комплексний закон про кібербезпеку та створює спеціальний орган з кібербезпеки для протидії зростаючим цифровим загрозам у зв'язку з швидкою цифровізацією державних послуг та економічних систем країни в рамках більш широкої ініціативи «Цифрова нація Пакистан», оголосила міністр інформаційних технологій Шаза Фатіма. Міністр підкреслила, що, хоча цифровізація відкриває значні можливості в галузі електронного урядування, безготівкової економіки та онлайн-послуг для населення, вона одночасно створює не менші, а то й більші виклики, що вимагають надійних систем кібербезпеки, а не зупинки цифрового прогресу…

Пакистан вже активував свою Національну команду реагування на комп'ютерні надзвичайні ситуації (CERT) та провінційні CERT для виявлення інцидентів та реагування на них, а також цілодобову міжвідомчу систему цифрового моніторингу, відому як Національна система розвідки загроз (NTIS). Міністр підкреслив, що кібербезпека вимагає численних технічних спеціалізацій та комплексного регулювання, попередивши, що швидке поширення технологій, заснованих на даних, особливо в таких галузях, як геноміка та прецизійна медицина, створює нові ризики, включаючи потенційне зловживання чутливими біологічними даними зловмисниками для розробки цілеспрямованих біологічних загроз…

Підкреслюючи існуючі можливості Пакистану в галузі кіберзахисту, міністр зазначила, що під час минулорічного конфлікту з Індією скоординовані зусилля міністерства інформаційних технологій, Національної телекомунікаційної корпорації (NTC), національних команд з кібербезпеки та кіберкомандних структур збройних сил успішно запобігли будь-яким порушенням зв'язку або проникненню в урядові системи, незважаючи на постійні спроби кібервійни. Цей досвід, за її словами, демонструє гостру необхідність подальшого зміцнення міжвідомчої координації в галузі кібербезпеки за допомогою запланованого законодавства та повноважень». ***(Iqra Hussain. Government says Pakistan preparing Cyber Security Act as digital expansion raises risks // SAUDI RESEARCH & PUBLISHING COMPANY (https://www.arabnews.com/node/2636032/amp). 11.03.2026).***

***

«…У 2025 році система управління кібербезпекою та захистом даних у Китаї перейшла від етапу формування базових інститутів до етапу систематичного функціонування та детального контролю за дотриманням вимог. Серед ключових законодавчих досягнень — перша системна редакція Закону про кібербезпеку (CSL), яка уточнила питання юридичної відповідальності та врегулювала питання управління штучним інтелектом, а також прийняття Положення про управління безпекою мережевих даних (NDSM); обидва ці документи суттєво зміцнили нормативно-правову базу. Акцент у регулюванні змістився з посилення базової безпеки на сприяння ефективному та відповідному вимогам обігу даних як економічного активу, забезпечуючи баланс між

запобіганням ризикам та ринковим потенціалом. Ключові події включали вдосконалення правил транскордонної передачі даних, що зробило шляхи дотримання вимог більш стабільними та передбачуваними, а також триваюче створення базової системи торгівлі даними для стандартизації обігу даних…

У сфері захисту персональних даних 2025 рік ознаменувався переходом від загальних принципів до конкретних практичних вимог. Важливою подією стало введення «Заходів щодо проведення аудитів дотримання вимог захисту персональних даних», які зобов'язують контролерів даних проводити проактивні аудити. Адміністрація кіберпростору Китаю (CAC) та Міністерство громадської безпеки (MPS) також посилили нагляд за технологіями розпізнавання обличчя, вимагаючи явної інформованої згоди, спеціального зберігання даних та обов'язкової реєстрації для суб'єктів, що зберігають дані про 100 000 або більше осіб. Крім того, різні сектори, включаючи споживання, громадську безпеку, охорону здоров'я та технології, видали конкретні рекомендації щодо дотримання вимог, такі як обмеження збору даних у послугах «сканування для замовлення» та створення національної системи онлайн-аутентифікації особи. Забезпечення дотримання вимог залишалося жорстким, з міжвідомчими заходами, спрямованими на проблеми з високою частотою, такі як обробка даних додатків та офлайн-розпізнавання обличчя…

З огляду на перспективи до 2026 року, очікується, що регуляторне середовище буде характеризуватися стабільністю норм із сильним акцентом на впровадженні, ефективності контролю за дотриманням та оцінці спроможності управління. Аудити дотримання вимог щодо персональних даних стануть рутинними, що вимагатиме суттєвої підзвітності та інтеграції в корпоративні системи управління даними. У сфері управління технологіями розпізнавання облич буде запроваджено більш суворий контроль та вдосконалення на основі конкретних сценаріїв, тоді як стандарти ідентифікації, деідентифікації та анонімізації даних будуть офіційно впроваджені для забезпечення чіткіших технічних рекомендацій. Загалом, регулярне міжвідомче правозастосування продовжуватиме розширюватися, змушуючи підприємства систематично вдосконалювати свої організаційні та технічні заходи щодо дотримання вимог, щоб забезпечити стале та довгострокове управління даними». ***(James Gong and Yiting Wang. China Data Protection and Cybersecurity: Annual Review of 2025 and Outlook for 2026 // Bird & Bird (https://www.twobirds.com/en/insights/2026/china/china-data-protection-and-cybersecurity-annual-review-of-2025-and-outlook-for-2026). 04.03.2026).***

***

«У 2026 році ситуація з кіберзагрозами в Індії перетворилася на надзвичайно складне та динамічне поле бою, що зумовлено стрімкою цифровізацією, геополітичною напруженістю та діяльністю висококваліфікованих зловмисників. Вийшовши за межі випадкової кіберзлочинності, середовище зараз домінують просунуті операції, що фінансуються державою, організовані групи, які використовують програми-вимагачі, та технічно зріла хвиля хактивізму. Суб'єкти, що підтримуються державою, все частіше використовують просунуті постійні загрози для

довгострокового шпигунства проти урядових мереж та стратегічної інфраструктури, тоді як хактивісти застосовують складні інструменти для здійснення ідеологічно мотивованих зривів, стираючи межі між традиційним активізмом та кібервійною… Водночас зловмисники переносять свою увагу на використання вразливостей ланцюга поставок, зокрема в галузях, що швидко переходять на цифрові технології, таких як охорона здоров'я, використовуючи сторонніх постачальників для компрометації численних взаємопов'язаних систем нижчого рівня. У відповідь на зростання кількості різноманітних атак — про що свідчать рекордні за останні роки випадки використання програм-вимагачів та компрометації ланцюгів поставок — індійські організації переходять від реактивних ІТ-заходів до комплексних стратегій захисту, що базуються на аналітичних даних… У перспективі ця ситуація ще більше ускладниться через триваючу гонку озброєнь у сфері штучного інтелекту та автоматизації, стирання відмінностей між різними групами зловмисників, які обмінюються інструментами та тактиками, а також критичний перехід до атак на операційні технології, що контролюють фізичні процеси. Як наслідок, кібербезпека в Індії вийшла за межі базових ІТ-функцій і стала надзвичайно важливим питанням національної та економічної безпеки, яке вимагає постійної, проактивної пильності». ***(India's Evolving Cyber Threat Landscape: State-Sponsored Attacks, Hacktivism, and What's Next in 2026 // Cyble Inc. (https://cyble.com/blog/india-cyber-threat-landscape-2026-attacks-trends/). 24.03.2026).***

***

Ізраїль, Туреччина та країни Близького сходу

«У дослідженні, проведеному Радою з кібербезпеки ОАЕ, міститься попередження про те, що стрімке поширення дистанційної роботи тісно пов'язане з щорічним зростанням кількості кібератак майже на 40 %, оскільки перехід від добре захищених корпоративних мереж до домашніх систем створив нові вразливі місця, якими активно користуються зловмисники. Домашні мережі зазвичай базуються на простих маршрутизаторах та особистих пристроях із слабким захистом, що робить домашні маршрутизатори та VPN-з'єднання типовими точками входу для несанкціонованого доступу до конфіденційних даних та комунікацій…

Цей ризик ще більше посилюється геополітичною напруженістю, зокрема конфліктом між Ізраїлем та Іраном, що може призвести до ескалації кібервійни та шпигунської діяльності, а також через все ширше використання штучного інтелекту, завдяки якому атаки стають більш витонченими та цілеспрямованими. З огляду на такі фактори, як зростання цін на пальне, що потенційно сприяє поширенню постійної або гібридної форми роботи з дому, площа атаки, ймовірно, продовжуватиме розширюватися, якщо не буде вдосконалено засоби захисту. Тому рада наголошує на необхідності підвищення обізнаності з питань кібербезпеки та вжиття практичних заходів серед працівників, які працюють віддалено, — таких як захист домашньої мережі Wi-Fi, оновлення систем та використання надійних

засобів безпеки — а також чітких організаційних вказівок та підтримки для захисту особистих і бізнес-даних». ***(Naveen Goud. Work From Home culture triggers Cyber Attacks surge by 40 percent // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/work-from-home-culture-triggers-cyber-attacks-surge-by-40-percent/). 23.03.2026).***

***

«Закон про кібербезпеку № 7545 набув чинності в Туреччині після його публікації в Офіційному віснику 19 березня 2025 року та встановлює комплексну національну систему захисту державних установ, фізичних осіб та приватних суб'єктів від кіберзагроз, що широко поширюється на всіх учасників, які діють у кіберпросторі. Центральну роль у цій системі відіграє Управління з питань кібербезпеки, уповноважене регулювати, перевіряти та забезпечувати дотримання вимог у всьому секторі, включаючи визначення критичної інфраструктури, координацію команд реагування на інциденти, встановлення стандартів, сертифікацію технологій та проведення всебічних перевірок на місцях із доступом до систем, даних та інфраструктури…

Суб'єкти господарювання повинні повністю співпрацювати, інакше їм загрожують значні адміністративні штрафи, які для компаній можуть сягати 5 % річного доходу. Постачальники IT-послуг та інших послуг зобов'язані впроваджувати заходи з кібербезпеки, повідомляти про інциденти та вразливості, дотримуватися національних політик та використовувати сертифіковані продукти в критично важливих системах, тоді як компанії, що займаються кібербезпекою, мають додаткові зобов'язання, такі як отримання дозволів на діяльність, експортних дозволів та регуляторних погоджень щодо корпоративних змін; недотримання цих вимог може призвести до визнання транзакцій недійсними та спричинити значні штрафи…

Закон також запроваджує нові кримінальні правопорушення, зокрема ненадання запитуваної інформації, несанкціоновані операції, зловживання даними, що стали об'єктом витоку, та поширення неправдивої інформації, пов'язаної з кібербезпекою, за які передбачено покарання від штрафів до позбавлення волі. Розмір адміністративних штрафів варіюється в широких межах, і постраждалі сторони можуть оскаржувати їх у суді. Деталі впровадження будуть уточнені в підзаконних актах протягом року, після чого настане перехідний період, протягом якого суб'єкти господарювання повинні будуть отримати необхідні сертифікати та дозволи або припинити свою діяльність, що стане значним посиленням регулювання у сфері кібербезпеки в Туреччині». ***(Turkish Cybersecurity Law enters into force // Paksoy (https://paksoy.av.tr/en/2025/03/turkish-cybersecurity-law-enters-into-force/). 26.03.2026).***

***

«Геополітична напруженість, зокрема ескалація конфлікту між США, Ізраїлем та Іраном, змінює попит на страхові послуги, і зараз кіберстрахування вважається найбільш вразливим до наслідків конфлікту сегментом комерційного страхування. Опитування GlobalData за III квартал 2025 року показало, що 27,4% фахівців у галузі страхування очікують, що попит на кіберстрахування зросте найсильніше в умовах зростання напруженості, випереджаючи страхування політичних ризиків (25%), ланцюгів поставок (23,8%) та переривання бізнесу (13,1%). Кіберінциденти, пов'язані з державними та недержавними суб'єктами, ухиленням від санкцій, порушенням ланцюгів поставок та атаками на операційні технології, оцінюються нарівні з традиційними військовими та політичними ризиками. Енергетичний коридор Близького Сходу пропонує тест у реальному часі: морські страховики призупинили покриття військових ризиків для суден у Перській затоці, премії в Ормузькій протоці різко зросли, а Американська корпорація з фінансування розвитку сигналізує про розширення гарантій політичних ризиків для морської торгівлі, тоді як військово-морський ескорт може підтримувати рух танкерів. Однак більшою зміною є те, що корпоративні менеджери з ризиків та страховики зараз планують поширення конфлікту на західні ринки через кібердіяльність, змушуючи страховиків уточнювати апетит, ціноутворення та контроль накопичення…

Корпоративні інвестиції в кіберконтроль також впливають на розвиток ринку. Опитування Marsh, в якому взяли участь 2200 лідерів у сфері кіберризиків з 20 країн, показує, що майже 75% респондентів висловили високу впевненість у своїх кіберстратегіях, а 66% планують збільшити витрати на безпеку в 2026 році — понад чверть очікують зростання бюджету на 25% або більше. Перестраховики прогнозують стабільне зростання: Swiss Re оцінює, що глобальні премії за кіберстрахування досягнуть 16,4 млрд доларів США у 2026 році (у порівнянні з 15,6 млрд доларів США у 2025 році), а Munich Re прогнозує, що премії можуть зрости більш ніж удвічі між 2025 і 2030 роками… У 2024 році прямі страхові премії в США дещо знизилися через посилення вимог страховиків до страхування, але в першому півріччі 2025 року на ринок надійшло близько 250 мільйонів доларів США нових перестрахових потужностей, що дозволило деяким страховикам пропонувати вищі ліміти, контролюючи при цьому волатильність. У 2026 році Marsh очікує більш детального страхування на основі доказів управління, технічного контролю, реагування на інциденти та управління постачальниками, з більш чітким розмежуванням між страхувальниками з розвиненими кіберпрограмами та тими, хто має менш розвинені системи. Брокери відіграють все більшу роль у допомозі клієнтам у приведенні їхньої системи безпеки у відповідність до вимог страхування. МСП, які залишаються порівняно недостатньо застрахованими, стають предметом особливої уваги. Незважаючи на збільшення витрат, загрози залишаються актуальними: близько 70% організацій зазнали принаймні одного істотного кіберінциденту з боку третіх осіб протягом минулого року, що підкреслює ризики ланцюга поставок та постачальників в управлінні портфелем. Сукупний ефект — кіберринок, який все більше формується

геополітичними конфліктами та інвестиціями в стійкість підприємств, при цьому страховики коригують свою схильність до ризику та ціноутворення, а страхувальники продовжують інвестувати в захист». ***(Roxanne Libatique. Middle East tensions set to increase demand for cyber insurance – GlobalData // KM Business Information US, Inc (https://www.insurancebusinessmag.com/us/news/cyber/middle-east-tensions-set-to-increase-demand-for-cyber-insurance--globaldata-568002.aspx). 10.03.2026).***

***

«Малі підприємства все частіше стають головними цілями кібератак, включаючи шкідливе програмне забезпечення, програми-вимагачі та порушення безпеки даних, що може призвести до серйозних фінансових втрат, простоїв, судових позовів та втрати довіри клієнтів. З огляду на те, що 46% малих підприємств стали жертвами таких атак, а майже кожне п'яте з них згодом закрилося або подало заяву про банкрутство, страхування кібервідповідальності стає критично важливим питанням. Малі підприємства вразливі через обмежені ресурси кібербезпеки, щоденну залежність від цифрових систем, таких як POS-мережі та хмарні сховища, а також високу ймовірність людських помилок, наприклад, потрапляння на фішингові електронні листи…

Страхування кібервідповідальності може зменшити ці ризики, покриваючи ряд витрат, пов'язаних з атакою. Типове покриття включає витрати на реагування на порушення безпеки даних (IT-експертиза, юридичні витрати, повідомлення клієнтів), виплати за вимагання викупу та витрати на переговори, витрати на переривання діяльності (втрачений дохід та операційні витрати), юридичний захист від судових позовів або регуляторних заходів, а також управління репутацією. Однак, як правило, воно не покриває тілесні ушкодження, пошкодження майна, раніше існуючі інциденти або умисні злочинні дії співробітників…

І навпаки, підприємства, які працюють виключно в офлайн-режимі, не використовують цифрові системи, не обробляють цифрові платежі та не зберігають конфіденційні дані клієнтів, на даний момент можуть не потребувати кіберстрахування. Щоб зробити страхування більш доступним та зменшити загальний кіберризик, підприємствам слід впровадити багатофакторну автентифікацію (MFA), навчити співробітників розпізнавати фішинг-шахрайство, регулярно оновлювати програмне забезпечення та зберігати резервні копії важливих даних. Крім того, об'єднання кіберстрахування з іншими полісами, такими як загальна відповідальність, може бути економічно вигідним способом забезпечити цей життєво важливий захист». ***(Erika Malzberg. Is cyber liability insurance worth it? // McClatchy Company, LLC (https://www.miamiherald.com/news/business/article314925119.html). 04.03.2026).***

***

«Новий звіт Центру нових технологій та безпеки (CETaS) Інституту Алана Тьюринга попереджає, що противники, які співпрацюють у сфері штучного інтелекту, становлять значну загрозу національній безпеці Великої Британії та її союзників. У дослідженні було проаналізовано країни «CRINK» — Китай, Росію, Іран та Північну Корею — та їх взаємодію у сфері штучного інтелекту з метою визначення потенційних шляхів ворожої співпраці у цій галузі. Хоча прямих доказів багатосторонньої співпраці країн CRINK у сфері штучного інтелекту виявлено не було, у звіті наведено «перші ознаки» двосторонньої співпраці… Китай стає однією з найпотужніших держав світу, використовуючи свої відносини з Росією для демонстрації своїх намірів та інновацій, одночасно активно розширюючи співпрацю в галузі безпеки та технологій за межі блоку CRINK. Це має суттєві наслідки для національної безпеки Великої Британії, оскільки супротивники можуть обмінюватися ворожими можливостями штучного інтелекту в інформаційній війні, наступальних кібероперація̈х та військових технологіях. Для захисту своєї країни уряд Великої Британії закликають надати пріоритет перешкоджанню ворожій співпраці в галузі штучного інтелекту, підвищенню національної стійкості та налагодженню надійних партнерських відносин… Майбутня робота повинна бути зосереджена на виявленні вразливих місць, встановленні неприйнятних червоних ліній для ворожої співпраці в галузі ШІ та моніторингу ранніх ознак, таких як програми обміну талантами. Як зазначає дослідниця Меган Хьюз, «ступінь, в якому супротивники та геостратегічні конкуренти можуть придбати, розвивати, застосовувати та експортувати ШІ, має значний стратегічний інтерес для Великобританії та її союзників», що робить цю сферу співпраці критично важливим пріоритетом політики». ***(How Worried Should We Be About Hostile State AI Collaboration? // DIGIT (https://www.digit.fyi/how-worried-should-we-be-about-hostile-state-ai-collaboration/). 09.03.2026).***

***

«Фінська служба безпеки та розвідки (Supo) у своєму звіті «Огляд національної безпеки 2026» попередила, що кібершпигунство з боку Росії та Китаю, яке підтримується державою, залишається постійною та зростаючою загрозою для країни, активно націленою на урядові мережі, технологічні компанії та науково-дослідні установи…

Росія все більше покладається на кібершпигунство, щоб компенсувати зниження традиційних розвідувальних можливостей, зосереджуючись на викраденні конфіденційної інформації, пов'язаної із зовнішньою політикою, оборонними технологіями та війною в Україні. Supo підкреслює, що Росія використовує слабкі місця в західних ланцюгах постачання, зокрема в хмарних сервісах, які забезпечують високий «коефіцієнт вхід-вихід», надаючи доступ до численних клієнтів через одне вторгнення. Російські розвідувальні служби також регулярно використовують фінську інфраструктуру в операціях проти третіх країн і застосовують тактику, яка традиційно асоціюється з Китаєм, наприклад, компрометацію мережевих пристроїв споживачів, таких як домашні

маршрутизатори, щоб замаскувати зловмисну діяльність під звичайний трафік і обійти заходи безпеки. Крім того, Росія використовує вкрадені дані як зброю в операціях «хак і витік», стираючи межу між кібершпигунством та інформаційною війною, тоді як межа між державними акторами та кіберзлочинцями зникла, а проросійські хактивістські групи продовжують DDoS-атаки проти Фінляндії та інших західних країн…

Китайські кібероперації, спрямовані проти Фінляндії, також залишаються активними і підкріплюються розгалуженою державною кібер-екосистемою, яка використовує законодавчі зобов'язання, фінансові стимули, а також освітній і бізнес-сектори. Китайські розвідувальні служби використовують національні кіберпідприємства для отримання інструментів і виявлення вразливостей, а законодавство Китаю, яке вимагає спочатку повідомляти про вразливості програмного забезпечення державним органам, надає його розвідувальним організаціям значну перевагу. Китай активно використовує фінську інфраструктуру, включаючи орендовані сервери та зламані маршрутизатори споживачів, для створення «тіньових мереж», які дозволяють здійснювати комплексний збір розвідданих та операції впливу на треті країни, що відображає його амбіції щодо створення глобальних можливостей збору розвідданих… Supo попереджає, що зростаючий контроль Китаю над ланцюгами постачання технологій збільшує залежність Заходу від китайських технологій, тим самим зменшуючи маневреність зовнішньої політики та ускладнюючи зусилля з протидії кібершпигунству. Окремо, у нещодавній білій книзі Cyber Defense Assistance Collaborative (CDAC) розглядаються уроки, винесені з досвіду України щодо постійних російських кібератак з моменту вторгнення у 2022 році, а також вивчається, як була організована міжнародна підтримка для зміцнення кіберстійкості». ***(Anna Ribeiro. Finland's National Security Overview 2026 flags Russian and Chinese cyber espionage targeting government, critical infrastructure // Industrial Cyber (https://industrialcyber.co/reports/finlands-national-security-overview-2026-flags-russian-and-chinese-cyber-espionage-targeting-government-critical-infrastructure/). 12.03.2026).***

***

«Через рік після того, як США припинили всі наступальні кібероперації проти Росії, вакуум, що утворився в американській кіберзахисті, спонукав європейські країни до швидкого розвитку власних проактивних і наступальних кіберможливостей. З огляду на ескалацію гібридних загроз, таких як нещодавні атаки на енергомережу Польщі, пов'язані з Росією, ключові європейські країни відходять від суто оборонної позиції. Німеччина вивчає законодавчі повноваження для «відповідного хакерського удару» по нападниках, Нідерланди прийняли стратегію превентивного проникнення та нейтралізації ворожих хакерських мереж, а такі країни, як Фінляндія та Польща, посилюють свою законодавчу базу для кращої інтеграції цивільної та військової кібербезпеки з метою забезпечення безперервних операцій на державному рівні…

Незважаючи на ці національні досягнення, загальний потенціал кіберзахисту в Європейському Союзі залишається дуже нерівномірним. Великі корпорації часто

покладаються на надійну внутрішню систему безпеки, тоді як менші компанії та менш підготовлені країни залишаються вкрай вразливими, особливо з огляду на те, що зростаюча цифровізація життєво важливої інфраструктури, такої як транспорт та децентралізовані мережі відновлюваної енергії, розширює потенційну площу для атак. Щоб усунути ці диспропорції та поліпшити виявлення загроз у режимі реального часу, експерти виступають за більш інтегровану континентальну стратегію кіберзахисту…

Оскільки повна співпраця в масштабах ЄС ускладняється через брак довіри до деяких держав-членів, таких як Угорщина, ця інтеграція, ймовірно, набуде форми добровільної коаліції охочих країн, що діятимуть під егідою ЄС або НАТО. Зрештою, створення централізованого європейського кіберкомандування та мережі обміну розвідданими не повністю усуне гібридні загрози, але створить потужний незалежний засіб стримування. Це дасть чіткий сигнал супротивникам, що Європа здатна здійснювати негайні кібердари у відповідь проти іноземних цілей, з американською підтримкою або без неї». ***(Marija Golubeva. A Joint Cyber Defense for Europe? // Center for European Policy Analysis (https://cepa.org/article/a-joint-cyber-defense-for-europe/). 03.03.2026).***

***

«За даними розвідувальних служб Нідерландів (MIVD та AIVD), хакери, пов’язані з російським урядом, проводять масштабну глобальну кампанію, спрямовану проти акаунтів у Signal та WhatsApp урядовців, військових, а також журналістів. Замість використання шкідливого програмного забезпечення зловмисники застосовують витончені фішингові та соціально-інженерні прийоми для захоплення акаунтів. У Signal хакери видають себе за офіційну службу підтримки додатка (яка насправді не надає підтримки в додатку) і надсилають прямі повідомлення з попередженням про «підозрілу активність» або витік даних, щоб змусити жертв поділитися SMS-кодом підтвердження та своїм PIN-кодом…

Зловмисники використовують ці коди для реєстрації нового пристрою під ім'ям жертви, щоб отримати доступ до її контактів, тимчасово блокуючи доступ жертві. При цьому жертва може помилково вважати, що їй не завдано шкоди, оскільки історія чатів зберігається локально. У WhatsApp хакери використовують функцію «Підключені пристрої», обманюючи жертв, щоб ті сканували шкідливі QR-коди або натискали на посилання, які таємно прив'язують пристрій хакера до облікового запису жертви, потенційно надаючи зловмиснику доступ до минулих повідомлень без виходу жертви з облікового запису. Як Signal, так і Meta (материнська компанія WhatsApp) відреагували на це, закликавши користувачів ніколи не ділитися своїми кодами підтвердження та бути пильними щодо підозрілих повідомлень і посилань...» ***(Lorenzo Franceschi-Bicchierai. Russian government hackers targeting Signal and WhatsApp users, Dutch spies warn // TechCrunch Media LLC. (https://techcrunch.com/2026/03/09/russian-government-hackers-targeting-signal-and-whatsapp-users-dutch-spies-warn/). 09.03.2026).***

***

«Останні події у сфері кібербезпеки підкреслюють дедалі тісніший взаємозв'язок між геополітичними конфліктами та цифровою війною, а також використання штучного інтелекту злочинними угрупованнями як зброї. У міру загострення конфлікту на Близькому Сході кібероперації стали доповненням до військових ударів: серед них — злом систем відеоспостереження та дорожніх камер для створення мереж стеження, дефейсинг новинних веб-сайтів і релігійних додатків, таких як BadeSaba, а також викрадення даних у великих виробників медичного обладнання, наприклад компанії Stryker…

Європол попередив, що ці напруження, ймовірно, спричинять зростання кількості атак на європейську інфраструктуру та сплеск онлайн-шахрайства, пов’язаного з дезінформацією щодо конфліктів, тоді як у звіті Всесвітнього економічного форуму зазначено, що 64 % організацій наразі враховують кіберзагрози геополітичного характеру у своїх оцінках ризиків. Водночас зловживання штучним інтелектом прискорює розвиток кіберзлочинності через автоматизовані романтичні афери, масштабні операції з впливу та демократизацію створення програм-вимагачів — прикладом чого є британський злочинець, який використовує моделі штучного інтелекту для створення та продажу шкідливого коду без технічних знань, а також північнокорейські суб’єкти, які використовують штучний інтелект для генерації фальшивих облікових даних та проникнення в організації…

Інтерпол повідомляє, що шахрайство з використанням штучного інтелекту приносить у 4,5 рази більший прибуток, ніж традиційні методи, і характеризує цю тенденцію як «індустріалізацію шахрайства», що здійснюється за допомогою автономних систем-агентів, здатних проводити цілі кампанії — від розвідки до вимагання викупу. Серед інших помітних інцидентів — глобальна кампанія хакерів, спрямована на акаунти у WhatsApp та Signal португальських урядовців та дипломатів, витік персональних даних приблизно 6 мільйонів клієнтів нідерландського телекомунікаційного провайдера Odido у даркнеті, а також застереження шведських властей енергетичному сектору щодо посилення захисту після кібератак у Польщі…

Ці безпосередні загрози ускладнюють довгострокові стратегічні виклики, зокрема нагальну необхідність переходу на постквантову криптографію, перш ніж нинішні системи шифрування стануть вразливими до майбутніх квантових технологій, а також необхідність посилення кіберстійкості в таких критично важливих секторах, як охорона здоров’я, де темпи цифрових інновацій часто випереджають інвестиції в безпеку». ***(Akshay Joshi. Cyber impact of conflict in the Middle East, and other cybersecurity news // World Economic Forum (https://www.weforum.org/stories/2026/03/cyber-impact-conflict-middle-east-other-cybersecurity-news-march-2026/). 17.03.2026).***

***

«Кіберризик, зумовлений геополітичною напруженістю, залишається високим, особливо для операторів критичної інфраструктури, фінансових установ, транспортних і телекомунікаційних вузлів, центрів обробки даних та інших підприємств, що працюють у глобальній мережі; проте навіть

організації, які не є безпосередніми цілями атак, можуть зазнати серйозних збитків у разі порушення роботи таких життєво важливих служб, як електропостачання, водопостачання, транспорт або доступ до Інтернету. Геополітичні кризи можуть збільшити кіберризики через пов'язаних з державою зловмисників, які використовують сторонню інфраструктуру для приховування своєї діяльності, а також через більш активні групи хактивістів, що генерують великі обсяги деструктивних, хоча й іноді менш витончених, атак. Наслідки можуть включати перебої в роботі, уповільнення часу реагування, підвищення витрат на відновлення, ризики, пов'язані з регуляторними вимогами, штрафні санкції за порушення умов договорів, шкоду репутації та ускладнення процедури поновлення кіберстрахування. У таких умовах менеджерам з управління ризиками необхідно оцінювати, як кібератаки можуть вплинути на діяльність у конкретних географічних регіонах, ланцюгах постачання, критичних залежностях, юридичних та регуляторних зобов'язаннях, фінансових показниках, термінах відновлення, резервних потужностях, частоті інцидентів, а також на належний баланс між утриманням ризику та його передачею страховикам…

Щоб приймати обґрунтовані рішення, організації повинні перевести геополітичні кіберризики у фінансові показники, поєднуючи аналітичні дані про загрози, оцінки засобів контролю та реалістичні сценарії для оцінки впливу на прибуток, баланс та розподіл капіталу. Це забезпечує чіткіше прийняття рішень у сферах управління ризиками, фінансів, IT та на рівні ради директорів, допомагає визначити, чи є страхові ліміти та стратегії утримання збитків адекватними, а також сприяє кращому плануванню на випадок найгірших сценаріїв збитків. Зрештою, розглядати кіберризик лише як технічну проблему вже недостатньо; його слід інтегрувати в управління ризиками підприємства, планування капіталу та стратегію страхування, щоб підприємства могли ефективніше реагувати та формувати довгострокову стійкість у дедалі більш невизначеному геополітичному середовищі». ***(Anthony Wilson, Omar Al-Shahery. Risk leaders: How to strengthen cyber resilience against geopolitical disruption // WTW (https://www.wtwco.com/en-gb/insights/2026/03/risk-leaders-how-to-strengthen-cyber-resilience-against-geopolitical-disruption). 16.03.2026).***

***

«Країни-члени НАТО та їхні партнери в Індо-Тихоокеанському регіоні домовилися посилити співпрацю в галузі кіберзахисту. Цей крок є відображенням зростаючої загрози цифрової війни та все більшої залежності від технологічної інфраструктури в різних критично важливих секторах.

Домовленість було досягнуто в ході широких консультацій, присвячених розробці спільних механізмів координації для протидії кібератакам та обміну розвідданими.

Крім того, було досягнуто згоди щодо підтримки потенціалу країн-партнерів у боротьбі з новими кіберзагрозами.

Учасники наголосили на важливості створення комплексної системи цифрової оборони, здатної захищати критично важливі мережі та чутливу інфраструктуру.

Це є особливо важливим з огляду на ескалацію кібератак, спрямованих як проти урядових, так і економічних інституцій.

Обговорення також були зосереджені на шляхах посилення спільного навчання та розвитку експертизи у сфері кібербезпеки.

Це включало акцент на технологічних інноваціях та використанні передових інструментів для виявлення загроз та швидкого реагування.

Цей крок є частиною зростаючої міжнародної тенденції до посилення цифрової безпеки, яку вважають одним із найгостріших викликів сучасності…» ***(Medhat Elsheikh. NATO and its partners are strengthening cyber defense in the Indo-Pacific region // Our Media Group (https://www.voiceofemirates.com/en/news/2026/03/17/nato-and-its-partners-are-strengthening-cyber-defense-in-the-indo-pacific-region/). 17.03.2026).***

***

«Характер сучасної війни змінився: сучасні конфлікти, такі як той, що відбувається між Іраном, Ізраїлем та США, розгортаються одночасно як на традиційних полях бою, так і в кіберпросторі. Нещодавня ескалація кіберактивності свідчить про те, що цифрові атаки, спрямовані проти державних інституцій та приватної інфраструктури, стали невід'ємною частиною геополітичного конфлікту. Хакерські угруповання, пов'язані з інтересами Ірану, розпочали деструктивні операції, такі як атака на компанію медичних технологій Stryker, подаючи їх як відповідь на військові дії та підкреслюючи, як кібердіяльність використовується для доповнення традиційних військових стратегій…

Таке включення кібероперацій до складу збройних конфліктів свідчить про значний стратегічний зсув, в результаті якого питання національної безпеки тісно пов'язується із захистом цифрових систем. Уряди сьогодні усвідомлюють, що порушення роботи цифрової інфраструктури супротивника дає значну стратегічну перевагу, тому кіберпотенціал стає центральним елементом планування національної оборони. Потенційні наслідки є масштабними: складні кібератаки здатні спричинити масові відключення електроенергії, порушити роботу фінансових систем та завдати шкоди критичній інфраструктурі, зокрема системам водопостачання та медичним службам…

Отже, кіберзахист сьогодні є ключовим пріоритетом для осіб, відповідальних за формування політики у сфері національної безпеки, що вимагає значних інвестицій в інфраструктуру та кваліфіковані кадри, а також тісної співпраці між урядом і приватним сектором. У таких регіонах, як Близький Схід, де зосереджені важливі глобальні активи, країни на кшталт Саудівської Аравії вже вкладають значні кошти у цифрову стійкість. Окрім оборони, розробка надійних засобів кіберзалякування — здатності нанести значні збитки зловмисникам — також вважається необхідною для підвищення ризиків для потенційних супротивників і змушення їх двічі подумати, перш ніж розпочати атаку…» ***(Majid Rafizadeh. Strong Cyber Defenses Critical In Modern Warfare – Analysis // Eurasia Review (https://www.eurasiareview.com/20032026-strong-cyber-defenses-critical-in-modern-warfare-analysis/). 20.03.2026).***

***

«На тлі посилення занепокоєння щодо кібердіяльності Ірану під час триваючого конфлікту, група Threat Intelligence Group компанії Google попереджає, що в 2025 році домінуючою загрозою нульового дня, спонсорованою державою, як і раніше, буде Китай. З 90 вразливостей нульового дня, які були виявлені в минулому році, 10 були пов'язані з шпигунськими групами з КНР — удвічі більше, ніж у 2024 році — причому такі кластери, як UNC5221 і UNC3886, зосередилися на засобах безпеки та периферійних пристроях, щоб забезпечити собі довгострокові, важко відстежувані позиції. Хоча іранські актори (наприклад, Handala, що використовує підключення Starlink, і MuddyWater, що застосовує бекдор нульового дня проти цілей у США) залишаються активними, аналіз Google підкреслює більш широку зміну: масове використання відбувається набагато ближче до публічного розкриття, що свідчить про те, що китайські оператори скоротили цикли розробки та розповсюдження і що нульові дні більше не є прерогативою лише найбільш ресурсних команд…

Примітно, що загальна частка державних груп зменшилася, оскільки комерційні постачальники шпигунського програмного забезпечення все частіше використовували уразливості нульового дня, але Китай залишився значним розробником і користувачем. Google радить організаціям посилити захист від кампаній, пов'язаних з Іраном і Китаєм, шляхом ведення інвентаризації активів у режимі реального часу, постійного моніторингу систем і мереж з виявленням аномалій, а також впровадження вдосконалених, дієвих систем оповіщення для виявлення загроз і реагування на них у міру їх виникнення». ***(Davey Winder. China, Not Iran, The Biggest Zero-Day Cyber Threat // Forbes Media LLC. (https://www.forbes.com/sites/daveywinder/2026/03/08/china-not-iran-the-biggest-zero-day-cyber-threat/). 08.03.2036).***

***

«Національне кіберуправління Ізраїлю попередило про сплеск кібератак, які приписують Ірану, проти організацій у різних секторах протягом останніх днів, що збіглося з операцією «Ревучий лев». Інциденти, спрямовані на знищення даних і систем з метою порушення роботи та економіки внутрішнього фронту, спонукали до цілодобових заходів з локалізації та надання допомоги, при цьому агентство повідомляє, що на даний момент не зафіксовано жодних збитків для організацій, які є важливими для функціонування цивільного населення. За словами глави управління Йосі Караді, ця хвиля показує, що організації будь-якого розміру є вразливими… Більшість вторгнень здійснювалися з використанням дійсних облікових даних користувачів, викрадених або виточених під час попередніх зломів, та зловживаючи слабкими місцями в системах віддаленого доступу організацій; проникнувши всередину, зловмисники видаляли системи та дані. Влада закликала вжити негайних захисних заходів, зокрема змінити паролі в системах віддаленого доступу, увімкнути двофакторну автентифікацію,

переконатися, що жоден незнайомий користувач не має прав адміністратора, оновити інструменти віддаленого доступу до поточних версій безпеки та перевірити надійність резервних копій. Про підозрілі інциденти слід повідомляти в центр екстреної допомоги 119 Національного кібердиректорату, оскільки тривають зусилля з блокування подальших атак та підтримки постраждалих організацій». ***(Itay Gal. Iran-linked hackers are wiping data from Israeli orgs., cyber officials say // Jpost Inc. (https://www.jpost.com/business-and-innovation/article-889314). 09.03.2026).***

***

«На тлі операції Ізраїлю «Ревучий лев» Національне кібернетичне управління повідомляє про понад 40 випадків злому державних і приватних камер відеоспостереження іранськими та іншими ворожими суб'єктами з метою збору розвідувальної інформації — відстеження переміщень військ, місць падіння ракет та інших важливих дій — що спонукало до загальнонаціональних зусиль з виявлення, перешкоджання та попередження власників підприємств, муніципалітетів, установ та будинків. Агентство зазначає, що зловмисники зазвичай використовують вбудовані програмні недоліки, відкритий віддалений доступ або незмінені заводські облікові дані; «цифрова недбалість», така як стандартні паролі, застаріле програмне забезпечення та функції P2P/UPnP, що створюють дірки в маршрутизаторах домівок та малих підприємств, залишає сотні тисяч камер доступними, їх легко знайти за допомогою таких інструментів, як Shodan, зламати за допомогою списків поширених облікових даних або отримати доступ через «задні двері» постачальників та відомі баги…

Після злому камери можуть слугувати інструментами спостереження, трамплінами для проникнення в локальну мережу або джерелами маніпульованих прямих трансляцій. Ризик варіюється залежно від рівня продукту: найменш безпечними є імпортні товари без бренду та деякі китайські марки, такі як Hikvision і Dahua (обмежені в США/Великобританії), середній рівень споживчих лінійок (наприклад, Xiaomi, TP-Link, Eufy) значною мірою покладається на хмарні сервіси, тоді як виробники вищого класу, такі як Axis, Hanwha Vision і Bosch, роблять акцент на шифруванні та частих оновленнях. Чиновники закликають власників запобігати прямому доступу до Інтернету, негайно замінювати стандартні паролі на надійні унікальні, вимикати P2P та UPnP, якщо це не є необхідним, оновлювати прошивку, сегментувати камери в окремих мережах, увімкнути двофакторну автентифікацію для пов'язаних додатків, обмежити доступ до громадських місць та відключати пристрої, які не використовуються; про підозри щодо порушення безпеки слід повідомляти на гарячу лінію 119 Управління…» ***(Israel Wullman. Iran trying to hack hundreds of thousands of Israeli security cameras, cyber directorate says // y net news (https://www.ynetnews.com/tech-and-digital/article/ry0p11rot11x). 09.03.2026).***

***

«…Дослідники з відділу дослідження загроз компанії Acronis повідомляють, що оператори, пов'язані з Хамасом, поширюють серед

ізраїльтян шпигунське програмне забезпечення для Android, замасковане під додаток для оповіщення про ракетну загрозу, за допомогою SMS-фішингу. Виявлена 1 березня після повідомлень громадян, ця кампанія троянізує широко використовуваний додаток Red Alert і видає себе за офіційну службу Ізраїлю «Oref Alert» за допомогою підроблених ідентифікаторів відправника та посилань bit.ly, які замість законного оновлення доставляють шкідливе програмне забезпечення для стеження. Ймовірно пов'язана з групою Arid Viper (APT-C-23), ця операція здається безрозбірливою, що спонукало Національне кібердиректорат Ізраїлю та провідні ЗМІ опублікувати попередження по всій країні…

Підроблена програма використовує підроблені сертифікати та джерело інсталятора, яке імітує Google Play, щоб уникнути перевірок Android, а потім запитує широкі дозволи (включаючи точне GPS, SMS, контакти та облікові записи на пристрої), використовує фішингові накладки для викрадення одноразових паролів та облікових даних, зберігається після перезавантаження та постійно викрадає дані на віддалений C2. Аналітики відзначають, що це відповідає більш широкій схемі, в якій теми, пов'язані з війною — аварійні сповіщення, попередження про ракетні атаки, «оновлення безпеки» — використовуються для поширення засобів спостереження, перетворюючи кібероперації на паралельний рівень розвідки, який відстежує цілі та картографує мережі під час збройного конфлікту. Масштаби зараження залишаються невідомими». ***(Jessica Lyons. Spyware disguised as emergency-alert app sent to Israeli smartphones // The Register (https://www.theregister.com/2026/03/06/spyware_disguised_as_emergency_alert/). 06.03.2026).***

***

«…Поки Близький Схід охоплений фізичним конфліктом, цифрові армії Ірану ведуть грізну кібервійну, націлену на газові компанії в Йорданії, ОАЕ та Катарі в рамках своєї наступальної операції «Велика епопея». Ця кібермайстерність була в основному сформована у відповідь на атаку Stuxnet 2010 року, спільну операцію США та Ізраїлю, яка вивела з ладу іранські ядерні центрифуги, але одночасно послужила сигналом тривоги, що змусило Тегеран активно розвивати власні наступальні кіберможливості. У наступні роки Іран створив такі органи управління, як Верховна рада кіберпростору, значно збільшив бюджет на кібербезпеку та спонсорував групи APT (Advanced Persistent Threat) через свої військові та розвідувальні агентства…

Ефективність Ірану підкріплюється потужною базою технічних талантів та очевидним обміном знаннями з союзниками, такими як Китай і Росія, чиї тактики часто віддзеркалюються в іранських операціях. Окрім офіційно організованих груп APT, Іран також користується мережею з понад 120 союзних хактивістських груп і стратегічно підтримує молодих іранців, щоб вони отримали роботу в західних технологічних компаніях, а потім шантажує їх, змушуючи стати шпигунами режиму. Ця здатність до цифрових атак стала ключовим стратегічним активом, що дозволяє Ірану проєктувати свою силу на глобальному рівні, незважаючи на військові та економічні обмеження, хоча залишаються питання щодо його здатності підтримувати ці операції в умовах триваючого конфлікту». ***(Chris Stokel-Walker.***

How Iran built such a formidable cyberwar machine // Mansueto Ventures, LLC (https://www.fastcompany.com/91502049/iran-cyberwar-stuxnet-history). 04.03.2026).

***

«США та Ізраїль відкрито публікують свої військові удари по Ірану, супроводжуючи їх професійними фотографіями та відео, проте вони зберігають мовчанку щодо своїх одночасних кібероперацій — це мовчання підкреслює як стратегічну важливість, так і непрозорість кібервійни. Адмірал Бред Купер натякнув на роль кіберпростору, згадавши удари «від морського дна до космосу та кіберпростору», а генерал Ден Кейн описав кібероперативників як «першопрохідців», які порушили здатність Ірану «бачити, спілкуватися та реагувати»… Кіберкампанія, судячи з усього, проходила в кілька етапів: місяці або роки попередньої підготовки шляхом проникнення в мережі протиповітряної оборони та військового зв'язку; тактичні удари з метою «засліпити» іранське керівництво, можливо, включаючи хакерські атаки на камери відеоспостереження та дорожнього руху для відстеження аятоли Хаменеї перед його вбивством, а також блокування або відключення мобільних мереж для запобігання скоординованій реакції; та постійні операції з пошуку та націлювання на іранські військові системи з використанням відкритих джерел інформації, супутникових знімків та кібершпигунства, ймовірно, доповнених інструментами штучного інтелекту… Міністр оборони Піт Хегсет хвалився, що іранські військовослужбовці «не можуть розмовляти чи спілкуватися», а президент Трамп приписав кібервійськам заслугу в тому, що вони роблять супротивників «сліпими і нерозумними» під час операцій. Ізраїль навіть звинуватили в зломі популярного додатку BadeSaba для визначення часу молитви, щоб надсилати push-повідомлення «допомога прибула» під час бомбардувань. Проте кібероперації залишаються в основному невизнаними в офіційних наративах, що є навмисною таємницею, яка, за словами експерта з кібербезпеки Тала Коллендера, корениться в логіці кібервійни: «цінність здатності часто залежить від того, що інша сторона не знає, як саме вона працює».

Історична стриманість США та Ізраїлю щодо кібероперацій — вони досі відмовляються повністю підтвердити деталі атаки Stuxnet 2010 року на ядерні об'єкти Ірану — відображає законні занепокоєння щодо оперативної безпеки. Однак експерти, такі як доктор Луїза Марі Хюрель з Королівського об'єднаного інституту оборонних досліджень, стверджують, що відкрите визнання кіберпростору невід'ємною частиною військової стратегії може загострити суспільну та юридичну дискусію про пропорційність, правила застосування зброї та те, що становить застосування сили. Примітно, що в цьому конфлікті відсутня видима кібервідповідь Ірану, незважаючи на репутацію Ірану як потужної кібердержави… У той час як західні компанії, що займаються питаннями безпеки, готуються до атак, спонсорованих державою або пов'язаних з державою, Іран в основному зберігає мовчання — це викликає подив, який може свідчити або про недієздатність Ірану внаслідок ізраїльських ударів, або про переоцінку іранських можливостей...Хурель застерігає від недооцінки потенціалу Ірану до відповідних дій, зазначаючи, що «патріотичні хакери іноді використовуються як прикриття для груп, пов'язаних з державою», що свідчить про те, що те, що виглядає як діяльність

хактивістів, може приховувати дії держави». ***(Joe Tidy. What role has cyber warfare played in Iran? // BBC (https://www.bbc.com/news/articles/c5yr0576ygvo). 12.03.2026).***

***

«…Іранські спецслужби, зокрема представники Міністерства розвідки та безпеки (MOIS), все частіше використовують екосистему кіберзлочинців не тільки як прикриття для діяльності, що фінансується державою, але й як практичний оперативний ресурс. Історично Іран використовував фізичні злочинні мережі для заперечення причетності до стеження та вбивств, і ця тактика зараз відбивається в кіберпросторі. Замість того, щоб просто приймати на себе роль хактивістів або розробників програм-вимагачів, щоб заплутати слід, іранські суб'єкти активно використовують комерційне шкідливе програмне забезпечення, злочинну інфраструктуру та партнерські програми для розширення свого оперативного охоплення та підвищення своїх технічних можливостей…

Кілька випадків підкреслюють цю еволюцію. Іранська група загроз «Void Manticore», що діє під псевдонімом «Handala» проти ізраїльських цілей, використовувала «Rhadamanthys», складний комерційний інфокрадій, що продається на форумах даркнету, разом із власними спеціальними програмами для знищення даних. Подібним чином, «MuddyWater», відомий підрозділ MOIS, пов'язаний з «Tsundere Botnet» і використовує сертифікати підпису коду разом з «CastleLoader» (пропозиція Malware-as-a-Service), демонструючи, як використання злочинного програмного забезпечення ефективно затуманює діяльність держави і вводить в оману аналітиків… Крім того, недавня кібератака на ізраїльський медичний центр Shamir, спочатку приписувана групі хакерів-вимагачів «Qilin», пізніше була оцінена ізраїльськими офіційними особами як робота операторів, пов'язаних з Іраном, які діють як філії Qilin. Цей інцидент, що є частиною ширшої кампанії, спрямованої проти ізраїльських лікарень, ілюструє, що використання усталених операцій «програм-вимагачів як послуги» (RaaS) забезпечує як правдоподібне заперечення, так і значну оперативну перевагу, що свідчить про чітку стратегічну зміну від простого імітування кіберзлочинців до активної інтеграції в їх екосистему. ***(Iranian MOIS Actors & the Cyber Crime Connection // Check Point Software Technologies LTD (https://research.checkpoint.com/2026/iranian-mois-actors-the-cyber-crime-connection/). 10.03.2026).***

***

«Південно-Східна Азія стає все більш вразливою до кібернебезпек, пов'язаних з ескалацією конфлікту між США, Ізраїлем та Іраном. Експерти з безпеки попереджають, що хакери, пов'язані з державою, та злочинні угруповання використовують глобальні мережі, пов'язані з енергетикою, судноплавством та банківською справою. Останні події підкреслюють цей ризик: Іран погрожує економічним інтересам США та Ізраїлю після атаки на свій банк, а ОАЕ повідомили про запобігання організованим кібератакам серед 90 000–200 000 щоденних спроб порушення безпеки. Експерти наголошують, що географічна віддаленість і політична нейтральність більше не забезпечують

захисту; компанії Південно-Східної Азії опинилися в «радіусі ураження», оскільки вони використовують ті самі глобальні хмарні системи, платіжні процесори та підводні кабелі, що й ті, хто безпосередньо залучений до конфлікту. Наприклад, нещодавні удари дронів по об'єктах Amazon Web Services в ОАЕ та Бахрейні порушили роботу служб для компаній Південно-Східної Азії, які використовували їх як майданчики для відновлення після аварій…

Ця вразливість посилюється зростаючою роллю Південно-Східної Азії як глобального центру обробки даних, особливо в Малайзії, яка отримала значні інвестиції від таких технологічних гігантів, як Microsoft і Google, що робить регіон привабливою «легкою мішенню». Ситуація з загрозами вже є серйозною: компанія Kaspersky повідомляє про 70,7% зростання кількості заблокованих шпигунських атак у Південно-Східній Азії в першій половині 2025 року, а в Малайзії цей показник зріс на 124%. Незважаючи на значні фінансові втрати від кіберзлочинності — тільки за перші 10 місяців 2024 року Малайзія втратила понад 310 мільйонів доларів — експерти попереджають, що багато регіональних компаній все ще недостатньо інвестують у кібербезпеку, закликаючи їх розглядати її не як центр витрат, а як фундаментальну вартість ведення бізнесу». ***(Iman Muttaqin Yusof. Southeast Asia faces spillover cyber risk from Iran war as 'blast radius' widens // South China Morning Post Publishers Ltd. (https://www.scmp.com/week-asia/economics/article/3346342/southeast-asia-faces-spillover-cyber-risk-iran-war-blast-radius-widens). 12.03.2026).***

***

«…Після військових ударів США та Ізраїлю по Ірану проіранські та проросійські хактивістські групи розгорнули хвилю кібератак, переважно DDoS-атак, псування веб-сайтів та перебільшених заяв про порушення, спрямованих проти Ізраїлю, країн Перської затоки та західних інтересів. Intel 471 зафіксував найсильніший вплив на Ізраїль, за ним йдуть Кувейт та Йорданія, де найбільше постраждали національний уряд, аерокосмічна/оборонна та технологічна галузі. Такі групи, як Handala Hack, Cyber Islamic Resistance, UniT 313, NoName057(16) та інші, заявили про вторгнення в нафтогазові компанії, телекомунікаційні компанії, оборонні підрядники і навіть про нібито доступ до ізраїльських електромереж і радара Iron Dome, хоча більшість заяв здаються перебільшеними з пропагандистською метою…

Проросійські колективи швидко висловили солідарність з Іраном, посиливши атаки під гаслами на кшталт #OpIsrael і розширивши свою присутність на Близькому Сході. Тим часом антиіранські хактивісти провели набагато менше операцій, здебільшого символічного характеру. Аналітики підкреслюють, що, незважаючи на великий обсяг, реальні технічні збитки залишаються незначними; основною метою є психологічний тиск і домінування в наративі…

Експерти відзначають, що цей інцидент підкреслює, як кібероперації тепер повністю поєдналися з традиційними конфліктами. Глобальні ланцюги постачання та взаємопов'язана інфраструктура означають, що компанії далеко за межами регіону стикаються з побічним ризиком від зривів або інформаційної війни. Посилене глушіння GPS на Близькому Сході також підкреслює вразливість

супутникової навігації, що спонукає до створення багаторівневої оборони та альтернативних систем у таких критично важливих секторах, як морський транспорт. Очікується, що в найближчому майбутньому атаки будуть продовжуватися у вигляді деструктивних, малоскладних форм; у довгостроковій перспективі тиск, ймовірно, будуть чинити лише найбільш віддані державні суб'єкти». ***(Anna Ribeiro. Cyber retaliation surges after US–Israel strikes on Iran as hacktivists hit governments, defense, critical sectors // Industrial Cyber (https://industrialcyber.co/reports/cyber-retaliation-surges-after-us-israel-strikes-on-iran-as-hacktivists-hit-governments-defense-critical-sectors/). 10.03.2026).***

***

«Корпус вартових Ісламської революції (IRGC) відкрито заявила про свій намір проводити цілеспрямовані кібероперації проти «технологічної інфраструктури ворога» на Близькому Сході, що свідчить про значне посилення її наступальної кіберпозиції. Хоча конкретні країни не були названі, аналітики інтерпретують цю загрозу як спрямовану в першу чергу проти Ізраїлю, США, країн Перської затоки та їхніх критично важливих систем — енергетичних мереж, фінансових мереж, телекомунікацій та військових командних структур…

Кібернетичні можливості IRGC стабільно розвивалися з 2010 року, коли атака Stuxnet на ядерну програму Іранської Республіки спонукала до створення спеціального Командування кіберзахисту. Серед минулих операцій – руйнівна атака Shamoon 2012 року на Saudi Aramco, удари з метою знищення даних в OAE та Бахрейні, а також збій в роботі урядових служб Албанії 2022 року. Нинішнє оголошення переходить від таємних дій до відкритого стримування, слугуючи як демонстрацією можливостей, так і психологічним тиском.

Регіональні уряди реагують на це посиленням захисту, обміном інформацією про загрози в рамках Ради співробітництва країн Перської затоки та залученням західних союзників і приватних компаній для виявлення та реагування. Однак швидка цифровізація критичної інфраструктури, яка часто базується на застарілих системах, робить сектори енергетики, водопостачання, транспорту та фінансів вкрай вразливими до просунутих постійних загроз (APT) та порушень ланцюгів постачання…

Це посилює існуючі напруження навколо ядерної програми Ірану та конфліктів за посередництвом, підкреслюючи, що кіберпростір став основною ареною для ескалації, яку можна заперечити. Оскільки міжнародне право все ще намагається обмежити кіберагресію, що підтримується державою, дії IRGC ставлять під сумнів крихкі норми та підвищують ризик ланцюгових порушень у глобальних енергопостачаннях, фінансовій стабільності та регіональному мирі». ***(Iran's Revolutionary Guard Escalates Cyber Warfare with Strategic Targeting of Enemy Tech Infrastructure // Algona Business Ltd. (https://cryptorank.io/news/feed/6a742-iran-revolutionary-guard-cyber-targeting). 11.03.2026).***

***

«У вівторок парламент Албанії підтвердив, що зазнав складної кібератаки, спрямованої на видалення даних і порушення роботи внутрішніх систем, що змусило тимчасово призупинити роботу адміністративних електронних поштових служб, тоді як основні системи та публічний веб-сайт продовжували працювати. Проіранська група хактивістів Homeland Justice, яку західні чиновники та дослідники пов'язують з Корпусом вартових Ісламської революції (IRGC), швидко взяла на себе відповідальність за цю атаку, опублікувавши нібито викрадені парламентські повідомлення та заявивши, що ця операція є помстою за те, що Албанія надала притулок іранській опозиційній організації Муджахедін-е-Халк (MEK) у Дурресі. Інцидент стався на тлі ескалації регіональної напруженості після ударів США та Ізраїлю по Ірану і збігся з недавнім оголошенням лідера MEK Маріам Раджаві про створення тимчасового уряду в екзилі. Албанські власті не підтвердили заяви про злом і все ще проводять розслідування, але атака відповідає схемі операцій, пов'язаних з IRGC, спрямованих проти албанських установ з 2022 року…» ***(Daryna Antoniuk. Iran-linked hackers claim cyberattack on Albania's parliament email systems // Recorded Future News (https://therecord.media/iran-linked-hackers-claim-cyberattack-albania-parliament). 11.03.2026).***

***

«Польща успішно відбила кібератаку на Національний центр ядерних досліджень, попередні дані вказують на Іран як джерело атаки, хоча влада попереджає, що слід може бути навмисно виведений в оману. Міністр цифрових справ Кшиштоф Гавковський повідомив телеканалу TVN24+, що вторгнення, виявлене в останні дні, було зупинено до того, як воно завдало шкоди, і що об'єкт залишається в безпеці. Польща зіткнулася зі сплеском кібератак після вторгнення Росії в Україну в 2022 році, хоча Москва заперечує свою причетність… Інцидент стався на тлі посилення напруженості в регіоні після авіаударів США та Ізраїлю по Ірану 28 лютого, в результаті яких загинув верховний лідер аятолла Алі Хаменеї, що спонукало Іран до відповідних дій проти Ізраїлю та країн Перської затоки, де розташовані американські бази, а також до перекриття судноплавства через Ормузьку протоку. Служби безпеки продовжують розслідувати справжнє джерело нападу». ***(Poland says foiled cyberattack on nuclear centre may have come from Iran // Reuters (https://www.reuters.com/world/poland-says-foiled-cyberattack-nuclear-centre-may-have-come-iran-2026-03-12/). 12.03.2026).***

***

«Дослідники в галузі кібербезпеки попереджають про значне зростання активності хактивістів у відповідь на скоординовані військові кампанії США та Ізраїлю проти Ірану під кодовими назвами Epic Fury та Roaring Lion. За даними Radware, між 28 лютого та 2 березня 2026 року відбулася хвиля кібератак, зосереджена переважно на двох групах, Keymous+ та DieNet, на які припадало майже 70% активності. Загалом 149 DDoS-атак було спрямовано проти 110 організацій у 16 країнах, причому переважна більшість (107 атак) була зосереджена на Близькому Сході, а саме в Кувейті (28%), Ізраїлі (27,1%) та Йорданії (21,5%).

Урядовий сектор був найбільш ураженим у всьому світі, на нього припадало майже 48% атак…

Серед загроз можна виділити пропалестинські, проросійські та іранські угруповання, що фінансуються державою. Туніська група Hider Nex ініціювала першу DDoS-атаку, а проросійські угруповання, такі як Cardinal, заявили про злом ізраїльських військових мереж, зокрема Iron Dome. Тим часом в рамках активної SMS-фішингової кампанії використовується підроблена програма ізраїльського командування внутрішнього фронту для розгортання шкідливого програмного забезпечення для стеження. На державному рівні Ісламська революційна гвардія Ірану (IRGC) націлилася на регіональну енергетичну та цифрову інфраструктуру, включаючи Saudi Aramco, щоб завдати економічних збитків. Інші активні групи включають Cotton Sandstorm, яка відродила стару персону для атаки на Бахрейн, та спонсоровану державою UNC1549, яка зосереджується на аерокосмічній та оборонній галузях…

Експерти, серед яких колишня співробітниця ФБР Синтія Кайзер, відзначають, що Іран історично використовує кібероперації, все частіше застосовуючи програми-вимагачі, для помсти за політичні образи і часто залучає приватних кіберзлочинців, щоб зберегти оперативну гнучкість. Як наслідок, компанії з кібербезпеки, такі як SentinelOne і CrowdStrike, з високою впевненістю оцінюють, що організації в Ізраїлі, США та союзних країнах піддаються серйозному ризику прямого або непрямого нападу, особливо в критичній інфраструктурі, обороні та фінансах. Щоб зменшити ці ризики, організаціям настійно рекомендується активувати постійний моніторинг, оновлювати інформацію про загрози, зменшувати зовнішні поверхні атаки та забезпечувати належну сегментацію між IT-мережами та мережами операційних технологій, оскільки іранські супротивники вдосконалили свої методи, щоб швидко експлуатувати хмарні та гібридні корпоративні середовища». ***(Ravie Lakshmanan. 149 Hacktivist DDoS Attacks Hit 110 Organizations in 16 Countries After Middle East Conflict // The Hacker News (https://thehackernews.com/2026/03/149-hacktivist-ddos-attacks-hit-110.html). 04.03.2026).***

***

«Іранська група Seedworm (також відома як MuddyWater), що спеціалізується на створенням постійних загроз і діє під егідою Міністерства розвідки та безпеки Ірану, з початку лютого 2026 року активно проникає в мережі численних американських та канадських організацій. Ця діяльність значно посилилася після скоординованих ударів США та Ізраїлю по Ірану 28 лютого, що свідчить про те, що іранські кіберзлочинці використовують ескалацію геополітичної напруги для прискорення вторгнень у системи американських та союзних цілей… Дослідники компанії Symantec виявили, що зловмисники з угруповання Seedworm заздалегідь проникли в системи важливих об’єктів — зокрема американського банку, аеропорту, неурядових організацій та компанії-розробника програмного забезпечення, пов’язаної з оборонною галуззю, — що свідчить про те, що вони підготувалися ще задовго до початку військового конфлікту. Примітно, що перебої з інтернет-зв’язком на території Ірану не

зупинили ці операції, оскільки зловмисники діють на міжнародному рівні та використовують альтернативні мережі, такі як Starlink.

Ситуація з кіберзагрозами ще більше ускладнюється через пов’язані з Іраном хактивістські угруповання, такі як Handala та DieNet, причому останнє здійснює DDoS-атаки на об’єкти критичної інфраструктури США. У своїх останніх шпигунських кампаніях угруповання Seedworm застосувало два нещодавно виявлені бекдори: Dindoor (який запускається через середовище виконання Deno для уникнення виявлення) та Fakeset (на базі Python), обидва підписані спеціальними сертифікатами, пов’язаними з раніше створеною інфраструктурою загроз. Зловмисники також використовували завантажувач Stagecomp для доставки відомого бекдору Darkcomp і намагалися викрасти дані за допомогою легітимного інструменту Rclone. Для боротьби з цим багатошаровим середовищем загроз організаціям настійно рекомендується впровадити багатофакторну автентифікацію, відстежувати аномальні виходячі передачі даних, оновлювати правила брандмауера, обмежувати доступ до зовнішніх хмарних сховищ та зберігати незмінні резервні копії в офлайн-режимі…» ***(Tushar Subhra Dutta. Iran-Linked Hackers Target U.S. Critical Infrastructure Amid Rising Cyber Threat Activity // Cyber Security News (https://cybersecuritynews.com/iran-linked-hackers-target-u-s-critical-infrastructure/). 09.03.2026).***

***

«Конфлікт на Близькому Сході стрімко поширився на кіберпростір, створивши серйозну загрозу, що постійно зростає, для підприємств, фінансових установ, енергопостачальних компаній та операторів критичної інфраструктури не лише в цьому регіоні, а й у Європі та Північній Америці. Іранські суб'єкти, що фінансуються державою, разом із широкою мережею проіранських хактивістських угруповань, активно націлюються на західні комерційні, фінансові, енергетичні, медичні, телекомунікаційні, аерокосмічні, логістичні та інші критичні сектори, і на початок березня 2026 року дослідники виявили понад 60 активних груп загроз, пов'язаних із конфліктом, більшість із яких підтримують Іран. Замість того, щоб ослабнути, ці кібероперації посилилися, а серед нещодавніх інцидентів — атаки на північноамериканську компанію з виробництва медичного обладнання, зірвана атака на ядерний сектор Польщі, DDoS-кампанії проти інфраструктури країн Перської затоки, фішинг із використанням підроблених офіційних додатків для оповіщення, а також попередження в ОАЕ про можливе розгортання шкідливого програмного забезпечення типу «wiper», призначеного для остаточного знищення даних. Методи атак є різноманітними та багатошаровими, включаючи цільовий фішинг, викрадення облікових даних, зловживання VPN та периферійними пристроями, шкідливе програмне забезпечення типу «wiper», DDoS-атаки, кампанії «hack-and-leak», компрометацію ланцюгів постачання, смішинг, фішинг із використанням штучного інтелекту та навіть фізичні удари по цифровій інфраструктурі, такі як атаки дронів на центри обробки даних AWS в ОАЕ та Бахрейні, що демонструє, як кіберзагрози та фізичні загрози зливаються воєдино. Важливо, що цілі не

обмежуються організаціями, безпосередньо пов’язаними з конфліктом; будь-яка відома або символічно значуща структура може стати об’єктом нападу за нагоди…

Для організацій, що зазнали атаки, ризики виходять за межі технічних збоїв і поширюються на санкції, регуляторні, договірні та управлінські ризики. Оскільки іранська інфраструктура загроз може включати суб’єктів, на яких накладено санкції, будь-яка виплата викупу або передача коштів може порушувати законодавство про санкції, зокрема за правилами США, що наражає компанії та навіть керівництво на суворі цивільні та кримінальні санкції. Водночас серйозний інцидент може спричинити численні обов’язки щодо повідомлення відповідно до законів про захист даних, нормативних актів з кібербезпеки, таких як британська система NIS або NIS2 ЄС, галузевих систем звітності у сфері фінансів та охорони здоров’я, а також правил, що стосуються операторів критичної національної інфраструктури. Атаки типу «Wiper» та руйнівні DDoS-інциденти також можуть спричинити серйозні перебої в роботі бізнесу, що породжує питання щодо форс-мажорних обставин, невиконання договірних зобов’язань, відповідальності перед клієнтами та партнерами, а також навіть відповідальності керівництва компанії у випадках, коли не було вжито належних заходів з кібербезпеки. Загалом, кібервимір конфлікту на Близькому Сході став одним із найскладніших середовищ загроз, з якими зараз доводиться стикатися, поєднуючи атаки, що підтримуються державою, ідеологічно мотивований хактивізм, інструменти на основі штучного інтелекту та потенціал реального пошкодження інфраструктури, що означає, що організації повинні підтримувати підвищену готовність до захисту та готуватися як до юридичних, так і до операційних наслідків». ***(Arran Roberts, Alexandra O'Hare, Joshua Mooney. Iran’s cyber warfare: legal implications for businesses // Kennedys Law LLP (https://www.kennedyslaw.com/en/thought-leadership/article/2026/iran-s-cyber-warfare-legal-implications-for-businesses/). 17.03.2026).***

***

«Ескалація збройного конфлікту на Близькому Сході суттєво підвищує кіберризики для австралійських організацій, оскільки війна та загальне зростання геополітичної напруженості провокують збільшення кількості кібератак, що здійснюються за підтримки держав або через посередників, проти критичної інфраструктури, фінансових служб, урядових та приватних структур по всьому світу. Такі атаки часто спрямовані на порушення роботи життєво важливих служб, ланцюгів постачання та економічної стабільності. Компанії, що займаються аналітикою кіберризиків, повідомляють про посилення активності з початку конфлікту, зокрема про збільшення кількості випадків фішингу, інцидентів із використанням програм-вимагачів, витоку даних та шкідливого програмного забезпечення, спрямованого проти енергетичних систем, фінансових установ та урядових мереж, а взаємопов’язаний характер ланцюгів постачання означає, що організації, розташовані далеко від регіону, зокрема в Австралії, можуть зазнати значного непрямого впливу…

З огляду на це, Національний центр кібербезпеки Великої Британії попередив, що всі галузі повинні очікувати посилення атак, спрямованих на спричинення масштабних економічних збитків — особливо ті, що залежать від Близького Сходу,

— тоді як Австралійський центр кібербезпеки (ACSC) опублікував попередження про активність досвідчених зловмисників, які використовують мережеву інфраструктуру…

Оскільки сучасні конфлікти часто поширюються на кіберпростір, організації, що зазнали впливу, можуть зіткнутися не лише з порушенням операційної діяльності, а й з обов'язковими вимогами щодо звітності, ретельним контролем з боку правоохоронних органів, репутаційними та фінансовими збитками, а також судовими позовами, що вимагає вжиття таких рекомендованих негайних заходів, як офіційне визнання та нагляд з боку ради директорів щодо ситуації підвищеної загрози, проактивний моніторинг ACSC та інших джерел інформації про загрози (включаючи налаштування систем виявлення відповідно до сучасних тактик та залучення постачальників керованих послуг, де це доречно), терміновий перегляд умов кіберстрахування на предмет виключень, пов'язаних з війною або діями держав, оперативне тестування планів реагування на інциденти за допомогою навчань на основі сценаріїв, а також цілеспрямовану переоцінку ланцюгів постачання та залежності від третіх сторін — особливо постачальників, пов'язаних із постраждалим регіоном або тих, що підтримують критично важливі технології та інфраструктуру». ***(Simon Burns, Christopher Flynn and Ross Phillipson. Heightened cybersecurity risk from Middle East conflict: key actions for boards and management // Gilbert + Tobin (https://www.gtlaw.com.au/insights/heightened-cybersecurity-risk-from-middle-east-conflict-key-actions-for-boards-and-management). 23.03.2026).***

***

«Американські чиновники підтвердили, що особистий акаунт Gmail директора ФБР Каша Пателя був зламаний групою хакерів «Handala Hack Team», пов'язаною з іранською державою. Ця група, яка нещодавно також взяла на себе відповідальність за кібератаку на гіганта медичної техніки Stryker, оприлюднила архів приватних фотографій, документів та електронного листування Пателя за період з 2010 по 2019 рік. Хакери представили цей злом як відповідь на нещодавні дії правоохоронних органів США, спрямовані проти їхньої цифрової інфраструктури… Хоча оприлюднені матеріали містять переважно неформальні знімки Пателя — наприклад, як він курить сигари чи робить селфі перед дзеркалом — і заяви хакерів про наявність більш конфіденційних даних залишаються неперевіреними, цей інцидент викликав серйозні занепокоєння щодо оперативної безпеки. Незважаючи на те, що зламаний поштовий ящик не був офіційною урядовою системою, успішний злом особистої пошти директора ФБР вказує на потенційні вразливості та ризик витоку даних про минулі контакти. Точний спосіб вторгнення — чи то фішинг, повторне використання облікових даних, чи інша тактика — залишається невідомим, оскільки розслідування триває…» ***(Alex Lekander. Iranian hackers breach FBI director's personal email and leak photos // CyberInsider (https://cyberinsider.com/iranian-hackers-breach-fbi-directors-personal-email-and-leak-photos/). 27.03.2026).***

***

«Уряд Японії ухвалив рішення дозволити Силам самооборони проводити наступальні кібероперації з 1 жовтня, посилаючись на дедалі складнішу ситуацію в галузі національної безпеки — найскладнішу з часів Другої світової війни — та зростаючу залежність суспільства від цифрових систем. Головний секретар Кабінету міністрів Мінору Кіхара заявив, що кібератаки зараз спричиняють значні порушення повсякденного життя та економічної діяльності, а отже, становлять серйозну загрозу національній безпеці, що спонукало уряд доопрацювати нормативні акти, які дозволяють застосовувати підхід «проактивної кіберзахисту», передбачений законодавством, прийнятим минулого року. Згідно з новою системою, урядовий комітет з кібербезпеки розглядатиме та затверджуватиме або відхилятиме запити на початок операцій; після отримання дозволу японська поліція та Силиам самооборони матимуть право «атакувати та виводити з ладу» інфраструктуру, що використовується для здійснення кібератак, одночасно захищаючи приватність громадян…

Цей крок є черговим переосмисленням конституційних обмежень Японії щодо військової агресії, встановлених після 1946 року — згідно зі статтею 9, її збройні сили чітко визначені як оборонні — і продовжує тривалий процес еволюції у тому, як Японія визначає дії, що відповідають самообороні. Японія приєднується до ширшої групи країн, що мають наступальні кіберможливості; Міжнародний інститут стратегічних досліджень оцінює, що принаймні 26 країн можуть здійснювати кібератаки, причому США посідають перше місце серед кібердержав, кілька країн вважаються другорядними, а Японія належить до третього рівня, що має певні сильні сторони, але й помітні прогалини, що свідчить про те, що Японія прагне усунути недоліки у своїх можливостях, розширюючи свою кіберпозицію». ***(Simon Sharwood. Japan to allow 'proactive cyber-defense' from October 1st // The Register (https://www.theregister.com/2026/03/18/japan_proactive_cyber_defense_enabled/). 18.03.2026).***

***

Кіберзахист критичної інфраструктури

«Кіберзагрози для систем водопостачання та водовідведення перетворилися з теоретичних ризиків на реальні небезпеки, які можуть підірвати довіру громадськості, поставити під загрозу безпеку та порушити роботу життєво важливих служб. У відповідь на цей нагальний виклик компанія Microsoft спільно з Інститутом кіберготовності (CRI) та Центром кібертехнологій та інновацій (CCTI) опублікувала звіт, у якому аналізується рівень кіберготовності у водогосподарському секторі та ефективність практичних заходів. Звіт базується на пілотній програмі, яка поєднувала безкоштовне навчання з кібербезпеки, орієнтоване на поведінку, з практичним наставництвом від сертифікованих CRI

кібертренерів, щоб допомогти комунальним підприємствам перетворити отримані знання на операційні політики, посібники та плани реагування на інциденти…

Пілотний проект дав три важливі висновки: по-перше, комунальні підприємства-учасники продемонстрували міцніші основи кібербезпеки, більшу впевненість у реагуванні на інциденти та виявлення раніше пропущених вразливостей, таких як відсутність планів забезпечення безперебійної роботи та слабкі протоколи паролів; по-друге, комунальні підприємства, які отримували індивідуальне наставництво, мали значно більшу ймовірність завершити програму, ніж ті, що навчалися самостійно; і по-третє, незважаючи на високий інтерес — про що свідчить 113 комунальних підприємств, які висловили початковий інтерес, 72, які розпочали, та 43, які завершили програму — обмеження ресурсів, включаючи нестачу персоналу, обмежене фінансування та залежність від сторонніх постачальників, продовжують перешкоджати повному впровадженню. Завдяки цим позитивним результатам програма стала постійною, надаючи водопостачальним підприємствам постійний доступ до практичного навчання та підтримки…

Результати дослідження свідчать про те, що політикам та зацікавленим сторонам галузі необхідно вийти за межі простого обміну інформацією та надавати сталу практичну допомогу у впровадженні заходів через авторитетні галузеві асоціації, на які комунальні підприємства вже покладаються. Ефективні стратегії повинні передбачати включення вимог щодо кібербезпеки до процедур професійного ліцензування та безперервної освіти з метою стимулювання участі, водночас визнаючи, що лише безкоштовні ресурси не можуть подолати структурні обмеження потужностей. Ця ініціатива доповнює більш широке зобов’язання Microsoft щодо позитивного впливу на водний баланс — мінімізації споживання та поповнення ресурсів — шляхом зміцнення операційної стійкості комунальних підприємств, що обслуговують громади по всьому світу». ***(Amy Hogan-Burney. New findings show how hands-on support can improve water sector cybersecurity // Microsoft (https://blogs.microsoft.com/on-the-issues/2026/03/19/how-hands-on-support-can-improve-water-sector-cybersecurity/). 19.03.2026).***

***

«Новий звіт консалтингової компанії з кібербезпеки Bridewell показав, що кібератаки зараз є майже повсюдним явищем у критичній національній інфраструктурі Великої Британії: 93% опитаних організацій зазнали принаймні одного успішного кіберинциденту протягом минулого року. Найпоширенішими наслідками стали порушення роботи IT-систем або їхні відключення, з якими зіткнулася половина респондентів, а також більш масштабні операційні збої, що торкнулися 34% опитаних. Фінансові та операційні наслідки також були значними: 36% збільшили бюджети на кібербезпеку у відповідь на інциденти, 31% повідомили про втрату доходів, а 31% зазнали втрати даних. Фішинг та компрометація ділової електронної пошти були визначені як основні точки входу, в середньому 11 атак на організацію щорічно, тоді як шкідливе програмне забезпечення становило в середньому вісім інцидентів, а програмне забезпечення для вимагання викупу, атаки на ланцюги постачання та крадіжка даних — по шість. Застарілі системи та труднощі з встановленням виправлень,

особливо в секторах з великою кількістю активів, таких як транспорт та комунальні послуги, також відіграли значну роль: застаріле програмне забезпечення або недоступні виправлення згадувалися в середньому у семи атаках…

У звіті також наголошується на зміні пріоритетів організацій: хоча захист даних та конфіденційність залишаються головним питанням для 43% респондентів, управління кіберризиками, пов'язаними зі штучним інтелектом, різко набрало обертів і зараз є другою за важливістю проблемою, яку назвали 39% опитаних. Організації все більше турбуються не тільки тим, хто саме має доступ до конфіденційних даних, а й тим, які системи та агенти штучного інтелекту можуть це робити і за яких умов. Bridewell попереджає, що штучний інтелект поширюється в організаціях так само, як колись поширювалася «тіньова IT» — швидко, корисно, але часто без належного контролю…

У звіті також зазначається, що зловмисники за лічені хвилини переходять від отримання початкового доступу до викрадення даних, тому надзвичайно важливими є оперативне виявлення та реагування. Водночас організації часто стикаються з труднощами не в теоретичному плануванні відновлення, а в ухваленні швидких і впевнених оперативних рішень під час реального інциденту. Bridewell також вказує на зростаюче навантаження, спричинене стрімким переходом на хмарні технології, яке випереджає темпи підготовки персоналу, можливості моніторингу та управління оновленнями, особливо у фрагментованих технологічних середовищах. Загалом, результати дослідження показують, що критична інфраструктура Великої Британії стикається з постійними та еволюціонуючими кіберзагрозами, а для забезпечення стійкості необхідні постійні інвестиції не лише в засоби контролю доступу, а й у навички, зрілість систем виявлення, реагування на інциденти та безпеку на етапі проектування». ***(Thomas Johnson. 93% of UK critical national infrastructure operators faced cyber attacks in past year // EMAP Publishing Limited (https://www.newcivilengineer.com/latest/93-of-uk-critical-national-infrastructure-operators-faced-cyber-attacks-in-past-year-20-03-2026/). 20.03.2026).***

***

«Після тривожного сигналу, яким стала атака на Colonial Pipeline, сформувалася нова реальність, в якій зловмисники, що діють за підтримки держави, все частіше націлюються на критичну національну інфраструктуру, зокрема електростанції, військові мережі та ядерні об'єкти. На відміну від комерційних підприємств, державні органи стикаються з супротивниками, що мають величезні ресурси та геополітичні мотиви, чиїми цілями є саботаж та шпигунство, а не фінансова вигода. Цей особливий ландшафт загроз вимагає спеціалізованого підходу, відомого як «суверенна кіберрозвідка», який зосереджується на зборі та аналізі даних про загрози саме для захисту інтересів національної безпеки…

Важливо, що цей метод є проактивним: він виходить за межі простої реакції на інциденти, відстежуючи плани та комунікації зловмисників на таких платформах, як форуми даркнету, щоб отримати попередження ще до початку атаки. Він об'єднує різні напрямки розвідки — кіберрозвідку, розвідку з відкритих джерел,

радіоелектронну розвідку та геополітичну розвідку — для забезпечення всебічного розуміння загроз та їхніх стратегічних наслідків. Потреба в такому підході стала нагальною, оскільки межі між кібероперaціями в мирний і воєнний час стираються, а супротивники постійно виявляють вразливі місця в критичній інфраструктурі та використовують слабкі місця ланцюгів постачання, щоб отримати непрямий доступ до добре захищених цілей…

Наразі розробляються спеціалізовані платформи, покликані підтримати цю стратегію шляхом забезпечення глибокого розуміння підпільних екосистем, зіставлення технічних даних із геополітичним контекстом та надсилання сповіщень у режимі реального часу про загрози для вразливих секторів. Зрештою, оскільки реактивні моделі кібербезпеки виявляються недостатніми для протидії стратегічним загрозам з боку держав, проактивна суверенна кіберрозвідка стає невід'ємною складовою сучасної національної безпеки…» ***(What Is Sovereign Cyber Intelligence — And Why Government Agencies Can No Longer Ignore It // Cyble Inc. (https://cyble.com/knowledge-hub/what-is-sovereign-cyber-intelligence/). 12.03.2026).***

***

«Супутники забезпечують функціонування багатьох життєво важливих служб — GPS-навігації та синхронізації часу, прогнозування погоди, глобальних комунікацій та оборони — і зростаюча залежність від цієї космічної інфраструктури посилює наслідки кібератак на неї. Оскільки супутники керуються через наземні станції та канали зв'язку, які можуть бути скомпрометовані, зловмисники, які отримають доступ, можуть порушити роботу систем, маніпулювати даними або, можливо, захопити контроль; при цьому супутники є особливо складними цілями, оскільки їх важко ремонтувати чи оновлювати, коли вони вже знаходяться на орбіті. Основною проблемою є перешкоди та підробка сигналів, коли фальшиві сигнали вводять в оману супутники або користувачів; наприклад, порушення роботи GPS може вплинути на авіацію, судноплавство, реагування на надзвичайні ситуації та фінансові системи, які покладаються на точний час, а скоординовані атаки на декілька супутників можуть спричинити транскордонні порушення у багатьох галузях…

Більш серйозні сценарії передбачають ланцюгові збої: якщо кібератака змінить траєкторію руху супутника, це може підвищити ризик зіткнення та спричинити утворення космічного сміття, яке пошкодить інші супутники, що породжує побоювання щодо ланцюгової реакції, пов'язаної з синдромом Кесслера, яка може зробити частини орбіти непридатними для використання на довгі роки. Геополітична напруга посилює цю загрозу, оскільки держави розвивають свої можливості у сфері кібер- та космічної війни і можуть використовувати кібероперації, спрямовані проти супутників, як стратегічні інструменти для виведення з ладу інфраструктури супротивника без відкритих військових дій. Незважаючи на це, повномасштабний «супутниковий апокаліпсис» залишається малоймовірним у найближчій перспективі, оскільки космічні агентства та комерційні оператори посилюють захист за допомогою шифрування, безпечного зв'язку та постійного моніторингу, а також завдяки розвитку міжнародної співпраці та регуляторних заходів; проте зростаюча складність загроз робить постійну

пильність та інвестиції в кібербезпеку супутників критично важливим пріоритетом». ***(Naveen Goud. How can Cyber Attacks trigger Satellite Apocalypse // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/how-can-cyber-attacks-trigger-satellite-apocalypse/). 23.03.2026).***

***

«У зв'язку з нещодавніми кібератаками, пов'язаними з іранським конфліктом, Національне агентство з кібербезпеки Греції опублікувало попереджувальне повідомлення найвищого пріоритету, в якому закликає судновласників та компанії у критично важливих секторах — зокрема у банківській, транспортній, медичній та енергетичній галузях — перевірити свої ІТ-системи на наявність ознак злому. Це попередження з'явилося після того, як група, пов'язана з Іраном, взяла на себе відповідальність за атаку на американську медичну компанію Stryker, а також після нещодавно зірваної атаки на парламент Албанії групою, що називає себе «Homeland Justice»…

У грецькій директиві організаціям було наказано виявляти конкретні індикатори загрози, такі як IP-адреси іранського походження та троян віддаленого доступу VShell, які, за повідомленнями, використовує досвідчений зловмисник, що застосовує дворівневу інфраструктуру для уникнення виявлення. Хоча грецькі джерела поки що не повідомляють про значні порушення, незважаючи на фіксацію деяких незначних підозрілих дій, морська галузь залишається в стані підвищеної готовності через одночасне зростання електронних перешкод у роботі комерційних навігаційних систем поблизу Ормузької протоки. У відповідь на цю загальну тенденцію кібервійни Албанія, яка раніше розірвала дипломатичні відносини з Іраном через хакерські атаки, спонсоровані державою, у 2022 році, успішно відбила останні вторгнення та ухвалила парламентську резолюцію, офіційно оголосивши Іран державою-спонсором тероризму». ***(Renee Maltezou, Yannis Souliotis. Greek firms scan computer systems as Iran war raises cyberattack risks, sources say // Reuters (https://www.reuters.com/world/middle-east/greek-firms-scan-computer-systems-iran-war-raises-cyberattack-risks-sources-say-2026-03-18/). 18.03.2026).***

***

Кіберзахист промислових об'єктів

«Згідно з новим глобальним опитуванням 473 керівників автомобільної промисловості, проведеним ABB Robotics and Automotive Manufacturing Solutions, кібербезпека випередила скорочення витрат, гнучке виробництво та впровадження штучного інтелекту як головну проблему для сектора. Опитування показує фундаментальну зміну пріоритетів: 95% респондентів вважають кібербезпеку «важливою», а 53% — «надзвичайно важливою», що робить її головним пріоритетом у всіх регіонах та на всіх рівнях постачальників на найближчі п'ять років. Таке посилення уваги зумовлене швидкою інтеграцією підключених технологій на виробничих майданчиках, таких як передова робототехніка, штучний інтелект та цифрові двійники, які забезпечують значне

підвищення продуктивності, але вимагають безпечних підключень для надійної роботи…

На відміну від попередніх років, коли кіберризики були лише однією з багатьох проблем, виробники тепер усвідомлюють, що кіберінциденти можуть зупинити виробництво та порушити ланцюги постачання навіть у середовищах, які не підключені безпосередньо до Інтернету. Йорг Регер, керуючий директор автомобільного підрозділу ABB Robotics, зазначає, що кібербезпека перетворилася на «основну дисципліну виробництва». Замість того, щоб уникати цифровізації — понад 90% респондентів планують збільшити використання штучного інтелекту, великих даних і цифрових двійників — виробники вимагають більш надійних гарантій безпечного та стійкого впровадження, особливо з наближенням таких нормативних актів, як Закон ЄС про кіберстійкість. Отже, галузь потребує безпечних за своєю конструкцією рішень, які забезпечують контроль над підключенням, одночасно надаючи розширені цифрові можливості». ***(Cybersecurity is now a bigger worry for car-makers than costs // DFA Media Group (https://drivesncontrols.com/cybersecurity-is-now-a-bigger-worry-for-car-makers-than-costs/). 04.03.2026).***

***

«Хоча центри обробки даних є основою світової цифрової економіки, оператори, які приділяють велику увагу енергоефективності та резервуванню, часто не беруть до уваги критичну вразливість: кібербезпеку основних систем будівлі. Такі основні функції, як охолодження, опалення, пожежогасіння та розподіл електроенергії, керуються тісно інтегрованими системами управління будівлею (BMS) та платформами управління інфраструктурою центрів обробки даних (DCIM), які об’єднують IT-середовища та середовища операційних технологій (OT)… Оскільки ці системи базуються на промислових протоколах, які ставлять сумісність вище за безпеку, вони створюють значну площину атаки. Зловмисникам не потрібно викрадати дані, щоб завдати серйозної шкоди; навіть просте змінення заданих значень температури або відключення сигналізації може призвести до катастрофічного виходу з ладу обладнання та простою, про що свідчать нещодавні випадкові відключення систем охолодження в Австралії та Сінгапурі, які спричинили масштабні перебої в роботі.

Загроза постійно еволюціонує: є дані, що свідчать про те, що зловмисники використовують шкідливі програми, такі як ShadowPad і PIPEDREAM, зловживають викраденими обліковими даними та проводять розвідку, спрямовану саме на ці операційні мережі з метою вимагання та порушення їхньої роботи. Оскільки попит на обчислювальні потужності для штучного інтелекту стимулює стрімке розширення центрів обробки даних та впровадження тісно інтегрованих технологій терморегулювання, цей ризик буде лише зростати… Щоб протидіяти цьому, оператори повинні переосмислити поняття стійкості об’єктів, впровадивши перевірені рамки кібербезпеки для операційних технологій (OT), наприклад, розроблені Інститутом SANS (SysAdmin, Audit, Network, Security). Впроваджуючи захищені архітектури, що розділяють мережі IT та OT, забезпечуючи безпеку віддаленого доступу та здійснюючи постійний моніторинг промислових

протоколів, оператори можуть захистити фізичну інфраструктуру, яка забезпечує функціонування цифрового світу, не гальмуючи при цьому технологічних інновацій». ***(Conor McLaren. The cybersecurity blind spot in data center building systems // Data Centre Dynamics Ltd (DCD) (https://www.datacenterdynamics.com/en/opinions/the-cybersecurity-blind-spot-in-data-center-building-systems/). 06.03.2026).***

***

«Промислові кіберзагрози в середовищах операційних технологій (OT) рідко проявляються явно; натомість вони часто виглядають як звичайна технологічна діяльність, доки у фізичному світі не трапляється якась проблема, наприклад, занадто раннє відкриття клапана, прийняття контролером неправомірної команди або виявлення операторами того, що поведінка установки більше не відповідає очікуваним умовам. Оскільки ці атаки мають кіберфізичний характер, реагування на інциденти в OT суттєво відрізняється від традиційного реагування в IT. У промислових умовах пріоритети зосереджені насамперед на безпеці, надійності та доступності, а конфіденційність відходить на другий план. Скомпрометовані PLC (програмовані логічні контролери), контур управління, система інструментальної безпеки (SIS) або базова система управління процесами (BPCS) можуть за лічені хвилини спричинити пошкодження обладнання, шкоду навколишньому середовищу або травмування людей, тому типові заходи реагування в IT, такі як негайне ізолювання або агресивне сканування, можуть насправді створити небезпечні умови експлуатації. Як наслідок, реагування в OT вимагає ретельного балансу між локалізацією загрози та підтриманням стабільної роботи…

У таких рекомендаціях, як NIST SP 800-82, повідомленнях ICS-CERT та стандарті IEC 62443, наголошується, що рішення щодо операційних технологій (OT) повинні враховувати реальні наслідки, зокрема ризики для людей, обладнання та навколишнього середовища. Експерти, на яких посилається Industrial Cyber, послідовно наголошують, що інциденти в операційних технологіях (OT) необхідно розглядати, ставлячи на перше місце безпеку, потім — безперебійність роботи, потім — цілісність системи, і лише потім — конфіденційність. Це фактично перевертає традиційну IT-тріаду CIA. Пол Шейвер з Mandiant зазначив, що, особливо в критичній інфраструктурі, відновлення роботи та виробництва часто є головним пріоритетом, але для безпечного виконання цього завдання необхідна участь інженерних, операційних, екологічних та безпекових команд, а іноді й третіх сторін, а не лише звичайної CSIRT. Мері Ганнон з GuidePoint Security також підкреслила, що інциденти в OT завжди повинні оцінюватися з огляду на їхній вплив на людей, процеси та навколишнє середовище. Майкл Метцлер із Siemens додав, що «безпечний стан» і «захищений стан» не завжди є одним і тим самим, а це означає, що кожна дія з локалізації повинна оцінюватися з огляду на її фізичні наслідки. Майк Холкомб також підкреслив, що реагування на інциденти в OT/ICS залежить від міждисциплінарної координації між кібербезпекою, інженерією та операційною діяльністю.

Виявлення загроз у сфері операційних технологій (OT) також ускладнюється тим, що зловмисники дедалі частіше маскуються під легітимні промислові протоколи, такі як Modbus та Common Industrial Protocol (CIP), вбудовуючи шкідливі команди у звичайний трафік. Це робить традиційний моніторинг недостатнім і підвищує необхідність у поведінковому аналізі, глибокому аналізі пакетів, перевірці на рівні 7 з урахуванням особливостей додатків та пасивному моніторингу. Ефективне виявлення залежить від того, чи розумієш, як виглядає нормальна робота на заводі. Експерти наголосили на важливості базових робочих параметрів, записів архіву даних, журналів OT та неінтрузивного моніторингу для виявлення аномалій, таких як незрозумілі зміни заданих значень або непідтримувані умови процесу. Навіть з автоматичними сповіщеннями людський досвід залишається важливим, оскільки промислові фахівці повинні інтерпретувати виявлення в контексті реальної роботи заводу…

Прийняття рішень під час кіберкризи в сфері операційних технологій (OT) також вимагає іншої моделі управління, ніж у сфері інформаційних технологій (IT). Оскільки часто доводиться обирати між ізоляцією систем для локалізації загрози та підтримкою виробничих процесів, щоб уникнути небезпечних або дорогих перебоїв у роботі, повноваження повинні бути чітко визначені ще до виникнення інциденту. Експерти рекомендують розробляти плани реагування на інциденти, що стосуються саме OT, проводити навчальні тренування, розробляти процедури для конкретних об'єктів та створювати централізовані структури прийняття рішень, такі як посада керівника з реагування на інциденти. Команди з безпеки можуть здійснювати моніторинг, проводити сортування та рекомендувати дії, але остаточні рішення, що впливають на фізичні процеси, повинні залишатися за керівництвом заводу та особами, відповідальними за операції. Ця модель управління є особливо важливою, оскільки ситуативні рішення під час інциденту в OT можуть створити таку ж небезпеку, як і сама атака.

Відновлення та перезапуск є однаково ризикованими процесами. Перед тим, як санкціонувати «холодний» перезапуск, організації повинні перевірити цілісність логіки PLC, конфігурацій інженерних робочих станцій, операційних систем, облікових даних, прошивки RTU та інших об’єктів операційних технологій (OT) на відповідність перевіреним еталонним значенням, «золотим» образам та файлам конфігурації. Залежно від масштабів впливу, відновлення може варіюватися від порівняння конфігурацій до повного процесу повторного введення в експлуатацію, що триває кілька днів або навіть місяців. Експерти попередили, що перезапуск систем без розуміння першопричини вторгнення або перевірки того, що скомпрометована логіка та механізми персистентності були видалені, створює ризик повторного проникнення зловмисника в діючі операції. Оскільки в багатьох OT-середовищах все ще відсутній належний моніторинг, організаціям часто важко точно визначити, що саме сталося під час інциденту, що робить відновлення особливо складним і вимагає додаткової обережності.

Захист застарілих активів рівня 1, таких як датчики та виконавчі механізми, є ще одним серйозним викликом, оскільки ці системи часто не підтримують оновлення і ніколи не були розроблені для сучасних мережевих підключень. У таких випадках акцент слід перенести з захисту самого пристрою на захист

навколишнього середовища. Експерти рекомендують застосовувати надійну сегментацію мережі, мікросегментацію, суворий контроль доступу, фізичну безпеку, пасивне виявлення активів, захист комірок, промислові брандмауери, шифрування VPN та постійний моніторинг вразливостей...Загалом, головний висновок полягає в тому, що інциденти в OT вимагають принципово іншого реагування, ніж інциденти в IT: такого, що базується на безпеці людей, безперебійності роботи, міждисциплінарній координації, ретельній перевірці та стійкій промисловій архітектурі». ***(Anna Ribeiro. Crisis lessons from OT incident response as cyber-physical attacks unfold within normal industrial operations // Industrial Cyber (https://industrialcyber.co/features/crisis-lessons-from-ot-incident-response-as-cyber-physical-attacks-unfold-within-normal-industrial-operations/). 22.03.2026).***

***

Кіберзахист закладів охорони здоров'я

«Через два роки після руйнівної кібератаки на Change Healthcare, яка порушила надання медичної допомоги пацієнтам і призвела до витоку конфіденційних даних, Конгрес вживає заходів для зміцнення системи охорони здоров'я країни проти подібних загроз. У рідкісному прояві двопартійності комітет Сенату з питань охорони здоров'я 22 голосами проти 1 просунув законопроєкт, який посилить координацію між федеральними агентствами, зобов'яже Міністерство охорони здоров'я та соціальних служб створити комплексний план реагування на інциденти та встановить гранти, щоб допомогти лікарням та іншим постачальникам послуг підготуватися до кібератак і відновитися після них. Законопроєкт також передбачає ключові заходи безпеки — багатофакторну автентифікацію та шифрування даних — які були явно відсутні під час порушення безпеки в 2024 році…

Законодавці та експерти стверджують, що цей захід є відповіддю на «облогу» сектора: сфера охорони здоров'я постійно страждає від найдорожчих випадків порушення безпеки даних, які в середньому коштують близько 10 мільйонів доларів за інцидент, часто з боку зарубіжних хакерів, які знаходяться поза межами досяжності правоохоронних органів США. Сенатор Білл Келсі (республіканець від Луїзіани) та інші спонсори описують цю ініціативу як спосіб зміцнити захист і захистити доступ пацієнтів до медичної допомоги. Пропозиція займає центристську позицію після того, як попередні, більш суворі законопроєкти демократів зустріли опір з боку медичної галузі, що дає їй кращі перспективи для прийняття. Незважаючи на це, лікарні залишаються обережними щодо нових зобов'язань з дотримання вимог, а законопроєкт стикається з процедурними перешкодами — переповненим календарем Конгресу, наближенням виборів та не пов'язаними з ним суперечками щодо політики в галузі охорони здоров'я — що може затримати остаточне голосування…

Ця міра отримала підтримку від ключових груп у галузі охорони здоров'я, включаючи Healthcare Trust Institute та Blue Cross Blue Shield Association, які

наголошують, що викрадені медичні дані є одними з найцінніших товарів на чорному ринку, а кіберінциденти можуть буквально становити загрозу для життя людей, оскільки зупиняють надання медичної допомоги. Як зазначають прихильники, увага Конгресу до кібербезпеки в галузі охорони здоров'я нарешті набирає обертів; залишається питання, чи витримає цей імпульс політичні відволікання, що чекають на нас у майбутньому…» ***(Peter Sullivan. Congress plans new response to health cyberattacks // Axios Media Inc. (https://www.axios.com/2026/03/09/congress-health-cyberattacks-cyber-security). 09.03.2026).***

***

«Компанія Stryker, що виробляє медичне обладнання, повідомила, що її діяльність поступово повертається до повної потужності після кібератаки 11 березня, яка порушила роботу систем обробки замовлень, виробництва та відвантаження. Компанія заявила, що більшість виробничих майданчиків та критично важливих ліній відновлено, а електронні системи замовлень знову працюють, і вона продовжує виконувати та доставляти замовлення… Атака, відповідальність за яку взяла на себе пов'язана з Іраном хакерська група Handala як помсту за удар по Ірану, зачепила пристрої під управлінням Microsoft Windows, зокрема ноутбуки та мобільні системи, підключені до мережі Stryker. Stryker співпрацює з експертами з кібербезпеки та органами влади, які розслідують інцидент, а її акції зросли, коли стало очевидним прогрес у відновленні роботи…» ***(Stryker says manufacturing mostly restored after cyberattack // Reuters (https://www.reuters.com/business/stryker-says-manufacturing-mostly-restored-after-cyberattack-2026-03-26/). 26.03.2026).***

***

«…У сфері охорони здоров'я кібератаки є неминучими, проте їхній вплив — фінансові втрати, шкода репутації і, перш за все, безпека пацієнтів — можна значно зменшити, якщо кіберстійкість розглядати як стратегічну необхідність на рівні правління, а не як проблему ІТ. Лише 27 % правлінь регулярно обговорюють питання кібербезпеки, але випадок порушення безпеки через програмне забезпечення-вимагач у 2024 році, який порушив роботу 74 % лікарень США, підкреслює, чому нагляд є критично важливим. Охорона здоров'я залишається найбільш вразливим сектором, що пояснюється високою цінністю медичних даних, поширеністю застарілих систем та низьким рівнем кіберзрілості (лише 13 % організацій досягли високого рівня)…

Ефективна стійкість вимагає цілісного підходу в масштабах всього підприємства: чітких пріоритетів відновлення, міжфункціональної координації, ретельного тестування та суворих стандартів для постачальників. Правління повинні перейти від пасивних оновлень до активного управління, задаючи конкретні питання — про критично важливі системи, ризики постачальників, перевірені терміни відновлення та узгодженість інвестицій — і наполягати на вимірюваному прогресі. Ця робота базується на п'яти ключових аспектах: стратегічна ясність щодо того, що ніколи не повинно виходити з ладу, безперебійні

міжфункціональні ролі в кризових ситуаціях, перевірені інструкція та навчання, суворий контроль сторонніх осіб та пристроїв, а також цільові інвестиції, підкріплені прозорими показниками та бенчмаркінгом…

Коли ради директорів ставлять кіберстійкість в центр своєї відповідальності, вони не тільки скорочують час відновлення та обмежують шкоду, але й захищають пацієнтів, зберігають довіру та забезпечують майбутнє організації в умовах постійно мінливого середовища загроз». ***(Russell Schaefer, Tom Retelewski, Adrian Ciuffetelli, Tad Roselund. Cyber Attacks Are Inevitable in Health Care. Patients Don't Have to Pay the Price // Boston Consulting Group (https://www.bcg.com/publications/2026/cyber-attacks-in-health-care-are-inevitable). 09.03.2026).***

***

«Велика лікарня в Щецині, на північному заході Польщі, працює в «паперовому режимі» з суботи пізно ввечері, коли хакери вивели з ладу її ІТ-мережу. Атака програм-вимагачів заблокувала персоналу доступ до медичних записів та інших критично важливих систем, після чого було висунуто вимогу про виплату «кількох мільйонів доларів» за відновлення доступу. Міністр оборони Польщі направив кіберкоманду Територіальних сил оборони для допомоги у відновленні та захисті мережі, але через чотири дні основна система все ще не працює; лише кілька робочих станцій, принтерів та модемів було знову ввімкнено для виконання найнеобхідніших завдань. Лабораторні та радіологічні послуги надаються лише стаціонарним пацієнтам, а амбулаторні пацієнти повинні приносити паперові копії медичних карток. Прокурори заявляють, що цей інцидент створив «серйозну загрозу життю та здоров'ю» численних пацієнтів. Цей злом підкреслює зростання кіберзагроз у Польщі: Check Point повідомляє, що польські урядові установи зараз стикаються з приблизно 3200 спробами атак на тиждень, що є найвищим рівнем у Центральній та Східній Європі». ***(Maria Kamińska. Soldiers deployed to restore IT access at Polish hospital after huge cyberattack // Telewizja Polska S.A. w likwidacji (https://tvpworld.com/92042349/soldiers-deployed-to-restore-it-access-at-hospital-in-szczecin-after-cyberattack). 11.03.2026).***

***

«У п'ятницю Управління охорони здоров'я Міддлсекс-Лондон (MLHU) підтвердило, що проводить розслідування інциденту з кібербезпекою, виявленого напередодні. Виявивши загрозу, MLHU негайно вжило заходів протидії, зокрема відключило низку програмних систем та телефонних ліній, щоб запобігти подальшому несанкціонованому доступу. Генеральний директор Емілі Вільямс заявила, що організація активно співпрацює з провідними експертами з кібербезпеки з метою локалізації порушення, відновлення систем та проведення ретельного криміналістичного розслідування.

Хоча на даний момент залишається незрозумілим, які саме системи стали об'єктом атаки та чи була викрадена будь-яка особиста медична інформація, MLHU вже повідомило про це правоохоронні органи, муніципальних партнерів, а також провінційні органи охорони здоров'я та захисту персональних даних. Управління

наголосило на своїй відданості захисту даних пацієнтів та співробітників, зазначивши, що у разі підтвердження витоку даних із усіма постраждалими сторонами буде встановлено зв'язок, а також повідомило про намір опублікувати оновлену інформацію щодо ситуації у понеділок». ***(Bailey Shakyaver. MLHU confirms they were targeted in cybersecurity incident // BellMedia (https://www.ctvnews.ca/london/article/mlhu-investigating-cybersecurity-incident/). 06.03.2026).***

***

Захист персональних даних та соціальні мережі

«Медіакомпанії обробляють величезні обсяги цінних, конфіденційних даних, включаючи невиданий контент, фінансові записи та дані про абонентів, що робить їх головними цілями для кіберзлочинців. Для захисту цих даних організації застосовують комплексну стратегію кібербезпеки, що поєднує передові технології, суворі політики та навчання співробітників. В основі їхньої системи захисту лежать надійні системи мережевої безпеки, що використовують брандмауери та системи виявлення вторгнень для моніторингу трафіку та блокування несанкціонованого доступу, а також сегментовані мережеві архітектури. Шифрування даних також має вирішальне значення, оскільки воно гарантує, що дані будуть недоступними для неавторизованих осіб як під час зберігання, так і під час передачі…

Крім того, контроль доступу суворо регулюється за допомогою багатофакторної автентифікації (MFA), яка додає додатковий рівень безпеки, що виходить за межі простих паролів. Медіакомпанії проактивно виявляють слабкі місця за допомогою регулярних аудитів безпеки та оцінок вразливості, що дозволяє їм застосовувати необхідні виправлення до того, як ними скористаються зловмисники. Розуміючи, що людська помилка є основною вразливістю, організації інвестують у навчання з кібербезпеки, щоб допомогти співробітникам виявляти та уникати таких загроз, як фішингові електронні листи. Крім того, підтримка безпечних систем резервного копіювання та відновлення даних є життєво важливою для швидкого відновлення роботи без поступки вимогам програм-вимагачів. Нарешті, медіакомпанії часто співпрацюють із зовнішніми експертами з кібербезпеки для забезпечення вдосконаленого моніторингу, аналізу загроз та швидкого реагування, щоб забезпечити постійний захист своїх цифрових активів та безперебійну доставку контенту. ***(Naveen Goud. How Media companies defend their Data against Cyber Attacks // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/how-media-companies-defend-their-data-against-cyber-attacks/). 09.03.2026).***

***

«У своєму звіті про результати правозастосування за 2025 рік, опублікованому 9 лютого 2026 року, французький орган з захисту даних

(CNIL, Національна комісія з питань інформатики та свобод) зазначив, що загальна сума штрафів склала 487 млн євро — переважно за рахунок санкцій, пов'язаних із файлами cookie, — при цьому звернув особливу увагу на різке зростання штрафів за неналежний захист персональних даних та за порушення безпеки даних. Ця увага є наслідком попередження 2024 року, в якому CNIL зазначила 20-відсоткове збільшення кількості повідомлень про порушення та сплеск масштабних інцидентів, пов'язаних із використанням повторюваних вразливостей, таких як скомпрометовані облікові дані, невиявлене вторгнення та недостатній нагляд за обробниками даних…

Лише за період з грудня 2025 року по січень 2026 року регулятор наклав значні штрафи, зокрема 1,7 млн євро на розробника програмного забезпечення для сфери соціального забезпечення, 1 млн євро на компанію, що обробляє маркетингові дані для стрімінгової платформи, 5 млн євро на французьку державну службу зайнятості та 42 млн євро на великого інтернет-провайдера. Ця тенденція у сфері правозастосування відповідає стратегічному плану CNIL на 2025–2028 роки, який визначає кібербезпеку як головний пріоритет, а також рекомендаціям, опублікованим 30 квітня 2025 року, що закликають до більш суворого управління ідентифікацією та доступом, ведення журналів мережі в режимі реального часу, регулярного навчання персоналу та більш ретельного нагляду за обробниками та субобробниками…

З огляду на 2026 рік, CNIL буде вимагати від організацій, що володіють базами даних, які містять інформацію про кілька мільйонів осіб, запровадити багатофакторну автентифікацію для всіх співробітників, партнерів, обробників даних та інших віддалених користувачів; для перевірки дотримання цих вимог заплановано проведення інспекцій; невиконання цієї вимоги може спричинити порушення адміністративного провадження. Орган також закликає дотримуватися рекомендацій, опублікованих раніше спільно з Національним агентством з безпеки інформаційних систем Франції (ANSSI)». ***(Nadège Martin, Laura Helloco, Geoffroy Coulouvrat. Cybersecurity and Personal Data: The CNIL toughens its stance // Norton Rose Fulbright LLP (https://www.dataprotectionreport.com/2026/03/cybersecurity-and-personal-data-the-cnil-toughens-its-stance/). 19.03.2026).***

***

Масштабні витоки персональних даних

«LexisNexis підтвердила витік даних після того, як хакери, які безуспішно намагалися шантажувати компанію, опублікували нібито викрадені дані на форумі кіберзлочинців. Зловмисники стверджують, що минулого тижня здійснили кібератаку, скориставшись вразливістю React2Shell і неналежним захистом інстанцій AWS, щоб викрасти понад 2 ГБ даних, які, за їхніми твердженнями, містять облікові дані співробітників, секрети розробки програмного забезпечення та особисту інформацію 400 000 осіб. Однак LexisNexis применшила серйозність інциденту, заявивши, що порушення наразі локалізовано і що воно торкнулося переважно серверів, на яких зберігаються дані до 2020 року…

Хоча компанія визнала витік певної інформації, такої як імена клієнтів, ідентифікатори користувачів, контактні дані підприємств та квитки підтримки, вона підкреслила, що її основні продукти та послуги не зазнали змін. Крім того, LexisNexis уточнила, що жодні особливо конфіденційні дані, такі як номери соціального страхування, фінансова інформація, активні паролі або контракти з клієнтами, не були скомпрометовані. Цей інцидент став черговим викликом у сфері безпеки для гіганта юридичних та ризикових рішень після окремого порушення з боку третьої сторони у 2024 році, яке торкнулося понад 360 000 осіб». ***(Eduard Kovacs. New LexisNexis Data Breach Confirmed After Hackers Leak Files // Wired Business Media, Inc. (https://www.securityweek.com/new-lexisnexis-data-breach-confirmed-after-hackers-leak-files/). 04.03.2026).***

***

«Компанія Mazda Motor Corporation нещодавно повідомила про інцидент з безпекою, виявлений у грудні минулого року, під час якого зловмисники скористалися вразливістю в системі управління складом, що використовується для запасних частин, які закуповуються в Таїланді. В результаті інциденту було викрадено 692 записи, що належали співробітникам та діловим партнерам, що містили конфіденційну інформацію, таку як повні імена, адреси електронної пошти, назви компаній та ідентифікатори користувачів або партнерів, хоча компанія підтвердила, що дані клієнтів не постраждали. У відповідь на інцидент японський автовиробник негайно повідомив про це Комісію з захисту персональних даних Японії, розпочав розслідування спільно з зовнішніми фахівцями та зміцнив свою IT-інфраструктуру шляхом застосування патчів безпеки, зменшення доступу до Інтернету та впровадження більш суворих політик доступу… Хоча компанія Mazda не виявила жодних доказів зловживання викраденими даними, вона закликала постраждалих осіб зберігати пильність щодо можливих фішингових атак. Крім того, незважаючи на заяви групи хакерів Clop, зроблені в листопаді 2025 року щодо проникнення в системи Mazda, представник компанії чітко підтвердив, що цей останній інцидент не пов’язаний з атакою програм-вимагачів або шкідливого програмного забезпечення, вимог про викуп не надходило, а виробнича та господарська діяльність компанії не зазнала жодних змін…» ***(Bill Toulas. Mazda discloses security breach exposing employee and partner data // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/mazda-discloses-security-breach-exposing-employee-and-partner-data/). 23.03.2026).***

***

Кібербезпека та хмарні технології

«У звіті Google «Cloud Threat Horizons Report 2025» зазначається, що зловмисники змінюють способи проникнення в хмарні середовища: вони все менше покладаються на слабкі або відсутні облікові дані і все частіше

використовують вразливості в сторонньому та зовнішньо керованому програмному забезпеченні. У першій половині 2025 року слабкі облікові дані все ще були основним методом початкового доступу, але до другої половини року прогалини в програмному забезпеченні стали провідною точкою входу, на яку припадало 44,5% випадків компрометації, випередивши слабкі облікові дані (27,2%), неправильні налаштування (21%) та незахищені інтерфейси (4,9%)…

Зловмисники також діють набагато швидше: часто вони використовують нещодавно виявлені вразливості вже через кілька днів, а іноді розгортають криптомайнери протягом 48 годин. Компанія Google також виявила, що 21 % випадків вторгнень у хмарні середовища пов'язані зі зловживанням довірчими відносинами зі сторонніми організаціями, зокрема зловживанням токенами OAuth та інтеграціями SaaS, такими як Salesloft Drift і Salesforce Gainsight. Ці висновки свідчать про те, що деякі вдосконалення основних практик хмарної безпеки можуть бути ефективними, але зловмисники зараз переорієнтовуються на слабші супутні елементи, такі як сторонні додатки, конвеєри CI/CD, інструменти розробників та ланцюги постачання SaaS». ***(Sead Fadilpašić. 'The cloud threat landscape is rapidly shifting': Google research warns hackers are targeting third parties and software flaws to gain entry // Future US, Inc. (https://www.techradar.com/pro/security/the-cloud-threat-landscape-is-rapidly-shifting-google-research-warns-hackers-are-targeting-third-parties-and-software-flaws-to-gain-entry). 10.03.2026).***

***

Кібербезпека Інтернету речей. Штучний інтелект

«…Кіберзлочинці все частіше «зламують» популярні чат-боти на базі штучного інтелекту, щоб планувати і здійснювати вторгнення, які раніше вимагали експертних навичок. Прикладом цього є кампанія, в результаті якої було викрадено 195 мільйонів ідентифікаційних даних з дев'яти систем мексиканського уряду. За даними ізраїльської компанії Gambit Security, зловмисники використовували Anthropic's Claude — спочатку відмовившись надавати допомогу — для генерації коду та покрокових планів після того, як закидали його понад 1000 запитів, а для аналізу даних та отримання вказівок щодо облікових даних звернулися до ChatGPT від OpenAI. В результаті операції було викрадено приблизно 150 ГБ даних про податки, транспортні засоби, народження та майно. Генеральний директор Gambit зазначив, що штучний інтелект «знижує вартість складних операцій майже до нуля». Anthropic і OpenAI заявляють, що заблокували відповідні акаунти, але цей випадок підкреслює, як можна обійти заходи безпеки. Схожі інциденти за участю штучного інтелекту включають низькокваліфікований злом 600 брандмауерів і захоплення тисяч роботів-пилососів DJI для доступу до відео, аудіо та планів поверхів у режимі реального часу…

Дослідники попереджають, що це лише початок стрімкого зростання можливостей: агенти ШІ тепер працюють автономно протягом годин, а витривалість завдань подвоюється кожні сім місяців; компанія Anthropic позначила

«точку перелому», зірвавши кампанію, пов'язану з КНР, використовуючи Claude проти 30 глобальних цілей. Хоча соціальна інженерія залишається найпоширенішим видом використання — LLM створюють індивідуальні, бездоганні приманки, які сприяли восьмикратному зростанню кількості скарг від літніх американців і втратам у розмірі 4,9 млрд доларів у 2025 році — зловмисники також використовують ШІ для пошуку вразливостей, обходу захисних систем, встановлення «задніх дверей» і викрадення даних. Захисники використовують ШІ для виявлення атак, аудиту коду та виправлення недоліків, але асиметрія залишається: захисники повинні бути правими кожного разу, а зловмисники — лише один раз. Навіть попри те, що великі лабораторії підписують урядові контракти, лідери галузі, такі як Даріо Амодей з Anthropic, застерігають, що сучасні системи є непередбачуваними і недостатньо надійними для повністю автономної зброї, що підсилює нагальні заклики до посилення заходів безпеки, перш ніж можливості випередять контроль…» ***(Nilesh Christopher. How our AI bots are ignoring their programming and giving hackers superpowers // Los Angeles Times (https://www.latimes.com/business/story/2026-03-05/how-our-ai-bots-are-ignoring-their-programming-giving-hackers-superpowers). 05.03.2026).***

***

«Чи можуть розробники передових технологій штучного інтелекту забезпечити їх безпеку? У міру зростання кількості реальних впроваджень ризики з потенційно катастрофічними наслідками випереджають прості способи їх усунення. OpenAI, Anthropic і Google випускають інструменти, які обіцяють виявляти і навіть виправляти недоліки безпеки у джерелі — Claude Code Security від Anthropic (зараз у стадії попереднього дослідження) виявляє вразливі місця і пропонує способи їх усунення, заявляючи про сотні давно пропущених знахідок; Aardvark від OpenAI (приватна бета-версія) моніторить коміти коду, щоб виявити вразливі баги та запропонувати виправлення; а CodeMender від Google DeepMind вже випустив 72 виправлення безпеки для проектів з відкритим кодом (близько 4,5 млн+ LOC), з попередньою перевіркою людьми перед поданням та можливістю подальшої інтеграції. Уолл-стріт вважає, що ці пропозиції становлять загрозу для AppSec, SAST та аналізу складу програмного забезпечення, похитнувши спостережуваність та акції хмарної безпеки на підставі того, що безпека коду може перейти на власні платформи постачальників моделей…

Але ризик, пов'язаний із програмним забезпеченням, є більшим, ніж ризик, пов'язаний з одним інструментом або однією базою коду. Сучасні додатки є комбінацією бібліотек, контейнерів і бінарних файлів; як зазначає технічний директор JFrog, працює саме «артефакт», а не вихідний код. Навіть ідеальне сканування коду не може замінити багаторівневу систему захисту: брандмауери для захисту від зловмисників, контроль кінцевих точок для запобігання півотуванню, SASE для перевірки користувачів та SIEM для виявлення інцидентів у реальному часі в усіх парках — можливості, які традиційні постачальники вже доповнюють штучним інтелектом і підтримують цілодобовою реакцією...Тим часом сучасні агентні системи штучного інтелекту мають власні конструктивні недоліки: дослідження MIT та Northeastern висвітлюють відсутність аудитів та

аварійних вимикачів, а також «хаос» у багатоагентних тестах (боти, що обмінюються шкідливим кодом, посилюючи погані практики). Усунення цих прогалин вимагатиме нової інженерії даних (наприклад, різноманітних суперечливих корпусів для стрес-тестування агентів), більш надійних заходів безпеки та, можливо, переосмислення архітектури штучного інтелекту. Також є питання управління — коли розробник коду продає інструмент безпеки, чи не виходить, що лисиця охороняє курник?

Штучний інтелект допоможе зменшити кількість уникнутих збоїв програмного забезпечення та підвищити рівень безпеки кодування, особливо при інтеграції в робочі процеси розробки. Але це не скасує необхідності традиційних заходів безпеки та спостережності, а також фундаментальних інженерних змін у самому штучному інтелекті. Коротко кажучи: використовуйте ці нові інструменти штучного інтелекту, але не плутайте їх із повним рішенням розгалужених системних ризиків епохи штучного інтелекту». ***(Tiernan Ray. Will AI make cybersecurity obsolete or is Silicon Valley confabulating again? // Ziff Davis company (https://www.zdnet.com/article/ai-cybersecurity-silicon-valley/). 02.03.2026).***

***

«Протягом десятиліть кібербезпека спиралася на три основні стовпи: безпеку кінцевих точок, мереж та хмарних технологій, кожен з яких був розроблений у відповідь на значні зміни в архітектурі обчислювальних систем. Сьогодні швидка інтеграція штучного інтелекту, а саме автономних агентів ШІ, здатних виконувати завдання від імені користувачів, зумовлює необхідність створення четвертого стовпа: безпеки ШІ…

Оскільки сучасні системи штучного інтелекту майже повністю працюють через інтерфейси прикладного програмування (API) для отримання даних, виклику служб і виконання транзакцій, API стали основною поверхнею ризику. Автономні агенти взаємодіють з корпоративними системами зі швидкістю машини, здатні генерувати величезні обсяги запитів API, які можуть легко використовувати недокументовані «тіньові» API, слабку автентифікацію або надмірні привілеї. Традиційні основи безпеки не були розроблені для цього. Безпека кінцевих точок зазнає труднощів, оскільки ШІ часто працює в бек-енд середовищах; мережева безпека не може легко інтерпретувати бізнес-логіку зашифрованого трафіку API; а хмарна безпека часто не має аналізу поведінки API під час виконання…

Хоча комплексна безпека ШІ також охоплює захист навчальних даних, запобігання швидкому введенню та встановлення управління агентами, API є критичним перехрестям, де ризик ШІ стає оперативною реальністю. Так само, як попередні обчислювальні революції вимагали нових парадигм безпеки, поява архітектур на основі ШІ та API вимагає від організацій розширення своїх стратегій безпеки для захисту складної структури API, яка з'єднує ці автономні системи з реальним світом». ***(Eric Schwake. Why AI Security Is Emerging as the Fourth Pillar of Cybersecurity // IT Security Guru (https://www.itsecurityguru.org/2026/03/09/why-ai-security-is-emerging-as-the-fourth-pillar-of-cybersecurity/). 09.04.2026).***

***

«…Неправильне використання штучного інтелекту співробітниками, яке часто називають «тіньовим ШІ», стало однією з головних проблем кібербезпеки для середніх і великих організацій Нової Зеландії, згідно з останнім звітом Kordia про кібербезпеку бізнесу. Дослідження 2026 року показує, що 24% підприємств вважають неправильне використання ШІ співробітниками серйозною проблемою, оскільки співробітники копіюють конфіденційні дані в несанкціоновані інструменти ШІ, не розуміючи ризиків. Відповідно, кількість атак, що використовують вразливості, пов'язані зі штучним інтелектом, зросла більш ніж удвічі — з 6% у 2024 році до 14% у 2025 році…

Хоча загальна частка організацій, які повідомили про кібератаки, зменшилася з 59% до 44%, фінансовий вплив і серйозність цих інцидентів значно зросли. Національний центр кібербезпеки (NCSC) повідомив про збільшення прямих фінансових втрат на 118% у третьому кварталі 2025 року. Також зростає кількість випадків вимагання: 19% постраждалих організацій стикаються з фінансовими вимогами; зокрема, 42% тих, хто стикається з вимогою викупу, вирішили заплатити, а 32% усіх опитаних підприємств заявили, що розглянуть можливість оплати в майбутньому. Ці цифри підкреслюють значні прогалини в стратегіях готовності до інцидентів та стійкості до них..

Одночасно спільна консультація регіональних органів з кібербезпеки підкреслила зростаючу загрозу з боку російської групи INC Ransom, яка використовує модель подвійного вимагання і з початку 2025 року все частіше націлюється на чутливі сектори, такі як охорона здоров'я, у Новій Зеландії та Тихоокеанському регіоні. У відповідь на ці зростаючі загрози бізнес-лідери висловлюють підтримку більш суворим змінам в управлінні та регулюванні; 36% виступають за більш суворі покарання за нездатність захистити дані та обов'язкове повідомлення про серйозні атаки, а 27% підтримують законодавство, що повністю забороняє виплату викупу. Очікується, що ці фактори в сукупності — зростання ризиків, пов'язаних з штучним інтелектом, серйозні кампанії з використанням програм-вимагачів та потенційні зміни в регулюванні — матимуть значний вплив на ринок кіберстрахування протягом 2026 року». ***(Roxanne Libatique. Staff AI misuse now key cyber risk for NZ firms – report // KM Business Information US, Inc (https://www.insurancebusinessmag.com/nz/news/cyber/staff-ai-misuse-now-key-cyber-risk-for-nz-firms--report-567984.aspx). 11.03.2026).***

***

«Штучний інтелект вже змінює федеральні операції та кіберзахист, але його швидке впровадження створює серйозну проблему: ШІ та кібербезпека більше не можуть бути окремими завданнями. Як попереджає звіт робочої групи ATARC, ШІ надає можливості як захисникам (завдяки швидшому виявленню аномалій), так і зловмисникам (завдяки автоматизованому фішингу та створенню шкідливого програмного забезпечення), що робить конвергенцію необхідною для національної безпеки. Уряд не може просто купити вихід із ситуації, що виникла через брак кваліфікованих кадрів; натомість він повинен розглядати освіту в галузі кібербезпеки та штучного інтелекту як стратегічну інфраструктуру, створюючи систему від початкової школи до вищих навчальних закладів та впроваджуючи

грамотність у всіх ролях, а не тільки у фахівців з безпеки… Щоб запобігти порушенням в управлінні, таким як витік даних або «галюцинаційні» юридичні посилання, агентствам потрібні дієві механізми, які передбачають людський нагляд і суворий контроль даних. Тому адміністрація повинна проявити ініціативу, привівши розвиток кадрів у відповідність до сучасних загроз, інтегрувавши управління ШІ в повсякденну діяльність та сприяючи глибокій співпраці між державним, приватним і академічним секторами, щоб забезпечити готовність федеральних кадрів до ери ШІ». ***(Keith Clement. Why the convergence of AI and cybersecurity must be a top priority for the administration // Government Media Executive Group LLC. (https://www.nextgov.com/ideas/2026/03/why-convergence-ai-and-cybersecurity-must-be-top-priority-administration/411837/). 03.03.2026).***

***

«EY повідомляє, що компанії стрімко автоматизують рутинні завдання з кібербезпеки за допомогою штучного інтелекту (ШІ), щоб вирішити проблему бюджетних обмежень та покращити операції з безпеки. 96% керівників служб безпеки вважають ШІ основним захисним інструментом, а 95% вже впроваджують його, хоча приблизно дві третини з них все ще перебувають на етапі тестування. Керівники вважають ШІ як інструментом, що змінює ситуацію, так і небезпечним: 99% очікують, що він докорінно змінить кіберзахист, тоді як 96% зазначають, що він також значно посилює можливості зловмисників, уможливлюючи швидші та більш витончені атаки. На основі опитування 500 керівників з кібербезпеки у великих підприємствах (з доходом понад 500 мільйонів доларів у різних секторах) опитування показує, що потенціал агентного ШІ ще не реалізовано повною мірою — приблизно половина користувачів повідомляє про прибуток менше 1 млн доларів, а 12% не побачили або не відстежували рентабельність інвестицій — проте керівники очікують, що ШІ незабаром візьме на себе основні функції, зокрема виявлення складних постійних загроз (62% протягом двох років), виявлення шахрайства (58%) та управління ідентифікацією й доступом (51%)…

Управління та людський нагляд виявляються вирішальними факторами: приблизно половина компаній почала впроваджувати механізми управління ШІ, але лише 26% повністю інтегрували їх у робочі процеси бізнес-підрозділів, і лише 20% стверджують, що управління є невід'ємною частиною корпоративної культури, незважаючи на те, що 97% вважають управління необхідним для створення цінності. Контроль з участю людини є поширеним (85% для важливих рішень), і 98% респондентів вважають, що інструменти, які діють самостійно, потребують людського нагляду, але дефіцит кваліфікованих кадрів є серйозним — 90% компаній стикаються з труднощами у наймі та утриманні персоналу, здатного керувати інструментами ШІ, а багато хто називає непідготовленість персоналу до атак на основі ШІ своєю найбільшою вразливістю.

З огляду на результати опитування, компанія EY зазначила, що підприємствам необхідно усвідомити чотири важливі реалії: бюджетні обмеження роблять штучний інтелект практично необхідним у сфері кібербезпеки; рентабельність інвестицій у штучний інтелект залежить від того, чи зможуть підприємства перейти від «автоматизації на рівні виконання завдань» до повністю автономних операцій;

людський контроль за штучним інтелектом є «необхідною умовою»; а надійний штучний інтелект ґрунтується на ефективних процесах управління». ***(Eric Geller. Companies know AI is essential for cyber defense but aren't yet seeing returns // TechTarget, Inc. (https://www.cybersecuritydive.com/news/cybersecurity-ai-agentic-governance-ey-survey/815311/). 20.03.2026).***

***

«Гонка озброєнь у сфері кібербезпеки вступила в нову фазу, що зумовлено розвитком штучного інтелекту, який різко прискорює виявлення та використання вразливостей «нульового дня». Для зловмисників ШІ перетворює пошук слабких місць на систематичну високошвидкісну операцію, дозволяючи їм аналізувати величезні кодові бази на наявність неочевидних точок входу, комбінувати незначні недоліки у складні ланцюжки атак та створювати приховані експлойти, що уникнуть виявлення. Ця зміна скорочує час реагування команд безпеки з місяців до лічених годин, що становить існувальну загрозу для непідготовлених підприємств…

Однак ця ж сама технологія надає захисникам безпрецедентну можливість випереджати загрози. Використовуючи штучний інтелект, організації можуть перейти до проактивного підходу до безпеки. Ключові стратегії включають впровадження «циклів пошуку ШІ», під час яких інструменти ШІ систематично перевіряють власну інфраструктуру організації на наявність вразливостей у заплановані періоди простою, надаючи захисникам вирішальну перевагу першопрохідця. Компанії також можуть створювати системи перевірки безпеки на основі штучного інтелекту, створюючи внутрішні «боти червоної команди», які постійно тестують захист і зміцнюють системи завдяки постійному циклу зворотного зв'язку. Крім того, штучний інтелект дозволяє створювати прогнозні моделі вразливостей, аналізуючи історичні дані та шаблони коду, щоб передбачити, де найімовірніше з'являться уразливості «нульового дня», що дозволяє командам безпеки заздалегідь зміцнити компоненти з високим рівнем ризику. У цю нову еру пасивний захист більше не є життєздатним; ключ до виживання полягає у використанні ШІ для виявлення та усунення власних слабких місць раніше, ніж це зроблять зловмисники». ***(Ashwin Krishnan. What AI zero days mean for enterprise cybersecurity // TechTarget, Inc. (https://www.techtarget.com/searchsecurity/tip/What-AI-zero-days-mean-for-enterprise-cybersecurity). 19.03.2026).***

***

«У звіті компанії Booz Allen Hamilton під назвою «Коли кібератаки відбуваються зі швидкістю штучного інтелекту» міститься попередження про те, що кібербезпека вступила в еру «швидкості машин», в якій штучний інтелект скорочує час між вторгненням і нанесенням шкоди, дозволяючи зловмисникам планувати, тестувати та здійснювати багатоетапні операції за лічені хвилини з мінімальним втручанням людини. У звіті стверджується, що зловмисники впроваджують штучний інтелект швидше, ніж захисники, використовуючи агентів штучного інтелекту для автоматизації розвідки, виявлення вразливостей, експлуатації та персистентності з темпами, що випереджають

традиційні операції з безпеки, керовані людьми, — де сортування може займати години, усунення — дні, а встановлення виправлень — тижні, — особливо у взаємопов’язаних IT- та OT-середовищах та критичній інфраструктурі. Ця невідповідність вже використовується: незважаючи на 15-денний термін усунення критичних вразливостей, встановлений CISA, Booz Allen зазначає, що 60% залишаються неусуненими після закінчення терміну, тоді як зловмисники можуть використовувати нові вразливості як зброю вже за кілька годин; вартість автоматичного створення експлойта CVE знизилася до приблизно 2,77 долара, а інструменти ШІ продемонстрували здатність виявляти сотні потенційних вразливостей «нульового дня» у відкритому коді… У звіті підкреслюється, наскільки швидко зараз розширюється масштаб зловживань, наводячи приклад кампанії, що відбулася в серпні–вересні 2025 року, під час якої зловмисник HexStrike використав уразливість CVE-2025-7775 на понад 8 000 кінцевих точках менш ніж за 10 хвилин, а також зазначається, що до 2025 року середній «час прориву» від початкового доступу до горизонтального переміщення скоротився до менше ніж 30 хвилин, а в деяких випадках займав лічені секунди. Booz Allen розглядає це прискорення в більш довгостроковій перспективі, яка включає підроблені ШІ токени OAuth, використані під час злом Storm-0558 у 2023 році в Microsoft Azure, що зачепив понад 25 урядових організацій США, масовий спірфішинг, згенерований ШІ, з боку груп, пов'язаних з державою, пізніше у 2023 році, автономне виявлення агентом ШІ уразливості «нульового дня» в SQLite у 2024 році, а також стрімкий прогрес у розробці наступальних інструментів на базі ШІ протягом 2025–2026 років, включаючи системи, здатні відтворювати значну частину відомих уразливостей у вигляді діючих експлойтів…

Як зазначається у звіті, щоб не відставати від темпів розвитку, організації повинні здійснити три основні зміни: привести кіберзахист у відповідність до швидкості роботи штучного інтелекту шляхом попереднього авторизування та автоматизації заходів раннього локалізування (таких як ізоляція систем, блокування трафіку, скасування сеансів та запуск заходів з усунення наслідків) у межах визначених обмежень, із можливістю відкату та аудиту; розглядати самі платформи ШІ як критичну інфраструктуру, оскільки вони централізують дані, ідентифікацію та робочі процеси, а отже, потребують обов’язкових базових стандартів безпеки для автентифікації, ведення журналів, обробки даних та облікових даних, інтеграції та конфігурацій із безпекою за замовчуванням; та впровадити модель співпраці людини та ШІ, де автоматизовані агенти за лічені секунди виконують рутинну сортування, оновлення виявлення, кроки розслідування та початкове локалізування, тоді як аналітики-люди здійснюють нагляд, зосереджуються на складних рішеннях та припиняють складні кампанії, спираючись на чітке управління щодо того, що можна автоматизувати та хто приймає рішення… Компанія Booz Allen робить висновок, що для подолання розриву в швидкості, який постійно збільшується, необхідна модернізація у сферах безпеки, мережевих операцій та IT/OT-операцій — на основі підходу «нульової довіри», інтегрованих операцій з використанням штучного інтелекту, а також більш тісної узгодженості між юридичними аспектами та керівництвом — оскільки захисники, які не здатні виявляти, локалізувати та усувати загрози в межах нового,

надзвичайно короткого часового вікна, ризикують виявити вторгнення лише після того, як зловмисники вже встановили контроль. У звіті також повторюється попереднє застереження Booz Allen про те, що Китайська Народна Республіка реалізує наполегливу стратегію «кіберприскорення», здатну діяти в глобальному масштабі через втручання уряду, маніпулювання ланцюгами постачання та діяльність з впливу, причому повний масштаб її впливу досі до кінця не з'ясований». ***(Anna Ribeiro. Booz Allen warns AI-driven cyberattacks outpace human-driven defenses across critical infrastructure // Industrial Cyber (https://industrialcyber.co/ai/booz-allen-warns-ai-driven-cyberattacks-outpace-human-driven-defenses-across-critical-infrastructure/). 17.03.2026).***

***

«Компанія Anthropic розробляє нову потужну модель штучного інтелекту під назвою Claude Mythos, інформація про існування якої нещодавно просочилася в мережу через помилку в налаштуваннях системи управління контентом компанії. За повідомленнями, Mythos, що позиціонується як новий рівень, вищий за поточні моделі Opus від Anthropic, демонструє значне поліпшення в сферах програмування, академічного мислення та кібербезпеки. Внутрішні документи також розкрили інформацію про другу версію, що знаходиться в розробці, під кодовою назвою «Capybara». Оскільки Mythos володіє надзвичайно просунутими можливостями кібер-експлуатації, які можуть випередити сучасні цифрові засоби захисту, Anthropic планує обережний, обмежений ранній доступ, спрямований насамперед на організації, що спеціалізуються на кібербезпеці… Незважаючи на оперативне видалення викрадених матеріалів, ця новина спричинила значне падіння акцій провідних компаній у сфері кібербезпеки, зокрема Palo Alto Networks та CrowdStrike… Така реакція ринку нагадує попередній обвал на суму 285 мільярдів доларів, спричинений запуском Claude Cowork — штучного інтелекту від Anthropic для автоматизації робочого процесу, — що підкреслює зростаючі побоювання інвесторів щодо того, що базові моделі штучного інтелекту дедалі частіше стають здатними руйнувати та безпосередньо конкурувати зі спеціалізованим корпоративним програмним забезпеченням…» ***(Jason Nelson. Anthropic's 'Most Capable' AI Model Claude Mythos Leaks, Deemed Major Cybersecurity Threat // Decrypt Media, Inc. (https://decrypt.co/362606/anthropic-most-capable-ai-model-claude-mythos-leaks). 27.03.2026).***

***

Штучний інтелект, як інструмент боротьби із кіберзлочинністю

«У все більш нестабільному геополітичному середовищі інтеграція штучного інтелекту в кібербезпеку стала необхідною для виявлення, пом'якшення та запобігання складним загрозам. ШІ глибоко трансформує стратегії захисту, використовуючи безперервне навчання та аналіз даних у реальному часі для виявлення аномалій та скорочення часу реагування, а також

революціонізує навчання персоналу за допомогою динамічних симуляцій на основі сценаріїв. У Європейському Союзі впровадження цих технологій значною мірою визначається новими нормативними рамками, зокрема Законом про ШІ 2024 року та Законом про кіберстійкість, які вимагають людського нагляду, прозорості та надійного управління ризиками. Як наслідок, організації використовують ШІ для автоматизації складних процесів дотримання вимог, аудиту та звітності, щоб відповідати цим суворим стандартам…

Окрім технічних і регуляторних застосувань, штучний інтелект у сфері кібербезпеки все частіше визнається важливим стратегічним активом і наріжним каменем європейського цифрового суверенітету. Оскільки кібератаки регулярно використовуються як інструменти глобального примусу, ЄС надає пріоритет технологічній автономії, щоб зменшити свою залежність від іноземної цифрової інфраструктури, тим самим захищаючи свої критичні системи та демократичні цінності… Однак впровадження ШІ пов'язане з низкою викликів, серед яких технічні помилки в класифікації, етичні дилеми та ризики, властиві технологіям подвійного призначення, коли супротивники використовують ті самі передові інструменти для кіберсаботажу та дезінформації. Щоб протидіяти цим вразливим місцям, ЄС і НАТО узгоджують свої оборонні стратегії, щоб перейти від реактивних до прогнозних моделей безпеки. Зрештою, забезпечення цифрового майбутнього Європи вимагає балансу між інноваціями та суворим етичним управлінням, захисту внутрішніх екосистем штучного інтелекту від іноземного втручання та підготовки висококваліфікованих кадрів, здатних орієнтуватися у складному перетині передових технологій та глобальної динаміки влади». ***(Stefano Bodrato. How AI can bolster Europe's cybersecurity // OMFIF (https://www.omfif.org/2026/03/how-ai-can-bolster-europes-cybersecurity/). 09.03.2026).***

***

«…Дослідники з Університету Суррея представили TwinGuard, систему захисту на базі штучного інтелекту, яка виявляє і нейтралізує складні кібератаки 5G менш ніж за 100 мілісекунд. Поєднуючи цифровий двійник у реальному часі — віртуальну копію мережі, що постійно оновлюється — з підкріплювальним навчанням, TwinGuard вивчає нормальні моделі поведінки і блокує аномалії, перш ніж вони спричинять порушення, перевершуючи традиційні системи на основі правил, які не можуть впоратися з новими або еволюціонуючими загрозами… У тестах із використанням модельованих багатокоміркових середовищ Open RAN та повністю віртуальних середовищ 5G core, ця платформа успішно запобігла атакам типу handover-flooding та E2-subscription-flooding. Цей прорив вирішує проблему підвищеної вразливості відкритих, гнучких архітектур 5G та закладає важливу основу для безпечних мереж 6G, які очікуються у 2030-х роках, де поведінкові, керовані штучним інтелектом засоби захисту будуть необхідними для протидії спритним супротивникам. Зараз команда планує масштабувати TwinGuard до більших багатокомірних розгортань». ***(Gaby Clark. AI-powered defense system stops 5G cyber-attacks in a fraction of a second // Science X™ (https://techxplore.com/news/2026-03-ai-powered-defense-5g-cyber.html). 10.03.2026).***

***

«Новий звіт Flashpoint попереджає, що агентна ШІ — системи, здатні виконувати складні завдання з мінімальним контролем з боку людини — різко посилює кіберзагрози національній безпеці, дозволяючи супротивникам, особливо групам, пов'язаним з Китаєм, автоматизувати складні атаки, вчитися на помилках і промислово впроваджувати вторгнення в мережі зі швидкістю машини. Тільки у 2025 році кількість незаконних дискусій та злочинної діяльності, пов'язаних зі штучним інтелектом, перевищила 1,5 мільярда, а кількість виявлених вразливостей програмного забезпечення перевищила 44 000, багато з яких були використані на державному рівні. Китайські APT націлилися на платформи, які широко використовуються урядами, оборонними підрядниками та транснаціональними корпораціями, тоді як Міністерство оборони та його екосистема поспішають впроваджувати агентний штучний інтелект для підвищення ефективності, не повністю усвідомлюючи розширення площі атаки, яке він створює…

Внутрішні загрози також різко зростають: у 2025 році було зафіксовано понад 91 000 спроб вербування та пропозицій хабарів, включаючи північнокорейських агентів, які видавали себе за співробітників і підрядників, що продавали секрети — часто дешевше, ніж розробка зовнішніх експлойтів. На полі бою дрони та безпілотні системи на базі штучного інтелекту створюють подібні ризики через вразливі ланцюги постачання, оновлення програмного забезпечення та канали передачі даних, а не через самі моделі штучного інтелекту. Flashpoint закликає до посилення управління, суворого контролю доступу, моніторингу поведінки та безпеки ланцюгів постачання, щоб протидіяти цій конвергенції прискорення розвитку штучного інтелекту, агресії з боку держави та зловживань з боку інсайдерів, перш ніж супротивники перетворять автоматизацію на вирішальну перевагу». ***(Tabitha Reeves. JUST IN: Agentic AI a 'Force Multiplier' for China's Cyberattacks, Report Says // National Defense Industrial Association (https://www.nationaldefensemagazine.org/articles/2026/3/11/just-in-ai-enabling-new-cyber-risks-report-says). 11.03.2026).***

***

«Генеративний штучний інтелект (GenAI) сприяє «фундаментальній перебудові» та індустріалізації сучасних кібератак, згідно з першим звітом Cloudflare Threat Report за 2026 рік, в якому аналізуються дані про 230 мільярдів загроз, які компанія блокує щодня. Як злочинці, що керуються жадобою наживи, так і державні суб'єкти швидко впроваджують штучний інтелект, про що свідчить «перша в історії атака на основі штучного інтелекту», під час якої хакери використовували штучний інтелект для пошуку цінних даних, що призвело до масштабного порушення ланцюга поставок, яке поставило під загрозу сотні корпоративних орендарів. Крім того, такі держави, як Північна Корея, використовують генеровані штучним інтелектом дипфейки та підроблені

посвідчення особи, щоб обійти протоколи найму та розмістити шпигунів у західних компаніях, використовуючи місцеві «ноутбукові ферми» замість VPN…

Cloudflare попереджає, що штучний інтелект утворює «нечесну трійцю» разом із соціальним інжинірингом та дедалі більш витонченими DDoS-атаками. Ботнети, такі як Aisuru, досягли рівня загрози для національної безпеки, здійснюючи рекордні атаки потужністю до 31,4 Тбіт/с, які перевершили можливості реагування людини і тепер вимагають повністю автономних засобів захисту. У світлі цих швидко розвиваючихся і приголомшливих тактик Блейк Дарше, керівник відділу аналізу загроз у Cloudflare, закликає організації перейти від реактивної позиції безпеки до позиції, що базується на оперативній інформації в режимі реального часу, щоб не відставати в цій гонці озброєнь у кіберпросторі, де ставки дуже високі». ***(Sead Fadilpašić. 'The total industrialization of cyber threats': Cloudflare report outlines how hackers are 'weaponizing the Internet' // Future US, Inc. (https://www.techradar.com/pro/security/the-total-industrialization-of-cyber-threats-cloudflare-report-outlines-how-hackers-are-weaponizing-the-internet). 04.03.2026).***

***

«Хакерські угруповання національних держав, включаючи пакистанське APT36 (Transparent Tribe) та іранське MuddyWater, все частіше звертаються до генеративної штучної інтелекту, щоб швидко створювати функціональне, хоча й часто примітивне, шкідливе програмне забезпечення, що отримало назву «vibeware». Bitdefender повідомляє, що APT36 почала доповнювати такі відомі інструменти, як Havoc і Warcode, одноразовими імплантатами, створеними за допомогою штучного інтелекту та написаними на нішевих мовах, таких як Nim, Zig або Crystal, щоб уникнути виявлення, при цьому щедро розсипаючи емодзі по всьому коду — це характерна риса допомоги LLM, яка також спостерігається в новому бекдорі Rust «Char» від MuddyWater та пов'язаних скриптах C2. Google і Group-IB раніше задокументували використання MuddyWater Gemini для фішингу та створення власного шкідливого програмного забезпечення, а проникнення Ctrl-Alt-Intel в інфраструктуру MuddyWater підтвердило наявність коду, насиченого емодзі та створеного за допомогою штучного інтелекту…

Хоча це програмне забезпечення далеко не є елегантним і рідко використовує нульові дні, воно надає пріоритет масштабованості та обсягу: зловмисники завалюють цілі багатомовними корисними навантаженнями, знаючи, що деякі з них проникнуть через захист, який не відстежує незвичайні мови або непідписані бінарні файли. Експерти підкреслюють, що базова гігієна кінцевих точок — блокування непідписаних виконуваних файлів, спостереження за аномальними викликами API до Discord/Slack/Google Sheets та підтримання надійного виявлення — залишається дуже ефективною проти цих малоскладних кампаній з великим обсягом, навіть коли їх проводять державні суб'єкти. Оскільки штучний інтелект знижує бар'єр для створення власного шкідливого програмного забезпечення, зростання кількості атак із використанням «коду вібрації» підкреслює, що для заподіяння реальної шкоди більше не потрібні елітні навички». ***(Mathew J. Schwartz. Nation-State Hackers Play the Vibes // Information Security Media Group,***

Corp. (https://www.inforisktoday.com/nation-state-hackers-play-vibes-a-30920). 05.03.2026).

***

«Згідно з доповіддю Kaseya «INKY Email Security Report 2026», 2025 рік став переломним моментом, коли штучний інтелект змінив як методи атак, так і засоби захисту: фішинг, створений за допомогою штучного інтелекту, став нормою, позбавивши атаки таких характерних ознак, як граматичні помилки чи недолугі домени, і змусивши захисників оцінювати наміри та контекст. Фішинг залишився головним вектором атак — 26 % скарг на кіберзлочини, що надійшли до ФБР — при цьому збитки від компрометації ділової електронної пошти склали 2,8 млрд доларів, а основний удар припав на малі та середні підприємства, оскільки 82 % атак програм-вимагачів були спрямовані на організації з чисельністю персоналу менше 1 000 осіб…

У 2025 році INKY опрацювала понад 4,5 мільярда електронних листів і зафіксувала випадки підробки 281 різних брендів, причому макети, створені за допомогою штучного інтелекту, дуже точно імітували повідомлення від провідних фінансових та роздрібних установ. У відповідь INKY розширив можливості виявлення GenAI, маркування на основі намірів, класифікації за кількома мітками та контекстного аналізу за допомогою комп'ютерного зору, щоб протидіяти новим видам шахрайства, включаючи запрошення в календарі, захищені документи та шахрайство з номерами для зворотного дзвінка — що ілюструє, що штучний інтелект тепер забезпечує як більш переконливі загрози, так і більш адаптивні засоби захисту». ***(Neil Trim. Kaseya Report Highlights Impact of AI on Cybersecurity Threat Landscape // Kingswood Media (https://technologyreseller.uk/kaseya-report-highlights-impact-of-ai-on-cybersecurity-threat-landscape/). 17.03.2026).***

***

Кіберзлочинність та кібертероризм

«У звіті CrowdStrike «Глобальні загрози 2026 року» 2025 рік названо роком ухильних супротивників, коли зловмисники в основному відмовляться від шкідливого програмного забезпечення на користь «життя з того, що є», викрадених ідентичностей та довіри підприємств, щоб уникнути спрацьовування засобів контролю… Цифри вражають: 82% виявлених випадків не містили шкідливого програмного забезпечення; середній час прориву скоротився до 29 хвилин (найшвидший — 27 секунд), що скоротило час на реагування захисників; кількість випадків використання уразливостей нульового дня до їх оприлюднення зросла на 42%; активність із використанням штучного інтелекту зросла на 89%; а кількість вторгнень у хмару зросла на 37%, включаючи 266% зростання, пов'язане з державними суб'єктами. Ідентичність зараз є на передньому плані — зловживання дійсними обліковими записами з'явилося в 35% випадків вторгнень у хмару, — тоді як такі групи, як Scattered Spider і Blockade

Spider, використовують сценарії фішингу проти служб технічної підтримки, щоб скинути облікові дані або зареєструвати нові пристрої MFA…

Супротивники діють у сліпих зонах захисників: ідентифікація, хмара, некеровані пристрої та, особливо, мережеве обладнання (брандмауери, VPN, маршрутизатори), яке використовують лише деякі організації; 40% атак, пов'язаних з Китаєм, спрямовані на периферійні пристрої, причому їхня мілітаризація часто відбувається протягом двох днів після розкриття, а стійкість може тривати роками (наприклад, Warp Panda — 22 місяці). Штучний інтелект розширює можливості соціальної інженерії та адаптивних операцій — фішинг без викривальних помилок, багатомовний синтетичний голос для вішингу та інструменти, такі як «Lamehug» від Fancy Bear, які запитують LLM про команди розвідки та динамічно викрадають файли, — тоді як поспішне впровадження штучного інтелекту створює нові дірки (наприклад, LangFlow, який використовується для розгортання програм-вимагачів; зловмисні сервери MCP, які викачують електронні листи)…

Компрометація ланцюга поставок залишається фактором, що підсилює вплив, про що свідчить крадіжка Північною Кореєю 1,46 млрд доларів з Bybit через уразливість Safe{Wallet}, що відбиває більш широкі тенденції у сфері зловмисних пакетів npm, типосквоттингу та отруєних ланцюгів інструментів. Захисники повинні надавати пріоритет виявленню загроз ідентичності в режимі реального часу (аномальні входи, реєстрація MFA, зловживання службовими обліковими записами, поперечне переміщення над законними обліковими даними), усуненню прогалин у міждоменній видимості на кінцевих точках/ідентичності/хмарі/некерованих пристроях, інтеграції аналізу шляхів атаки в управління вразливістю для розриву ланцюгів, що можуть бути використані, та розглядати системи штучного інтелекту як першокласні поверхні атаки з реєстрацією та управлінням доступом; водночас вони не повинні нехтувати заходами проти рішучих зловмисників, які все ще використовують нульові дні та спеціальне шкідливе програмне забезпечення. Хоча звіт відображає точку зору постачальника, його дані та тенденції узгоджуються з незалежними спостереженнями, підкреслюючи ситуацію, в якій зловмисники досягають успіху, маскуючись та діючи швидко». ***(Tony Bradley. Hackers Don't Need Malware Anymore And That Changes Everything // Forbes Media LLC. (https://www.forbes.com/sites/tonybradley/2026/03/06/hackers-dont-need-malware-anymore-and-that-changes-everything/). 06.03.2026).***

***

«Нещодавно опублікований IBM X-Force Threat Intelligence Index 2026 висвітлює значні зміни в способах здійснення атак кіберзлочинцями, підкреслюючи, що складні загрози часто є вторинними порівняно з використанням основних прогалин у безпеці. За останні п'ять років кількість порушень у ланцюгах постачання та у сторонніх організаціях зросла в чотири рази, оскільки зловмисники обходять добре захищені основні системи, використовуючи вразливості у взаємопов'язаних мережах, постачальниках та хмарних API. Одночасно з цим використання загальнодоступних додатків зросло на 44% у порівнянні з минулим роком, в основному через помилки конфігурації. Явною

вразливістю організацій є те, що 56% відстежених слабких місць можна було б використати без будь-якої форми аутентифікації, що вказує на те, що зловмисники використовують прості, не виправлені недоліки, а не потребують викрадених облікових даних або обходу багатофакторної аутентифікації (MFA)…

Однак, коли метою є облікові дані, зростаюча інтеграція чат-ботів та агентів на базі штучного інтелекту створює нову привабливу площину для атак, і сотні тисяч облікових даних ChatGPT вже виставлені на продаж у даркнеті. З географічної точки зору, Північна Америка вперше за шість років стала регіоном, який найчастіше стає мішенню атак, що пояснюється високим рівнем цифровізації, взаємопов'язаними ланцюгами постачання та значною залежністю від хмарних послуг, що робить її високоприбутковою мішенню для зловмисників. Незважаючи на зростання популярності інструментів безпеки на основі штучного інтелекту, у звіті підкреслюється, що фундаментальні прогалини в кібербезпеці, такі як відсутність постійного моніторингу, постійного управління ризиками та надійного контролю доступу, залишаються основною причиною порушень, відкриваючи ворогам широкі можливості». ***(Judith Aquino. Cyberthreats in 2026: X-Force and industry experts weigh in // IBM (https://www.ibm.com/think/insights/more-2026-cyberthreat-trends). 11.03.2026).***

***

«Як один з найбільш пов'язаних комерційних центрів світу, Лондон є високоцінною мішенню для кіберзлочинців, а підприємства столиці стикаються з особливо інтенсивними загрозами. Організації в Лондоні особливо вразливі через три фактори, що збільшують ризик: висока щільність цінних і регульованих даних, значна залежність від зовнішніх постачальників та швидкий темп роботи, що збільшує вразливість до соціальної інженерії. Як наслідок, найпоширенішими загрозами є фішинг та компрометація ділової електронної пошти (BEC) з метою перенаправлення високоцінних платежів, багаторівневе вимагання викупу за допомогою програм-вимагачів, крадіжка облікових даних та компрометація ланцюгів постачання. Крім того, регулярне використання неперевірених «тіньових IT-ресурсів», таких як обмін файлами між споживачами або несанкціоновані розширення браузерів нетехнічним персоналом, непомітно розширює площу атаки…

Наслідки цих порушень виходять далеко за межі IT-незручностей, часто призводячи до серйозних перебоїв у роботі бізнесу, значних фінансових втрат, пов'язаних із шахрайством, та суворих регуляторних санкцій. Щоб ефективно боротися з цими загрозами, лондонські підприємства повинні підняти кібербезпеку з рівня технічної проблеми до рівня операційної та бізнес-безперебійності на рівні правління. Для підвищення стійкості необхідно опанувати основні проактивні засоби захисту, такі як забезпечення суворої безпеки ідентифікації за допомогою багатофакторної автентифікації, підтримка незмінних і регулярно перевірених резервних копій, а також активне зменшення площі атаки шляхом виправлення систем і обмеження доступу постачальників. Нарешті, організації повинні підготуватися до неминучості атаки, розробивши чіткий план реагування на інциденти на перші критичні 24 години, заздалегідь визначивши ролі керівництва

та забезпечивши суворий фінансовий контроль під час хаосу, що виникає під час порушення, щоб запобігти вторинному шахрайству». ***(Sarah Dunsby. Cybersecurity risks facing London businesses // London loves Business (https://londonlovesbusiness.com/cybersecurity-risks-facing-london-businesses/). 09.03.2026).***

***

«Нещодавній глобальний звіт про загрози від Barracuda визначив атаки на основі ідентифікації та некеровані пристрої як провідні ризики кібербезпеки для сучасних організацій, виявивши, що зловмисники все частіше використовують рутинні операційні прогалини, а не складні технічні експлойти. На основі аналізу понад двох трильйонів IT-подій, зареєстрованих у 2025 році, глобальний звіт про загрози Barracuda Managed XDR виявив, що некеровані або несанкціоновані кінцеві точки були присутні в кожному проаналізованому інциденті безпеки. За словами Метта Каффрі, старшого архітектора рішень у Barracuda, зловмисники часто використовують повсякденні «сліпі зони», такі як пристрої, що працюють поза стандартними системами моніторингу, неактивні облікові записи або вимкнені засоби контролю безпеки, щоб отримати початковий доступ…

Як наслідок, різко зросла кількість атак, пов'язаних з ідентифікацією, про що свідчить виявлення понад 42 000 аномальних входів у Microsoft 365 та 22 000 сповіщень про «неможливі подорожі», що явно вказує на компрометацію облікових даних. Після проникнення в мережу загроза швидко зростає. У звіті зазначається, що 96 % інцидентів, пов'язаних з латеральним переміщенням, в кінцевому підсумку призвели до атак програм-вимагачів. Ця загроза становить серйозний виклик для організацій, які намагаються управляти складними технологічними середовищами з обмеженими ресурсами безпеки, особливо для середніх компаній, які швидко впроваджують хмарні платформи, дистанційну роботу та стикаються з нестачею фахівців з кібербезпеки. Для боротьби з цими вразливостями Barracuda радить організаціям надавати пріоритет виявленню некерованих пристроїв, посилювати захист ідентичності та ретельно стежити за незвичайною поведінкою під час входу в систему, щоб запобігти проникненню зловмисників у корпоративні мережі». ***(Identity attacks and unmanaged devices are rising cyber risks // MySecurity Media Pty Limited (https://australiancybersecuritymagazine.com.au/identity-attacks-and-unmanaged-devices-are-rising-cyber-risks/). 12.03.2026).***

***

«Звіт Check Point «Global Threat Intelligence» за лютий 2026 року показує, що британські організації щотижня зазнавали 1504 кібератаки, що значно нижче середнього світового показника (2086), але річний приріст на 36 % значно перевищив світовий показник (9,8 %). Найбільше постраждали такі сектори, як освіта, енергетика та комунальні послуги, державне управління, охорона здоров'я та фінанси. Програми-вимагачі залишаються головною загрозою, а Великобританія посідає третє місце у світі за кількістю жертв (3 %),

поступаючись лише США (51 %) і Канаді (6 %), причому домінували такі програми, як Qilin, Clop і The Gentlemen…

Тим часом, некеровані генеративні інструменти штучного інтелекту збільшують ризики витоку даних: один із 31 корпоративних запитів GenAI у всьому світі мав високий потенціал витоку, що вплинуло на 88 % звичайних користувачів, а 16 % містили конфіденційні облікові дані, дані клієнтів або інтелектуальну власність. Оскільки організації в середньому використовують 11 різних інструментів GenAI, а користувачі генерують 62 запити щомісяця — часто без нагляду ІТ-відділу або політики — ймовірність випадкових витоків зростає. Check Point підкреслює, що, незважаючи на коливання обсягів виманок, загальна загроза залишається незмінною, і закликає до профілактичних заходів, захисних систем на базі штучного інтелекту для протидії як традиційним атакам, так і новим ризикам, пов'язаним з GenAI». ***(Phil Muncaster. Cyber-Attacks on UK Firms Increase at Four Times Global Rate // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news/cyberattacks-uk-firms-increase/). 11.03.2026).***

***

«Згідно з опитуванням Amárach для .IE, майже кожна п'ята з провідних компаній Ірландії зазнала значних кібератак протягом останніх двох років. Цей висновок збігається з даними Garda, які показують, що кількість злочинів, пов'язаних із шахрайством, зросла на 137% за останній рік, головним чином через банківські афери, фішинг та смфінг. У відповідь на це національний реєстр доменів Ірландії .IE запустив першу в країні систему Digital Trust Mark, яку можна описати як NCT для онлайн-ідентифікації, щоб допомогти компаніям продемонструвати, що їхні веб-сайти, електронна пошта та конфігурації доменів відповідають визнаним стандартам найкращої практики… Організації можуть подати заявку через DigitalTrust.ie, де їхня присутність в Інтернеті оцінюється за допомогою запатентованої системи балів; ті, хто отримає оцінку «А», можуть розміщувати символ вовкодава на своєму веб-сайті та в підписі електронної пошти протягом 12 місяців, а ті, хто не відповідає вимогам, отримують рекомендації щодо поліпшення. .IE заявляє, що ця ініціатива покликана підвищити довіру споживачів і цифрову стійкість країни, особливо з огляду на те, що фішинг і вразливість систем залишаються найпоширенішими точками атаки, і застосовується не тільки до доменів .ie, але й до доменів .com та інших доменів, які використовують ірландські організації». ***(Louise McKeown Doogan. Fifth of companies experienced a cyber attack in last two years – survey // Tech Network (https://www.techcentral.ie/fifth-of-copmanies-experienced-cyber-attacks-in-last-two-years-survey/). 03.03.2026).***

***

«…Нова витончена афера в WhatsApp обходить традиційні засоби захисту паролем, перетворюючи надійних контактів на несвідомих спільників, при цьому користувачі навіть не підозрюють, що їхні акаунти зламано. Обман починається з начебто невинного повідомлення від знайомого контакту — наприклад, «Це ти?» — разом із посиланням. Натискання на це посилання перенаправляє користувача на переконливу фальшиву сторінку в соціальній

мережі, яка запитує його номер телефону та подальший код підтвердження WhatsApp, нібито для «безпеки». Вводячи цей код, користувач несвідомо надає дозвіл новому пристрою підключитися до свого облікового запису, надаючи шахраям повний, непомітний доступ до своїх розмов, фотографій та контактів, не викликаючи перезавантаження пароля або виходу користувача з системи…

Згубність цієї афери полягає в її прихованості та здатності до поширення. Поки користувач продовжує користуватися додатком у звичайному режимі, кіберзлочинці можуть читати приватні повідомлення та привласнювати особистість жертви, щоб атакувати її список контактів, тим самим запускаючи небезпечну ланцюгову реакцію. Ризик ще більше посилюється сучасними інструментами штучного інтелекту, здатними швидко імітувати голоси, що збільшує ймовірність шантажу та більш глибокого обману. Щоб захиститися від цього тихого вторгнення, користувачі повинні залишатися пильними: слід стежити за повідомленнями WhatsApp про нові входи на пристрої, регулярно перевіряти розділ «підключені пристрої» у налаштуваннях, увімкнути двоступеневу верифікацію та зберігати здоровий скептицизм щодо нечітких або надзвичайно коротких повідомлень, що містять посилання, навіть від близьких друзів». ***(Ethan Collins. How hackers now use your friends to steal your WhatsApp account // Talk Android (https://www.talkandroid.com/520790-how-hackers-now-use-your-friends-to-steal-your-whatsapp-account/). 08.03.2026).***

***

«Нова техніка обходу, названа «Zombie ZIP», розроблена дослідником у сфері безпеки Крісом Азізом, дозволяє зловмисникам приховувати шкідливі дані всередині стиснутих архівних файлів шляхом навмисного спотворення заголовків ZIP, успішно обходячи 50 із 51 антивірусних двигунів на VirusTotal. Маніпулюючи полем «Method» у заголовку, щоб вказати, що файл нестиснений (Method=0, або STORED), хоча насправді він залишається стисненим за допомогою стандартного алгоритму DEFLATE, ця техніка обманює механізми аналізу безпеки, змушуючи їх сканувати «стиснений шум» замість фактичного корисного навантаження, що призводить до відсутності виявлення сигнатур. Як наслідок, спроба відкрити ці файли за допомогою стандартних утиліт, таких як WinRAR або 7-Zip, призводить до помилок або пошкодження даних. Однак зловмисник може використовувати спеціально розроблений завантажувач, призначений для ігнорування помилкового заголовка та ідеального розпакування корисного навантаження…

Координаційний центр CERT (CERT/CC) опублікував бюлетень щодо цієї загрози, присвоївши їй ідентифікатор CVE-2026-0866, та закликав виробників засобів безпеки запровадити більш сувору перевірку методів стиснення та структур архівів. Однак багато дослідників у сфері кібербезпеки категорично не погоджуються з класифікацією «Zombie ZIP» як легітимної уразливості, що заслуговує на CVE. Вони стверджують, що оскільки ця техніка навмисно пошкоджує структуру файлу — роблячи його неможливим для відкриття стандартними інструментами розпакування на цільовій системі — і вимагає спеціального завантажувача для функціонування, це означає, що пристрій вже

скомпрометований, а отже, це лише новий метод розповсюдження шкідливого програмного забезпечення, а не справжня уразливість». ***(Bill Toulas. New 'Zombie ZIP' technique lets malware slip past security tools // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/new-zombie-zip-technique-lets-malware-slip-past-security-tools/). 10.03.2026).***

***

«Згідно з шостим щорічним звітом HYPR «State of Passwordless Identity Assurance», в рамках якого було опитано понад 950 керівників у сфері IT та безпеки, генеративна штучна інтелігенція та автоматизовані агенти офіційно витіснили викрадені облікові дані з позиції головної проблеми безпеки ідентифікації для підприємств. Цю зміну, яку назвали «переходом до штучного інтелекту», підкреслюють 53 % керівників у сфері безпеки, які називають генеративну штучну інтелігенцію, та 45 %, які вказують на агентивну штучну інтелігенцію як на свої головні ризики. Дослідження виявляє «парадокс швидкості», за якого, незважаючи на швидше виявлення, автоматизовані інструменти дозволяють зловмисникам викрасти дані задовго до того, як людські команди зможуть зреагувати…

Підробка особи є одним із аспектів цієї загрози, що стрімко набирає обертів: 87 % організацій стикаються з аудіо- або відео-діпфейками, а 40 % повідомляють про випадки клонування голосу, спрямовані, зокрема, на такі сфери, як кол-центри. Згідно з прогнозами HYPR, до 2026 року автоматизовані агенти стануть причиною витоку більшої кількості паролів, ніж людські помилки, тому характер ризиків, пов’язаних з ідентифікацією, зміщується у бік автоматизації машин у промислових масштабах. У відповідь на ці складні та швидкі загрози компанії все частіше надають пріоритет постійній верифікації ідентичності; хоча 76% все ще покладаються на застарілі системи облікових даних, 71% повідомляють, що активно переходять на методи аутентифікації без паролів, щоб краще захистити своїх співробітників». ***(Wayne Williams. AI has overtaken stolen passwords as the top identity threat, report says // BetaNews, Inc. (https://betanews.com/article/ai-has-overtaken-stolen-passwords-as-the-top-identity-threat-report-says/). 10.03.2026).***

***

«…Дослідники компанії Aryaka виявили приховану атаку, що тривала цілий рік і була спрямована проти відділів кадрів та рекрутерів. Її організував російськомовний зловмисник, який понад усе прагнув уникнути виявлення. Операція починається з ISO-файлу на тему резюме, який, ймовірно, розповсюджується через спам-листи з посиланнями на хмарні сховища, такі як Dropbox. Після монтування ISO-файл відображає іконку PDF, яка насправді є шкідливим файлом ярлика Windows (.lnk); при запуску він запускає складний ланцюжок інфікування, що включає скрипти PowerShell, які витягують приховані дані з PNG-зображення для завантаження zip-файлу, замаскованого під «SumatraPDF». Цей архів використовує бічне завантаження DLL для виконання шкідливого файлу DWrite.dll, який негайно починає перевірки на наявність антивірусного аналізу, припиняючи роботу, якщо виявляє віртуальні машини,

пісочниці або якщо жертва знаходиться в Росії чи країні СНД. Щоб ще більше приховати свої сліди, шкідливе програмне забезпечення модифікує ключі реєстру Windows Defender, щоб вимкнути хмарний захист та перевірку налаштувань цілісності пам'яті. Найбільш примітно, що зловмисники використовують раніше не задокументований EDR-кілер під назвою «BlackSanta», який завантажує вразливі драйвери режиму ядра (такі як RogueKiller та IObitUnlocker) для втручання в системну пам'ять та програмної нейтралізації засобів захисту кінцевих точок і агентів реєстрації перед розгортанням остаточного корисного навантаження — ймовірно, програми для викрадення інформації…» ***(Zeljka Zorz. HR, recruiters targeted in year-long malware campaign // Help Net Security (https://www.helpnetsecurity.com/2026/03/10/hr-recruiters-malware-resume/). 10.03.2026).***

***

«Аналіз 418 публічно оголошених заходів правоохоронних органів щодо боротьби з кіберзлочинністю за період з 2021 року до середини 2025 року, зібраних у звіті «Security Navigator 2026» від Orange Cyberdefense, спростовує стереотип про те, що кіберзлочинці — це переважно дуже молоді люди. Серед 193 випадків, за якими є дані про вік, найбільшу групу становлять особи віком 35–44 роки (37%), за ними йдуть 25–34 роки (30%) та 18–24 роки (21%), що свідчить про діяльність, яка триває аж до середини кар'єрного дорослого віку та відповідає злочинам, що вимагають планування, технічної компетентності та обдуманого ризику. Моделі злочинів також змінюються з віком: молодші дорослі частіше пов'язані з широким хакерством та експериментами, група 25–34 років демонструє перехід до діяльності, спрямованої на отримання прибутку, а у віковій групі 35–44 років домінують кібершантаж (22%) та шкідливе програмне забезпечення (19%) поряд зі шпигунством, хакерством та відмиванням грошей — операціями з більшим фінансовим або політичним впливом, що вимагають координації та інфраструктури…

Злочинці представляють 64 національності, хоча 58 % ідентифікованих осіб припадає на п'ять з них, що свідчить як про транскордонний характер кіберзлочинності, так і про неоднаковість практики оприлюднення інформації. Автори застерігають, що набір даних охоплює лише ті випадки, які були оприлюднені, і може відрізнятися залежно від юрисдикції, проте вимальовується картина, згідно з якою це, скоріше, досвідчені дорослі особи, які здійснюють складні кібероперації з метою отримання прибутку, а не переважно підлітки-хакери». ***(Anamarija Pogorelec. The people behind cyber extortion are often in their forties // Help Net Security (https://www.helpnetsecurity.com/2026/03/10/cyber-extortion-cybercrime-age-profile/). 10.03.2026).***

***

«…Серія гучних кібератак у 2025 році на провідних британських ритейлерів, зокрема Marks and Spencer, Harrods та аеропорт Хітроу, яскраво продемонструвала зростаючу загрозу, яку становлять вразливості ланцюга поставок. Ці інциденти були спрямовані не на безпосередні порушення безпеки, а

на сторонніх логістичних операторів, IT-постачальників та платформи обслуговування клієнтів, які злочинці використовують для масштабування та прискорення атак з метою отримання доступу до численних організацій, що знаходяться нижче за ланцюгом поставок. Сучасний ланцюг поставок вийшов за межі перевезень і включає мережу взаємопов'язаних програмних платформ та постачальників керованих послуг, що збільшує площу атаки…

Ці ризики ланцюга поставок проявляються різними способами, наприклад, зловмисники можуть зламати систему невеликого незахищеного підрядника, щоб отримати доступ, зловживати надійними каналами зв’язку, такими як API, або вбудовувати шкідливе програмне забезпечення у звичайні оновлення програмного забезпечення. Кінцеві наслідки часто поєднують порушення операційної діяльності з викраденням конфіденційних даних клієнтів, співробітників або стратегічних даних з метою вимагання.

З юридичної точки зору, роздрібні продавці залишаються відповідальними за порушення безпеки даних, навіть якщо вони відбуваються через третю сторону. Такі нормативні акти, як британський GDPR, вимагають від організацій забезпечити, щоб їхні партнери мали «відповідні технічні та організаційні заходи», а нові стандарти безпеки платежів (PCI DSS v4) та майбутнє законодавство, таке як законопроект про кібербезпеку та стійкість, посилюють контроль за стійкістю постачальників…

Щоб зменшити ці ризики, організації повинні розглядати безпеку ланцюга поставок як одну з основних функцій бізнесу. До основних заходів захисту належать: складання карти ланцюга поставок для виявлення критично важливих постачальників, дотримання принципу мінімальних привілеїв для мінімізації «радіусу ураження» потенційного порушення, а також включення суворих вимог щодо безпеки та прав на аудит у договори з постачальниками. Замість того, щоб покладатися на обіцянки, роздрібні торговці повинні вимагати підтвердження дотримання вимог безпеки за допомогою незалежних гарантій, таких як звіти SOC 2. Нарешті, вони повинні розробити та регулярно тестувати посібники з реагування на інциденти, спеціально призначені для випадків збою в ланцюгу постачання. Позитивним результатом цих нещодавніх атак є зростання обізнаності, що змушує постачальників покращувати свою безпеку, створюючи ринок, на якому процвітатимуть безпечні постачальники, а вся екосистема роздрібної торгівлі зможе стати більш стійкою». ***(Ed Hayes. Opinion: How 2025’s cyber ‘10 days of doom’ exposed the UK supply chain threat // Retail Gazette (https://www.retailgazette.co.uk/blog/2026/03/cyber-supply-chain/). 19.03.2026).***

***

«Нещодавнє дослідження, проведене компанією з кібербезпеки LevelBlue, показало, що майже третина державних, місцевих та освітніх організацій зазнала кібератак протягом минулого року, причому багато з них не встигають протистояти складним атакам. Опитування 200 керівників у сфері технологій державного сектору виявило значний розрив між загрозами, з якими вони стикаються, та здатністю реагувати на них: 46% респондентів зазнали збільшення кількості атак. Основною проблемою є зростання загроз, пов'язаних із

штучним інтелектом, які розширюють площину атаки та створюють більш переконливі спроби фішингу; хоча 45% респондентів очікують на такі атаки, лише 28% вважають себе готовими до них…

Цю проблему ускладнює значний ризик у ланцюжку поставок, який називають «ахіллесовою п’ятою», оскільки 44 % агентств не мають повного уявлення про свої системи та партнерів, що дозволяє зловмисникам обходити прямі засоби захисту, націлюючись на надійних постачальників. Для посилення кіберзахисту у звіті наголошується на необхідності більш активної участі керівництва, кращого розуміння екосистем постачальників та постійного навчання персоналу. Дослідження, в якому відзначаються серйозні зриви у роботі урядових структур у 2025 році в таких місцях, як Невада та Сент-Пол, показало, що найбільш стійкими є ті організації, де кібербезпека розглядається як спільна відповідальність, що підтримується на рівні керівництва, що надає їм «попутний вітер» для реалізації програм забезпечення стійкості…» ***(Rae D. DeShong. Report: AI-Driven Cyber Attacks Outpace Public-Sector Defenses // e.Republic LLC (https://www.govtech.com/security/report-growing-threat-surface-challenge-cyber-resilience). 18.03.2026).***

***

«2026 рік став переломним моментом у сфері кібербезпеки, ознаменувавши кардинальний зсув у бік індустріалізації кіберзлочинності та широкого використання штучного інтелекту в злочинних цілях. Згідно з дослідженням компанії Cyble, тіньова економіка перетворилася на повноцінний ринок, де платформи «вимагальне програмне забезпечення як послуга» (RaaS) та посередники з надання початкового доступу (IAB) знизили бар’єри для входу, що дозволило навіть початківцям-злочинцям здійснювати складні атаки…

Зловмисники також широко використовували штучний інтелект у своїх атаках, створюючи надзвичайно реалістичні фішингові кампанії та застосовуючи технологію «діпфейк» для здійснення шахрайства з великими сумами, прикладом чого є переказ 25 мільйонів доларів, санкціонований під час відеодзвінка з використанням «діпфейку». Домінуючим методом вторгнення стала тактика «living off the land» (LotL), за якої зловмисники використовують легітимні системні інструменти, щоб залишатися непоміченими протягом місяців, що робить традиційну безпеку на основі сигнатур неефективною. Це ускладнювалося зловживанням надійними платформами, такими як Google Drive та GitHub, для розповсюдження шкідливого програмного забезпечення…

Крім того, атаки на ланцюги постачання набули більш стратегічного характеру: зловмисники навмисно компрометували сторонніх постачальників, щоб отримати доступ до сотень цілей, розташованих нижче за ланцюгом постачання. Межі між кіберзлочинністю та діяльністю держав розмилися, оскільки геополітична напруга підживлювала атаки на критичну інфраструктуру. У відповідь на цю нову еру доступних і витончених загроз у звіті робиться висновок, що реактивна безпека більше не є життєздатною. До 2027 року організації повинні прийняти проактивну стратегію захисту, зосереджену на прогнозній розвідці, виявленні поведінкових аномалій та підході «припускати проникнення», щоб

ефективно протидіяти мінливому ландшафту». ***(How Cybercriminals Changed Tactics in 2026: Trends Cyble Tracked and What They Mean for 2027 // Cyble Inc. (https://cyble.com/knowledge-hub/cybercriminals-evolved-in-2025-cyble-2026/). 18.03.2026).***

***

«Звіт Expel про загрози на 2026 рік, заснований на понад мільйоні сповіщень SOC за 2025 рік, виявив, що зловмисники все ще переважно покладаються на викрадені облікові дані: понад 68% зареєстрованих інцидентів — це спроби отримати доступ до систем компаній на основі ідентифікаційних даних, використовуючи облікові записи законних користувачів (часто через неавторизованих агентів, що вказує на те, що справжній користувач не входив у систему), а ще 12% — це входи з підозрілих місцевостей, що підкреслює важливість моніторингу та блокування доступу з неавторизованих регіонів або країн…

У звіті також зазначається, що «підроблені редактори PDF» залишаються серйозною загрозою: співробітники, які не мають офіційно затвердженого інструменту для роботи з PDF-файлами, можуть завантажити троянські програми, такі як SupremePDF, які здатні встановлювати механізми персистентності та «задні двері», захоплювати контроль над браузерами, викрадати збережені облікові дані, виконувати довільний код, перехоплювати конфіденційні дані та використовувати зашифрований PowerShell для завантаження корисних навантажень другого рівня. Як тільки це друге корисне навантаження потрапляє в систему, зловмисники можуть переміщатися по мережі та викрадати дані. Ці висновки підкреслюють необхідність постійного навчання співробітників щодо захисту імен користувачів та паролів, розпізнавання спроб викрадення облікових даних та уникнення використання несанкціонованого програмного забезпечення, а також необхідність для організацій надавати затверджені інструменти та посилювати контроль доступу на основі місцезнаходження». ***(Linn Foster Freedman. Expel Annual Threat Report Shows Identity Compromise Continues to Be Threat Actors' Favorite Tool // Robinson & Cole LLP (https://www.dataprivacyandsecurityinsider.com/2026/03/expel-annual-threat-report-shows-identity-compromise-continues-to-be-threat-actors-favorite-tool/). 19.03.2026).***

***

«ФБР та Агентство з кібербезпеки та безпеки інфраструктури США (CISA) попередили, що хакери, пов'язані з російською розвідкою, націлилися на користувачів популярних месенджерів, таких як Signal, і вже зламали тисячі облікових записів. Згідно зі спільним повідомленням, кампанія спрямована на осіб, що мають високу розвідувальну цінність, зокрема на діючих та колишніх урядовців США, військових, політиків та журналістів. Агентства наголосили, що шифрування та базова інфраструктура самих додатків не були порушені; натомість зловмисники використовували складні фішингові техніки, видаючи себе за співробітників служби безпеки та обманюючи користувачів, щоб ті розкрили свої коди безпеки…

Попередження США збігається з нещодавнім повідомленням голландських спецслужб, в якому також йшлося про глобальну операцію, підтриману Росією, з метою проникнення в акаунти Signal і WhatsApp, якими користуються державні посадовці та інші важливі об'єкти. У відповідь компанія Signal заявила, що ці атаки ґрунтувалися на методах соціальної інженерії, а не на недоліках її шифрування чи систем, підкресливши, що головна вразливість полягає в обмані користувачів, а не в самих платформах для обміну повідомленнями». ***(Cyber actors linked to Russia targeting users of messaging apps, FBI says // Reuters (https://www.reuters.com/technology/cyber-actors-linked-russia-are-targeting-users-commercial-messaging-apps-fbi-2026-03-20/). 20.03.2026).***

***

«24 березня Європейська комісія стала жертвою кібератаки, яка зачепила її хмарну інфраструктуру, на якій розміщена веб-платформа «Європа». За попередніми даними, з цих веб-сайтів було викрадено дані, повідомила Комісія в п'ятницю.

У заяві зазначено, що інцидент було швидко локалізовано, а повні наслідки атаки наразі ще розслідуються…

Комісія не назвала жодної групи чи особи, відповідальної за цю кібератаку». ***(EU Commission web platform hit by cyber-attack on March 24 // Reuters (https://www.reuters.com/technology/eu-commission-web-platform-hit-by-cyber-attack-march-24-2026-03-27/). 27.03.2026).***

***

«Нідерландський футбольний клуб «AFC Ajax» повідомив про витік даних після того, як хакер отримав несанкціонований доступ до внутрішніх систем, внаслідок чого були оприлюднені обмежені особисті дані менше ніж 20 осіб, яким заборонено відвідувати стадіон. Однак незалежне розслідування виявило більш серйозні недоліки в системі безпеки мобільного додатку клубу та його серверних систем, що могло б дозволити зловмисникам маніпулювати обліковими записами, передавати абонементи без згоди власників, а також змінювати чи скасовувати заборони на відвідування стадіону. Під час демонстрації журналіст зміг за лічені секунди переоформити VIP-квиток, що належав директору клубу… Через недостатньо захищені API-інтерфейси було виявлено додаткові вразливості, що призвели до витоку конфіденційних даних понад 500 уболівальників, яким заборонено відвідувати матчі. Хоча клуб «Ajax» заявив, що доказів зловживання даними немає, цей інцидент викликав широке занепокоєння щодо таких ризиків, як крадіжка квитків та їх перепродаж на чорному ринку. З того часу клуб усунув ці вразливості, залучив експертів з кібербезпеки, повідомив про порушення владі та попередив користувачів про необхідність бути пильними щодо можливих фішингових атак». ***(Amar Ćemanović. AFC Ajax data breach exposed fan information, risked ticket theft // CyberInsider (https://cyberinsider.com/afc-ajax-data-breach-exposed-fan-information-risked-ticket-theft/). 26.03.2026).***

***

«…Складна кібератака, яка, як вважається, була здійснена підтримуваною Іраном хакерською групою Handala, паралізувала глобальну діяльність американської медичної технологічної компанії Stryker, зупинивши роботу її 56 000 співробітників, у тому числі 4000 працівників на її головній базі в Корку, Ірландія. Нічна атака знищила більшість робочих пристроїв, включаючи особисті телефони з робочим профілем Stryker, і порушила роботу систем, що підключаються до мережі компанії в Європі, Азії та США…

У повідомленнях для співробітників Stryker підтвердив «серйозні глобальні порушення» і заявив, що вони активно співпрацюють з Microsoft для усунення «критичного інциденту в масштабах підприємства», хоча основна причина залишається невідомою. Тим часом, у непідтвердженій заяві Handala взяла на себе відповідальність за атаку, стверджуючи, що вона була помстою за недавній ракетний удар по іранській школі. Хакери заявили, що знищили понад 200 000 систем і викрали 50 терабайт критично важливих даних. В результаті співробітники наразі не можуть працювати, і джерела передбачають, що збій матиме значний ланцюговий ефект для компанії». ***(Danny De Vaal. Stryker cyber attack: Thousands of Irish unable to work as hackers cripple global systems // MGN Limited (https://www.irishmirror.ie/news/irish-news/stryker-cyber-attack-thousands-irish-36850017). 11.03.2026).***

***

«Вебсайт, яким керує «Handala Hack Team» — угруповання, пов'язане з Міністерством розвідки та безпеки Ірану (MOIS), — швидко відновив роботу вже через день після того, як ФБР та Міністерство юстиції США заблокували кілька його доменів у зв'язку з кібератакою 11 березня 2026 року на американську компанію з виробництва медичного обладнання, як повідомляється, Stryker. Американські власті заявили, що є достатні підстави вважати, що ця група здійснила руйнівну атаку за допомогою шкідливого програмного забезпечення, тоді як хакери відкинули це як спробу їх заглушити…

Експерти зазначають, що таке швидке відновлення діяльності підкреслює стійкість кіберзлочинців, пов'язаних з Іраном, які часто відновлюють свою присутність в Інтернеті попри неодноразові перешкоди. Компанія, що стала об'єктом атаки, підтвердила, що відновлює уражені системи, та наголосила на безпеці своїх продуктів, водночас висловивши вдячність уряду за зусилля з протидії цій загрозі». ***(A.J. Vicens. Iran-linked hackers restore website after US seizes domains // Reuters (https://www.reuters.com/technology/iran-linked-hackers-restore-website-after-us-seizes-domains-2026-03-20/). 20.03.2026).***

***

«Лише через кілька днів після того, як ФБР заблокувало веб-сайти іранської хакерської групи Handala внаслідок руйнівної кібератаки на гіганта медичної техніки Stryker, група знову дала про себе знати, оприлюднивши конфіденційні особисті дані 28 інженерів компанії Lockheed Martin, які

працюють в Ізраїлі. Діючи, ймовірно, як прикриття для Міністерства розвідки Ірану, Handala опублікувала імена інженерів, дані їхніх паспортів, ідентифікаційні номери та місця служби, націлившись на осіб, які, як стверджується, працюють над критично важливими військовими проектами Ізраїлю, зокрема над системою протиракетної оборони THAAD та винищувачами F-35 і F-22. У рамках цілеспрямованої кампанії залякування хакери безпосередньо зв'язалися з працівниками, продемонструвавши, що мають доступ до їхніх особистих даних, та поставили їм 48-годинний ультиматум покинути Ізраїль…

Handala погрожував, що невиконання вимог призведе до фізичної розправи або «візитів» до сімей інженерів, які проживають у Сполучених Штатах. Дослідники у сфері кібербезпеки підтвердили автентичність викрадених даних, що збігається з окремою, поки що непідтвердженою заявою іншої проіранської групи, APT Iran, про викрадення 375 ТБ конфіденційних корпоративних даних та креслень у компанії Lockheed Martin. Експерти попереджають, що ці скоординовані інциденти відображають зростаючу тенденцію використання хактивістів як прикриття для відплатної, спонсорованої державою кібервійни, мобілізація якої безпосередньо пов'язана з нещодавніми військовими ударами США та Ізраїлю по Ірану». ***(Gintaras Radauskas. Iranian group behind Stryker breach threatens Lockheed Martin staff in Israel // Cybernews (https://cybernews.com/security/lockheed-martin-israel-breach-handala/). 26.03.2026).***

***

«Дослідники Cisco Talos виявили пов'язану з Китаєм групу кібершпигунів, відому під назвою UAT-9244, яка з 2024 року атакує південноамериканських телекомунікаційних провайдерів з метою отримання постійного доступу до конфіденційних даних зв'язку. Ця група має значні спільні риси з відомими китайськими групами APT (Advanced Persistent Threat) — Famous Sparrow та Tropic Trooper…

У рамках цієї кампанії використовуються три раніше не задокументовані родини шкідливого програмного забезпечення для проникнення в критичну інфраструктуру та збереження контролю над нею. Перша з них, TernDoor, — це бекдор для Windows, що розгортається шляхом бічного завантаження DLL-файлів і вбудовується в звичайні системні процеси. Він забезпечує свою стійкість за допомогою запланованих завдань та модифікацій реєстру, а також встановлює шкідливий драйвер для обходу систем моніторингу безпеки, що дозволяє операторам віддалено виконувати команди та маніпулювати файлами. Другий інструмент, PeerTime, — це універсальний бекдор для Linux на базі ELF, розроблений для різних архітектур процесорів (включно з ARM та MIPS), що використовуються в телекомунікаційних серверах та маршрутизаторах. Варто зазначити, що він використовує децентралізований протокол BitTorrent для зв'язку з командним центром, приховуючи інфраструктуру зловмисників, та містить рядки налагодження спрощеною китайською мовою. Третій інструмент, BruteEntry, — це програма на базі Go, яка перетворює скомпрометовані периферійні пристрої на розподілену мережу сканування (операційні релейні бокси). Він проводить атаки методом грубої сили на облікові дані проти відкритих служб, таких як SSH та

Postgres, надсилаючи успішні логіни назад зловмисникам для полегшення подальшого розширення мережі…» ***(Pooja Tikekar. China-Linked Hackers Use Malware Trio for Telecom Espionage // Information Security Media Group, Corp. (https://www.databreachtoday.co.uk/china-linked-hackers-use-malware-trio-for-telecom-espionage-a-30940). 06.03.2026).***

***

«Група хакерів-вимагачів «Qilin», пов'язана з Росією, взяла на себе відповідальність на своєму сайті в даркнеті за кібератаку на Tennessee Valley Electric Cooperative (TVEC) — енергопостачальну компанію, що обслуговує округи Вейн і Хардін у Західному Теннессі через електромережу протяжністю 2 000 миль і є членом федеральної мережі Tennessee Valley Authority. TVEC ще не підтвердила цей інцидент, і масштаби порушення залишаються незрозумілими, оскільки Qilin лише вказала назву компанії, не оприлюднивши зразків даних — це типова початкова тактика шантажу, покликана чинити тиск на жертв, перш ніж погрожувати оприлюдненням викрадених даних у разі невиконання вимог щодо викупу. Дослідники попереджають, що викрадення даних про критичну інфраструктуру або операційні процедури може сприяти подальшим цілеспрямованим атакам, а викрадення інформації про клієнтів або співробітників може призвести до шахрайства та соціальної інженерії…

Вперше виявлена у 2022 році, угруповання Qilin стало найактивнішим угрупованням-вимагачем у 2025 році, нарахувавши понад 1 455 жертв з 2023 року. Ця група має досвід атак на відомі організації та об'єкти критичної інфраструктури по всьому світу. Серед останніх жертв — Malaysia Airlines, Міжнародний аеропорт Талси, SK Telecom, Volkswagen Group France та Nissan Japan. Варто зазначити, що це не перша їхня атака на енергетичний сектор Північної Америки; минулого року Qilin атакувала дві електричні кооперативи в Техасі — San Bernard та Karnes — а згодом заявила, що викрала 222 ГБ даних у Spark Power, канадської компанії з надання електричних послуг, що працює в США». ***(Paulina Okunytė. "US power provider attacked," claim Russian cyber gang // Cybernews (https://cybernews.com/security/qilin-ransomware-us-power-grid-attack/). 06.03.2026).***

***

«Таємна кампанія з кібершпигунства, яку пов'язують із пов'язаною з Китаєм групою Red Menshen, спрямована проти глобальних телекомунікаційних провайдерів. У ній використовується вдосконалений бекдор для Linux під назвою BPFdoor, що забезпечує тривалий прихований доступ. На відміну від типового шкідливого програмного забезпечення, BPFdoor працює на рівні ядра та пасивно відстежує мережевий трафік, активуючись лише після отримання спеціально сформованих «магічних» пакетів, що дозволяє йому залишатися практично непомітним для стандартних засобів безпеки… Зловмисники проникають у мережі через системи, підключені до Інтернету, такі як VPN, брандмауери та маршрутизатори, після чого розгортають додаткові інструменти для забезпечення стійкості та збору облікових даних, перш ніж глибше вбудувати BPFdoor в інфраструктуру. Оскільки телекомунікаційні мережі

передають величезні обсяги конфіденційних даних — зокрема, повідомлення, метадані та інформацію про місцезнаходження — такий доступ відкриває можливості для масштабного стеження, а не лише для простого викрадення даних… Нові варіанти BPFdoor ще більше покращують прихованість, ховаючи тригери в зашифрованому HTTPS-трафіку та забезпечуючи приховане спілкування через ICMP, ефективно маскуючи зловмисну діяльність під звичайну мережеву активність. Через низький рівень функціонування виявлення цієї загрози вимагає більш глибокого моніторингу системної та мережевої активності, що виходить за межі звичайних засобів захисту». ***(Bill Mann. New stealthy BPFdoor malware variant discovered in telecom networks // CyberInsider (https://cyberinsider.com/new-stealthy-bpfdoor-malware-variant-discovered-in-telecom-networks/). 27.03.2026).***

***

«Група APT41, пов'язана з Китаєм, яка діє з 2012 року (також відома під назвами Wicked Panda, Brass Typhoon та BARIUM), використовує надзвичайно витончену гібридну модель атак, що органічно поєднує шпигунство, спонсороване державою, з кіберзлочинністю, спрямованою на отримання фінансової вигоди. Використовуючи розгалужену сучасну поверхню атаки підприємств, APT41 агресивно націлюється на хмарні робочі навантаження, ланцюги постачання, віддалені пристрої та операційні технології (OT) у різних секторах, таких як охорона здоров'я, телекомунікації, ігри та фінанси. Світова морська галузь є яскравим прикладом розширення їхнього впливу; група успішно проникла в судноплавні та логістичні підприємства по всій Європі та Азії, використовуючи конвергенцію IT- та OT-систем за допомогою сучасних фреймворків шкідливого програмного забезпечення, таких як DUSTTRAP, ShadowPad та VELVETSHELL…

Для збереження прихованості, розширення прав доступу та забезпечення довгострокового постійного доступу APT41 використовує широкий оперативний інструментарій, що налічує понад 90 сімейств шкідливого програмного забезпечення, вміло поєднуючи загальнодоступні утиліти, такі як Cobalt Strike та Mimikatz, із спеціально розробленими імплантами, такими як KEYPLUG та MoonBounce. Масштабність та серйозність їхніх кампаній, які іноді передбачають використання програм-вимагачів, спонукали американські органи влади у 2019 та 2020 роках оприлюднити звинувачення проти кількох членів угруповання у несанкціонованому доступі, крадіжці особистих даних, відмиванні грошей та рекетирстві… Зрештою, захист від високоадаптованої та двоцільової загрози APT41 вимагає від організацій виходу за межі традиційних точкових рішень та впровадження комплексного, безперервного управління поверхнею атаки для захисту своїх дедалі більш взаємопов'язаних середовищ». ***(China's APT41 and the Expanding Enterprise Attack Surface: What Security Teams Must Prepare For // Cyble Inc. (https://cyble.com/blog/apt41-enterprise-attack-surface-cyber-risk/). 27.03.2026).***

***

«…постачальник платформи кібербезпеки Huntress повідомляє, що зловмисники використовують інтерес до популярного AI-асистента OpenClaw, розміщуючи підроблені інсталятори в репозиторіях з відкритим кодом, що змушує користувачів завантажувати шкідливе програмне забезпечення замість справжньої програми. Дослідник Джей Мінтон виявив розміщений на GitHub «інсталятор» (який згодом було видалено), що використовував Stealth Packer для проникнення в системи, скидання правил брандмауера та розгортання GhostSocks, перетворюючи комп'ютери жертв на ретранслятори трафіку, здатні обходити засоби захисту від шахрайства та MFA; пакети можуть містити додаткові корисні навантаження…

Ця кампанія з підробки особи відрізняється від раніше спостережуваних зловмисних «навичок» OpenClaw і була посилена, коли результати пошуку Bing, згенеровані штучним інтелектом, рекомендували зловмисне репозиторій, направляючи навіть технічних користувачів до заражених пакетів. У більш широкому сенсі надання агентних інструментам штучного інтелекту глибокого доступу до системи підвищує ризики — витік даних, швидке введення та надмірно привілейовані ланцюжки інструментів, якими можуть скористатися зловмисники. Порада Huntress: не піддавайтеся FOMO, отримуйте інсталятори тільки з офіційних джерел, перевіряйте походження та підписи репозиторіїв і двічі перевіряйте інструкції з інсталяції перед розгортанням помічників штучного інтелекту…» ***(Eoin Higgins. New vulnerability in open-source repositories uses fake OpenClaw install to attack // Morning Brew Inc. (https://www.itbrew.com/stories/2026/03/03/new-vulnerability-in-open-source-repositories-uses-fake-openclaw-install-to-attack). 04.03.2026).***

***

«Дослідники Trend Micro виявили новий шкідливий код на мові C/C++, призначений для викрадення даних, який отримав назву BoryptGrab. Він поширюється з кінця 2025 року через численні ZIP-архіви, розміщені у фальшивих репозиторіях GitHub, що маскуються під безкоштовні програмні інструменти. Ця шкідлива програма, розроблена з використанням дедалі більш витончених технічних рішень, застосовує різні методи виконання — зокрема завантаження DLL-файлів, сценарії VBS, виконувані файли .NET та завантажувач на мові Golang під назвою HeaconLoad — і містить перевірки віртуальних машин та антианалітичні механізми, намагаючись запускатися з підвищеними привілеями…

Після запуску BoryptGrab систематично збирає широкий спектр конфіденційних даних. Він витягує інформацію з майже десятка веб-браузерів (використовуючи технології шифрування Chrome App Bound Encryption та допоміжний модуль Chromium), збирає дані з настільних криптовалютних гаманців і розширень браузера, а також викрадає системну інформацію, файли з певними розширеннями, файли Telegram, паролі браузерів і токени Discord. Він також робить знімки екрана, а потім архівує та викрадає всі вкрадені дані на сервер управління та контролю (C&C) зловмисника. Крім того, деякі версії BoryptGrab

розгортають додатковий корисний вантаж під назвою TunnesshClient. Цей бекдор встановлює зворотний SSH-тунель для C&C-комунікації, що дозволяє зловмисникам виконувати команди оболонки, діяти як SOCKS5-проксі та повністю маніпулювати файловою системою жертви шляхом завантаження, вивантаження, пошуку та передачі цілих папок». ***(Ionut Arghire. Malware & Threats Over 100 GitHub Repositories Distributing BoryptGrab Stealer // Wired Business Media, Inc. (https://www.securityweek.com/over-100-github-repositories-distributing-boryptgrab-stealer/). 07.03.2026).***

***

«Після п'ятирічної перерви, протягом якої група покладалася на прості фішингові імпланти, відома російська група зловмисників Sednit, що діє за підтримки держави, повернулася до використання надзвичайно складного, спеціально розробленого набору шкідливих програм. Ця відновлена кампанія, виявлена дослідниками ESET під час розслідування у 2024 році щодо зломів, спрямованих проти українських військовослужбовців, свідчить про відродження розробки Sednit передового шкідливого програмного забезпечення, ймовірно, під впливом триваючої війни в Україні…

Основу цього нового набору інструментів складають два основні імпланти, призначені для довгострокового кібершпигунства. Перший — Covenant — це суттєво модифікована версія фреймворку з відкритим кодом для пост-експлуатації на базі .NET, що підтримує понад 90 функцій, зокрема витік даних, горизонтальне переміщення та моніторинг цілей, і слугує основним інструментом шпигунства угруповання. Другий — це BeardShell, абсолютно новий, ретельно розроблений імплант, що діє як інтерпретатор PowerShell. BeardShell функціонує насамперед як резерв для повторного розгортання Covenant у разі його виявлення. Варто зазначити, що BeardShell інтегрується з легітимним хмарним сервісом Icedrive для комунікацій управління та контролю (C2) — складне досягнення, досягнуте шляхом реверс-інжинірингу клієнта, оскільки Icedrive не має публічного API…

Для проникнення в системи жертв Sednit зазвичай використовує методи соціальної інженерії через Signal або WhatsApp, спонукаючи жертв відкривати заражені троянами документи Excel або Word, а іноді навіть безпосередньо телефонуючи їм. Впровадження цих шкідливих програм значно ускладнює їх виявлення та нейтралізацію для захисників; спеціальні ланцюжки завантаження постійно оновлюються, а завдяки використанню різних легальних хмарних інфраструктур для зв’язку з C2 зловмисники можуть легко обходити традиційні засоби моніторингу мережі та ускладнювати спроби знешкодження їхньої інфраструктури». ***(Jai Vijayan. Russian Threat Actor Sednit Resurfaces With Sophisticated Toolkit // TechTarget, Inc. (https://www.darkreading.com/cyber-risk/sednit-resurfaces-with-sophisticated-new-toolkit). 10.03.2026).***

***

«ThreatDown, підрозділ компанії Malwarebytes, виявив першу задокументовану кібератаку, в якій для розгортання безфайлового шкідливого програмного забезпечення використовується легітимне середовище

виконання JavaScript Deno. Ця складна кампанія починається з приманки соціальної інженерії «ClickFix» — наприклад, підробленої помилки браузера або CAPTCHA — яка спонукає жертв вручну запустити початковий скрипт. Цей скрипт непомітно встановлює Deno, використовуючи надійний, підписаний кодом інструмент розробника для запуску зашифрованого шкідливого коду та обходу традиційних засобів захисту кінцевих точок у рамках вдосконаленого розширення техніки «living-off-the-land». Потім зловмисники використовують стеганографію для вилучення прихованого, зашифрованого корисного навантаження з начебто нешкідливого зображення у форматі JPEG та вводять його безпосередньо в пам'ять системи…

Оскільки шкідливе ПЗ ніколи не записує виконуваний файл на диск, воно залишається повністю невидимим для стандартних антивірусних двигунів, що сканують файли. Після запуску кінцевий шкідливий модуль — троян віддаленого доступу під назвою CastleRAT — бере під повний контроль уражену машину для проведення прихованого шпигунства, що включає фіксацію натискань клавіш, крадіжку криптовалюти, несанкціоноване спостереження за веб-камерою та мікрофоном, а також створення стійких, невидимих «задніх дверей»… Отже, експерти з безпеки наголошують, що боротьба з такими вкрай важко виявляємими загрозами вимагає вдосконаленого моніторингу поведінки кінцевих точок, здатного виявляти аномальне виконання процесів та несанкціоновані комунікації типу «команда-контроль» під час роботи системи». ***(ThreatDown Uncovers First Cyber Attack Abusing Deno JavaScript Runtime for Fileless Malware Delivery // Business Wire, Inc. (https://www.businesswire.com/news/home/20260310775713/en/ThreatDown-Uncovers-First-Cyber-Attack-Abusing-Deno-JavaScript-Runtime-for-Fileless-Malware-Delivery). 10.03.2026).***

***

«Згідно з доповіддю Thales Bad Bot Report за 2025 рік, у 2024 році понад половина всього інтернет-трафіку (51 %) була автоматизованою, причому 37 % було класифіковано як відверто шкідливе. Ці боти вже не є примітивними скриптами; завдяки штучному інтелекту та великим мовним моделям вони тепер досконало імітують людські кліки, паузи, ритм набору тексту і навіть відповіді у розмові, що робить традиційні методи виявлення дедалі менш ефективними. Глобальні збитки вражають: за оцінками Imperva, атаки ботів та зловживання API коштують бізнесу до 186 мільярдів доларів щорічно через скрейпінг, накопичення запасів, шахрайство, дезінформацію та атаки типу «відмова в обслуговуванні»…

Саме по собі блокування або обмеження пропускної здатності — це програшна стратегія; витрати зловмисників на запуск тисяч ботів залишаються незначними, тоді як захисники опиняються у пастці нескінченної гри в «кота й мишу». Єдиний надійний спосіб перемогти, як стверджує Тім Ейлінг, віцепрезидент з питань кібербезпеки в регіоні EMEA компанії Thales, — це змінити економічну ситуацію: зробити атаку настільки обчислювально затратною, щоб вона стала збитковою.

Найелегантнішим рішенням є сучасна «цифрова отруйна пігулка», побудована на основі невидимих завдань типу Proof-of-Work (PoW). Кожного разу, коли клієнт

запитує сторінку, виклик API або дію, сервер видає невелику криптографічну задачку, яку справжній браузер без зусиль вирішує у фоновому режимі один раз. Легітимний користувач нічого не відчуває, але бот, який намагається виконати ту саму дію тисячі разів на хвилину, швидко витрачає величезні ресурси процесора та час, перетворюючи свою найбільшу силу (швидкість і масштаб) на руйнівний тягар…

Цей підхід виявився надзвичайно ефективним у випадку з високоцінними цілями, такими як авіакомпанії, де боти видають себе за клієнтів, щоб скуповувати квитки, спотворювати ціни та порушувати роботу систем. Поєднуючи точну ідентифікацію поведінкових відбитків із поступовим підвищенням витрат на PoW, захисники змушують зловмисників або сповільнитися до людської швидкості (що руйнує їхню бізнес-модель), або накопичувати непосильні рахунки за хмарні обчислення. По суті, ця стратегія запозичує як корпоративні тактики захисту (захисні заходи при ворожих поглинаннях), так і фехтування: замість того, щоб намагатися парирувати кожен удар, ви робите кожну атаку настільки виснажливою та дорогою, що супротивник зрештою опускає захист або відступає. У добу ботів на базі штучного інтелекту перемога більше не належить тому, хто виявляє найбільше загроз; вона належить тому, хто робить атаку просто невартим зусиль». ***(Tim Ayling. The poison pill that malicious bots can't digest // Future US, Inc. (https://www.techradar.com/pro/the-poison-pill-that-malicious-bots-cant-digest). 10.03.2026).***

***

«Нещодавно виявлене шкідливе програмне забезпечення для ботнету під назвою KadNap активно атакує маршрутизатори ASUS та інші периферійні мережеві пристрої, з серпня 2025 року заразивши приблизно 14 000 пристроїв з метою створення однорангової проксі-мережі для передачі шкідливого трафіку. За даними дослідників з Black Lotus Labs (Lumen Technologies), шкідливе програмне забезпечення використовує модифікований протокол розподіленої хеш-таблиці (DHT) Kademlia для підключення до своєї інфраструктури управління та контролю (C2), децентралізуючи мережу, щоб уникнути традиційних заходів з її виведення з ладу та внесення до списків блокування. Майже половина заражених пристроїв підключається до серверів C2, призначених для ботів ASUS, а решта — до двох окремих серверів управління; географічно 60 % жертв знаходяться у США, за ними йдуть значні групи у Тайвані, Гонконзі та Росії…

Ланцюг зараження починається зі шкідливого скрипта (aic.sh), який забезпечує свою стійкість за допомогою завдання cron, що виконується кожні 55 хвилин, і розгортає бінарний ELF-пакет під назвою «kad». Хоча спеціальний протокол Kademlia ефективно приховує IP-адреси C2 в системі peer-to-peer, дослідники виявили критичну вразливість: заражені вузли постійно підключаються до двох конкретних проміжних вузлів, перш ніж досягти серверів управління, що частково підриває децентралізацію та викриває інфраструктуру. KadNap пов'язаний із проксі-сервісом Doppelganger — ймовірним ребрендингом сервісу Faceless, пов'язаного зі старішим ботнетом TheMoon, — який монетизує мережу, продаючи доступ до скомпрометованих пристроїв як резидентні проксі для DDoS-атак, атак

методом підбору облікових даних та кампаній методом грубої сили. Lumen проактивно заблокував весь трафік до інфраструктури C2 у власній мережі та оприлюднює індикатори компрометації, щоб допомогти ширшій спільноті з безпеки зруйнувати цей ботнет». ***(Bill Toulas. New KadNap botnet hijacks ASUS routers to fuel cybercrime proxy network // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/new-kadnap-botnet-hijacks-asus-routers-to-fuel-cybercrime-proxy-network/). 10.03.2026).***

***

«Загрози, пов'язані з файлами, залишаються одними з найскладніших викликів у сфері кібербезпеки, особливо коли йдеться про нове шкідливе програмне забезпечення або шкідливі програми типу «нульового дня», які традиційні засоби виявлення не в змозі ідентифікувати. У відповідь на це компанія Glasswall, що спеціалізується на захисті файлів, випустила Glasswall Foresight — рішення на базі штучного інтелекту, яке поєднує машинне навчання з перевіреною технологією Content Disarm and Reconstruction (CDR) для надання прогнозної інформації щодо загроз, пов'язаних з файлами…

На відміну від традиційних підходів, таких як поведінкова пісочниця або моделі штучного інтелекту, що покладаються на зовнішні джерела інформації про загрози, Foresight отримує аналітичні дані безпосередньо з детермінованого аналізу структури файлів, що виконується під час процесу CDR, що дозволяє йому виявляти ознаки шкідливості навіть у файлах, які вже пройшли очищення, або в автономних середовищах з ізольованим доступом, де традиційні інструменти виявляються неефективними. Інтегроване в платформу Meteor компанії, це рішення призначене для доповнення існуючих робочих процесів CDR, а не для їх заміни, розширюючи підхід Glasswall «Zero Trust» від очищення файлів до практичної інформації про загрози. За словами компанії, Foresight пропонує організаціям шлях до зменшення залежності від дорогої та операційно вимогливої інфраструктури пісочниць, одночасно забезпечуючи більш чітку видимість ворожої файлової активності, що потрапляє в їхні середовища…» ***(Ian Barker. New solution uses AI to spot file-based threats // BetaNews, Inc. (https://betanews.com/article/new-solution-uses-ai-to-spot-file-based-threats/). 10.03.2026).***

***

«Дослідники з компаній Symantec та Carbon Black виявили цілеспрямовану кампанію з розповсюдження шкідливого програмного забезпечення, в якій використовується зламана версія продукту безпеки Cobra DocGuard від Esafenet для пошуку та викрадення конфіденційних даних про системи балістичних ракет на віддалені сервери, що посилює занепокоєння щодо національної безпеки та кібершпигунства. Хоча підтвердженого зв'язку з китайською розвідкою немає, використання спеціально розробленого штаму під назвою Speagle вказує на вкрай стратегічну операцію зі збору інформації. Зловмисники використовують статус DocGuard як легітимного інструменту безпеки для створення надійних каналів «клієнт-сервер», що дозволяє шкідливій діяльності

зливатися з оточенням і залишатися непоміченою — це зловживання довірою до інфраструктури безпеки…

Цей інцидент став продовженням попередніх випадків компрометації Cobra DocGuard, зокрема порушення безпеки у 2022 році та атаки на ланцюжок постачання, про яку компанія ESET повідомила у травні 2023 року, спрямованої проти гемблінг-компанії з Гонконгу. Це викриває постійні слабкі місця в ланцюжку постачання програмного забезпечення та ризики, пов'язані з використанням сторонніх рішень у сфері безпеки. Загалом, це відкриття підкреслює зростаючу витонченість загроз, спрямованих на цінні оборонні дані, та необхідність постійного моніторингу, аудиту та перевірки навіть «надійних» інструментів у критично важливих середовищах». ***(Naveen Goud. Malware hunts for information related to Ballistic Missiles // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/malware-hunts-for-information-related-to-ballistic-missiles/). 19.03.2026).***

***

«Атака NotPetya 2017 року, яку згодом Велика Британія та США приписали російській військовій операції, поширилася далеко за межі своїх цільових об'єктів в Україні та завдала світовій економіці збитків, що, за оцінками, становлять 10 мільярдів доларів, що робить її одним із найзначніших кіберінцидентів, які коли-небудь фіксувалися. У статті основна увага приділяється не її впливу на іноземних жертв, а менш дослідженому питанню про те, скільки шкоди Росія могла завдати сама собі через побічні наслідки кібератаки. Під «ефектом переливу» маються на увазі ненавмисні наслідки наступальних кібероперацій для держав, що не беруть у них участі, або навіть для власних систем зловмисника, і NotPetya подається як важливий приклад для оцінки того, чи є такі ризики настільки серйозними, як часто побоюються. Хоча кіберзброю іноді зображують як дешеву, потужну та потенційно катастрофічну, реальні факти зазвичай свідчать про більш обмежені та тимчасові наслідки…

На основі публічних звітів, даних страхових компаній та порівняння з аналогічними показниками великих західних компаній-жертв, таких як Merck і Maersk, автори аналізу приходять до висновку, що власні збитки Росії від вірусу NotPetya, ймовірно, були незначними — приблизно 245 мільйонів доларів, і навіть за найвищою оцінкою, отриманою в результаті стрес-тестування (735 мільйонів доларів), вони все одно становитимуть лише близько 0,047 % ВВП Росії, що значно нижче загальноприйнятих порогових значень, які визначають істотну економічну шкоду. За повідомленнями, російські компанії, такі як «Роснефть» і «Сбербанк», зазнали впливу, але не настільки, щоб це серйозно зашкодило їхній основній діяльності…

Отже, навіть у цьому прикладі, який є майже найгіршим сценарієм кіберрозповсюдження та самоушкодження, економічний вплив на зловмисника був обмеженим і навряд чи змінить процес прийняття стратегічних рішень. Хоча ризики наступальних кібероперацій все ще слід сприймати серйозно, дані щодо NotPetya свідчать про те, що побоювання щодо катастрофічного самоушкодження можуть бути перебільшеними і не повинні надмірно обмежувати майбутнє

мислення щодо використання наступальних кіберможливостей». ***(Tom Johansmeyer. Friendly Cyber Fire: How Much Did NotPetya Cost Russia? // Irregular Warfare Initiative (https://irregularwarfare.org/articles/notpetya-cost-russia/). 20.03.2026).***

***

«Атака на ланцюжок постачання, спрямована на широко використовувану бібліотеку LiteLLM для Python на PyPI, призвела до впровадження шкідливого програмного забезпечення для викрадення облікових даних у версії 1.82.7 та 1.82.8, які короткий час поширювалися, незважаючи на те, що не відповідали офіційному коду проекту на GitHub. Атака, яку приписують групі TeamPCP, полягала у вставці невеликої кількості зашифрованого коду, що автоматично виконувався під час імпорту, а в одну з версій було додано більш досконалий механізм персистентності, що дозволяв запускати шкідливе ПЗ навіть без безпосереднього використання бібліотеки… Після запуску шкідливе ПЗ збирало конфіденційні дані — зокрема облікові дані для хмарних сервісів, ключі SSH, секретні дані Kubernetes та системну інформацію — шифрувало їх і виводило на інфраструктуру, контрольовану зловмисниками. Воно також забезпечувало горизонтальне переміщення в середовищах Kubernetes шляхом розгортання привілейованих подів та встановлення постійного бекдору для безперервного доступу. Ця кампанія має тісний зв'язок із попередніми атаками тієї ж групи, зокрема з компрометацією інструментів CI/CD… З огляду на широке використання LiteLLM у робочих процесах штучного інтелекту, цей інцидент становить значний ризик, що спонукає до рекомендацій видалити уражені версії, змінити всі облікові дані та посилити заходи безпеки ланцюга постачання, такі як фіксація залежностей та перевірка цілісності пакетів». ***(Bill Mann. New supply chain attack hits LiteLLM with 95M monthly downloads // CyberInsider (https://cyberinsider.com/new-supply-chain-attack-hits-litellm-with-95m-monthly-downloads/). 24.03.2026).***

***

Програми-вимагачі

«Програми-вимагачі залишаються основною кіберзагрозою для організацій, а ситуація в цій сфері характеризується більш швидкими, витонченими та високо персоналізованими атаками. Згідно з щорічним звітом S-RM «Cyber Incident Insights Report», в якому проаналізовано 800 глобальних інцидентів у 2025 році, 24% жертв програм-вимагачів заплатили викуп, що є значним збільшенням порівняно з 14% у 2024 році. Середній розмір виплаченого викупу становив 296 000 доларів, а найвищий — 1,9 мільйона доларів. США залишаються країною, яка найчастіше стає мішенню атак, на яку припадає 60% інцидентів, хоча в Азіатсько-Тихоокеанському регіоні кількість організацій, згаданих на сайтах з витоками інформації, зросла на 59%, а у Великобританії кількість жертв зросла на 5%. Хоча 45% інцидентів спричинили такі відомі групи,

як Akira та Qilin, організації зіткнулися загалом із 67 різними зловмисниками, що на 16% більше, ніж раніше, причому все більшу стурбованість викликають нові, непередбачувані групи…

Оскільки 88% організацій зараз мають резервні копії даних, зловмисники адаптувалися, зробивши викрадення даних своєю стандартною тактикою (що відбувається в 80% випадків), що дозволяє їм «подвійно шантажувати» жертв, погрожуючи продати або оприлюднити викрадені дані. Незважаючи на ці зростаючі загрози, багато організацій страждають від слабкої кібергігієни. Лише 22% жертв мали активну систему виявлення та реагування на кінцевих точках (EDR), а 47% жертв компрометації ділової електронної пошти (BEC) не застосовували багатофакторну автентифікацію (MFA)… До типових точок входу належать вразливості VPN (68% випадків використання програм-вимагачів), однофакторні рішення для віддаленого доступу (39%) та вразливості в інфраструктурі, що є загальнодоступною (27,6%), тоді як фішинг облікових даних став причиною 80% атак BEC. Найбільш уразливими секторами були фінансові послуги, професійні послуги та будівництво, які були обрані через їхню сприйняту заможність та потенціал для порушення роботи. Експерти наголошують, що організації повинні застосовувати цілісний, гнучкий підхід, що поєднує безпеку та оперативну стійкість, щоб протистояти цим неминучим атакам». ***(Rachel Sim. Report: 24% of Ransomware Victims End Up Paying Out // DIGIT (https://www.digit.fyi/report-24-of-ransomware-victims-end-up-paying-out/). 10.03.2026).***

***

«Згідно з останнім щорічним кіберзвітом Pinsent Masons, в якому розглядаються інциденти, що трапилися з січня по грудень 2025 року, 52% всіх кіберінцидентів припадає на програми-вимагачі, а найпоширенішим зловмисником є група Akira (вона причетна до 26% випадків). У звіті відзначається перехід до більш тривалих операційних і фінансових збитків, оскільки 59% інцидентів були пов'язані з втратою або крадіжкою даних. Найбільше постраждали сектори охорони здоров'я (13%) і роздрібної торгівлі (12%), причому особливо вразливими виявилися організації, що покладаються на складні, критичні за часом ланцюги поставок; нещодавні гучні зриви роботи таких британських компаній, як Co-Op і Marks & Spencer, обійшлися в сукупності в понад 1 млрд фунтів стерлінгів… Вимоги щодо викупу значно варіювалися: від 10 000 доларів до 1 мільйона доларів, про які домовилися в результаті переговорів. Хоча експлуатація вразливостей і фішинг залишалися основними методами атак, у звіті містилася позитивна інформація: 83% клієнтів фірми мали кіберстрахування, що свідчить про активну участь керівництва в управлінні ризиками. Дивлячись у майбутнє, Лора Гіллеспі, партнерка компанії, підкреслила, що надійна кібербезпека зараз є фундаментальною вимогою бізнесу, особливо в умовах посилення регуляторного середовища. Великобританія та Ірландія просувають нове законодавство у сфері кібербезпеки, таке як британський законопроект про кібербезпеку та стійкість, а уряд Великобританії розглядає більш жорсткі заходи, включаючи обов'язкове повідомлення про інциденти та цільову заборону на виплати викупу, що робить

надзвичайно важливим для організацій постійне оновлення своїх протоколів реагування на інциденти». ***(Shannon Williams. Ransomware dominates UK cyber incidents, data loss surges // TechDay (https://securitybrief.co.uk/story/ransomware-dominates-uk-cyber-incidents-data-loss-surges). 10.03.2026).***

***

«Згідно з доповіддю MGA «Cyber Claims Report 2026», ситуація з кібершантажем змінюється: хоча початкові вимоги викупу за допомогою програм-вимагачів зросли на 47% у 2025 році, рекордні 86% жертв відмовилися платити. Така зростаюча стійкість пояснюється вдосконаленням систем резервного копіювання, поліпшенням планів реагування на інциденти та переговорами за підтримки страхових компаній. Хоча вимагання викупу залишається найдорожчим видом страхових виплат — в середньому 269 000 доларів за інцидент, що часто супроводжується дорогою тактикою «подвійного вимагання», коли дані одночасно шифруються і викрадаються, — насправді воно становить меншу частину від загальної суми страхових виплат…

Натомість, більшість кіберінцидентів відбувається за допомогою старих методів, причому 58% усіх випадків припадає на компрометацію ділової електронної пошти (BEC) та шахрайство з переказом коштів (FTF). Цікаво, що хоча загальна частота страхових випадків дещо зросла на 3%, середня тяжкість усіх страхових випадків знизилася на 19% до 116 000 доларів. Коаліція також успішно відшкодувала 21,8 мільйона доларів викрадених коштів для страхувальників, підкресливши важливість раннього повідомлення…

У звіті підкреслюється розбіжність у націленості на основі розміру компанії: підприємства з доходом понад 100 мільйонів доларів стикалися з претензіями в п'ять разів частіше, ніж менші організації, через більшу площу атаки. Однак середні збитки для цих більших компаній фактично зменшилися, що свідчить про те, що їхні інвестиції в засоби контролю безпеки та реагування на інциденти ефективно обмежують збитки. Для малих і середніх підприємств (МСП), які не мають таких внутрішніх можливостей, ці висновки підкреслюють необхідність страхових продуктів, що об'єднують послуги з безпеки та встановлюють чіткі мінімальні стандарти». ***(Josh Recamara. Revealed - what's changing about cyber claims // KM Business Information US, Inc (https://www.insurancebusinessmag.com/us/news/cyber/revealed--whats-changing-about-cyber-claims-567598.aspx). 05.03.2026).***

***

«Дослідники з MalBeacon виявили, що партнерська група-розповсюджувач програм-вимагачів Velvet Tempest (також відома як DEV-0504) використовувала поєднання техніки соціальної інженерії «ClickFix» та легітимних утиліт Windows для розгортання шкідливого ПЗ DonutLoader та бекдору CastleRAT. Ця 12-денна операція була відстежена в лютому в імітованому середовищі американської некомерційної організації, що налічувало понад 3 000 кінцевих точок. Атака розпочалася з кампанії зловмисної реклами, яка обманом

змушувала жертв через підроблену CAPTCHA вставляти шкідливу команду у діалогове вікно «Виконати» Windows (техніка ClickFix)…

Ця дія запустила вкладені ланцюжки команд, у яких використовувалися такі інструменти, як finger.exe та PowerShell, для завантаження корисних даних — зокрема архіву, замаскованого під PDF-файл, — компіляції компонентів .NET за допомогою csc.exe та забезпечення стійкості за допомогою компонентів Python. Отримавши початковий доступ, зловмисники провели детальне вивчення Active Directory та хостів, а також використали скрипт PowerShell для збору облікових даних Chrome. Операція завершилася розгортанням DonutLoader та бекдору CastleRAT — інструменту, відомого тим, що розповсюджує різні RAT та програми для викрадення інформації…

Хоча скрипт PowerShell було відстежено до IP-адреси, яка раніше пов'язувалася з атаками програм-вимагачів Termite, а група Velvet Tempest історично відома тим, що використовує руйнівні штами програм-вимагачів з подвійним вимаганням, такі як Ryuk, Conti та LockBit, зловмисники, що здійснили цю конкретну атаку, не застосовували програму-вимагач Termite». ***(Bill Toulas. Termite ransomware breaches linked to ClickFix CastleRAT attacks // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/termite-ransomware-breaches-linked-to-clickfix-castlerat-attacks/). 07.03.2026).***

***

«У 2025 році різко зросла кількість атак програм-вимагачів на світовий енергетичний сектор: було зафіксовано 187 підтверджених інцидентів, які викрили критичні вразливості в інфраструктурі, що забезпечує функціонування сучасного суспільства. Ці атаки, здійснені організованими угрупованнями, такими як RansomHub, Akira та Play, спричинили серйозні реальні наслідки, зокрема значні фінансові збитки та перебої у наданні таких життєво важливих послуг, як опалення. Цей сектор залишається особливо вразливим через застарілі операційні технології, посилену взаємодію між IT- та OT-системами, а також географічно розрізнені активи, що розширюють площину атаки… Ситуація з загрозами ще більше загострюється через діяльність посередників, які продають облікові дані для доступу до мереж, а також через зростання активності хактивістів, спрямованої проти операційних систем. Зловмисники часто використовують відомі вразливості швидше, ніж організації встигають їх усунути, створюючи стійкі прогалини в системі безпеки. У відповідь на це енергетичні компанії вживають таких заходів, як сегментація мереж, посилений моніторинг діяльності кіберзлочинців, прискорення процесу виправлення вразливостей та підвищення рівня готовності до інцидентів, проте масштаби та витонченість атак свідчать про постійний і зростаючий ризик для критичної інфраструктури в усьому світі…» ***(Ashish Khaitan. The Energy Sector Isn't Ready for Ransomware—and 2025 Proved It // The Cyber Express (https://thecyberexpress.com/energy-sector-ransomware-threats-2025/). 27.03.2026).***

***

«Рано вранці у вівторок порт Віго став жертвою атаки програм-вимагачів, яка серйозно порушила роботу цифрових систем управління вантажами та призвела до відключення веб-сайту адміністрації порту. Виявлена близько 5:45 ранку, ця атака змусила IT-команду порту негайно ізолювати уражені сервери, щоб локалізувати загрозу та запобігти подальшому зломленню. Хоча президент порту Карлос Ботана підтвердив, що фізична діяльність порту не була повністю зупинена, цифровий збій змусив персонал та користувачів порту покладатися на повільніші, ручні паперові методи планування, координації та митних процедур, наприклад, на прикордонному контрольно-пропускному пункті… Наразі триває криміналістичне розслідування, метою якого є з'ясування, яким чином зловмисники отримали доступ до системи та чи були викрадені якісь конфіденційні дані. Наразі немає прогнозів щодо термінів відновлення нормальної роботи цифрових систем, оскільки влада дотримується обережного підходу, залишаючи системи відключеними до завершення всебічних перевірок безпеки, щоб уникнути повторного зараження. Зрештою, цей інцидент підкреслює значну залежність сучасної морської логістики від цифрової інфраструктури та зростаючу вразливість глобальних ланцюгів постачання до руйнівних кіберзагроз…» ***(Samiksha Jain. Port of Vigo Hit by Ransomware Attack, Cargo Systems Disrupted // The Cyber Express (https://thecyberexpress.com/port-of-vigo-cyberattack-disrupts-systems/). 26.03.2026).***

***

Шпигунське програмне забезпечення

«Google виявив потужний набір експлойтів для iPhone під назвою Coruna, який, судячи з усього, потрапив з рук урядового замовника в руки злочинців. Вперше виявлений у лютому 2025 року під час спроби постачальника засобів спостереження встановити шпигунське програмне забезпечення від імені уряду, цей самий набір пізніше з'явився в широкій кампанії проти українських користувачів, яку проводила російська шпигунська група, а згодом був використаний хакером з Китаю, який мав фінансові мотиви — це свідчить про появу «вторинного» ринку, де експлойти державного рівня перепродаються та використовуються в інших цілях. Компанія з мобільної безпеки iVerify, яка провела реверс-інжиніринг цих інструментів, пов'язала Coruna зі США на основі схожості з раніше відомими можливостями і зазначила, що широке використання збільшує ймовірність витоку інформації. Wired також повідомила про збіги з компонентами, виявленими в «Операції Тріангуляція» 2023 року, в якій російська ФСБ звинуватила США. Походження та шлях витоку залишаються непідтвердженими…

Можливості Coruna є надзвичайно широкими: вона може зламати iPhone через простий візит на веб-сайт із пасткою (атака типу «водопій»), використовуючи п'ять різних ланцюжків експлойтів, побудованих на основі 23 вразливостей, що впливають на пристрої з iOS 13 до 17.2.1 (випущений у грудні 2023 року). Цей епізод підкреслює, як експлойти, розроблені урядом, можуть вийти за межі контролю і бути використані недержавними суб'єктами, що нагадує минулі витоки,

такі як EternalBlue від NSA, який пізніше був використаний у спалаху вірусу-вимагача WannaCry, та судове переслідування колишнього керівника L3Harris Trenchant, який продав кілька нульових днів брокеру, пов'язаному з Росією». ***(Zack Whittaker. A suite of government hacking tools targeting iPhones is now being used by cybercriminals // TechCrunch Media LLC. (https://techcrunch.com/2026/03/03/a-suite-of-government-hacking-tools-targeting-iphones-is-now-being-used-by-cybercriminals/). 03.03.2026).***

***

«Компанія Google виступає одним із провідних критиків поширення комерційної індустрії шпигунського програмного забезпечення: раніше вона підтримала позов проти NSO Group (розробника Pegasus) та опублікувала ґрунтовні звіти про те, як комерційні постачальники засобів стеження (CSV) дають урядам можливість відстежувати журналістів, активістів та політиків. Незважаючи на спротив з боку технологічних гігантів та агресивну позицію адміністрації Байдена, ситуація загострюється…

Згідно з останнім щорічним звітом Google Threat Intelligence Group (GTIG), у 2025 році на частку CSV та їхніх клієнтів припало більше випадків експлуатації вразливостей «нульового дня» (34,9 %, або 15 із загальних 90 випадків у 2025 році), ніж на частку традиційних шпигунських угруповань, що фінансуються державою (27,9 %, або 12 випадків) — це сталося вперше в історії. Ця зміна свідчить про зростаючу здатність CSV надавати небезпечні хакерські інструменти ширшому колу зловмисників, про що свідчать нещодавні судові справи щодо зловживання шпигунським програмним забезпеченням в Італії та Греції…

Проте державні суб'єкти залишаються дуже активними; угруповання, пов'язані з Китаєм, здійснили щонайменше 10 атак із використанням уразливостей «нульового дня», зосередившись на периферійних та мережевих пристроях, які важко контролювати. Google зазначає, що китайські оператори стають дедалі вправнішими у швидкій розробці, обміні та розповсюдженні експлойтів серед різних груп, скорочуючи проміжок між виявленням вразливості та масовим зловживанням, тоді як, навпаки, хакерам, спонсорованим Північною Кореєю, які були відповідальними за п’ять атак «нульового дня» у 2024 році, у 2025 році не було зафіксовано жодної». ***(Jeffrey Burt. Spyware Makers Topped Google’s List of Zero-Day Exploits for the First Time in 2025 // Techstrong Group Inc. (https://securityboulevard.com/2026/03/spyware-makers-in-2025-for-the-first-time-topped-googles-lists-of-zero-day-exploits/). 06.03.2026).***

***

Фішингові атаки

«…Зловмисники використовують домен верхнього рівня спеціального призначення «.arpa», а саме зворотну зону DNS «ip6.arpa» для IPv6, щоб проводити фішингові кампанії, які обходять традиційні перевірки репутації доменів та шлюзи безпеки електронної пошти. Зазвичай домен «.arpa»

зарезервований для інтернет-інфраструктури, що дозволяє системам зіставляти IP-адреси з іменами хостів. Однак зловмисники виявили, що, зарезервувавши власний простір IPv6-адрес за допомогою таких сервісів, як Hurricane Electric і Cloudflare, вони можуть отримати контроль над зворотною зоною DNS для цього діапазону і налаштувати шкідливі записи A замість очікуваних записів PTR…

Це дозволяє їм створювати фішингові URL-адреси з випадково згенерованими піддоменами під «ip6.arpa», які вони потім вбудовують як посилання на зображення у фішингові електронні листи, обіцяючи винагороди або повідомлення про облікові записи. Коли жертва натискає на посилання, вона перенаправляється через систему розподілу трафіку, яка перевіряє її дійсність, перш ніж перенаправити її на фішинговий сайт. Короткочасний характер цих посилань і відсутність стандартних даних про реєстрацію домену, таких як інформація WHOIS для домену «.arpa», ускладнюють виявлення цих атак засобами безпеки та їх аналіз дослідниками. Компанія Infoblox, яка спостерігала за цією кампанією, також зазначила, що зловмисники використовували інші техніки, такі як викрадення підвішених записів CNAME законних організацій, щоб ще більше зброїти надійні функції зворотного DNS і уникнути виявлення». ***(Lawrence Abrams. Hackers abuse .arpa DNS and ipv6 to evade phishing defenses // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/hackers-abuse-arpa-dns-and-ipv6-to-evade-phishing-defenses/). 08.03.2026).***

***

«Кіберзлочинці дедалі частіше поєднують психологію з технологіями, і сучасні фішингові атаки зазвичай відбуваються за простим, але надзвичайно ефективним сценарієм: початковий «гачок», повідомлення, покликане спонукати одержувача до негайних дій, а також дедалі ширше використання штучного інтелекту, щоб атака виглядала переконливою та законною. За даними Gallagher, ця тенденція стає все більш збитковою для австралійських підприємств: за повідомленнями, збитки від кіберзлочинів зростуть на 50% у 2024–2025 роках, що призведе до середніх збитків у розмірі 56 600 доларів на один інцидент для малих підприємств та близько 202 700 доларів для великих організацій. Людська поведінка є центральною проблемою: 37% випадків витоку даних в Австралії пов'язані з людською помилкою, фішинг залишається основною причиною зловмисних атак, а про кіберінцидент повідомляється кожні шість хвилин… Саме на фішинг припадає приблизно 60 % зареєстрованих інцидентів, причому зловмисники скоріше використовують реакцію людей на тиск, ніж покладаються виключно на технічні слабкі місця систем. Вони часто видають себе за авторитетні установи, такі як банки, державні органи чи керівників вищого рівня, і створюють відчуття терміновості за допомогою повідомлень, які спонукають співробітників клікати на посилання, вводити дані для входу, сканувати QR-коди або затверджувати платежі без ретельної перевірки. Як тільки людина реагує, атака може перерости в більш технічні методи, такі як підробка ідентичності відправника, оманливі посилання, клоновані сторінки входу, що в режимі реального часу перехоплюють облікові дані та коди аутентифікації, або схеми компрометації ділової електронної пошти, які, за словами Gallagher, у 2025

році були пов’язані з такими тактиками приблизно у трьох чвертях випадків. Штучний інтелект робить ці атаки ще переконливішими, дозволяючи створювати досконалі електронні листи, персоналізований контент на основі публічної інформації та навіть шахрайство з імітацією голосу, що передбачає підроблені повідомлення від керівництва…

Окрім фішингу, підприємства також стикаються з ризиками, пов’язаними з крадіжкою облікових даних, несанкціонованим доступом, використанням особистих пристроїв, неперевіреним програмним забезпеченням, слабкими засобами контролю доступу, застарілими системами та повторним використанням паролів, особливо в умовах гібридної роботи. Галлахер наголошує, що багатьох із цих атак все ще можна запобігти за допомогою простих, але суворих заходів безпеки, таких як перевірка незвичайних запитів, ретельна перевірка адрес відправників, підтвердження платіжних інструкцій через надійні канали, обмеження доступу до системи та використання багатофакторної автентифікації для зменшення збитків у разі витоку облікових даних. Компанія також наголошує, що навчання персоналу має бути постійним і реалістичним, а не одноразовим заходом, і що планування реагування на інциденти є надзвичайно важливим, оскільки перші 48 годин після порушення часто визначають, наскільки можна обмежити збитки. У цьому середовищі співробітники є не лише потенційними слабкими ланками, а й першою та найважливішою лінією оборони проти кіберінцидентів, спричинених фішингом». ***(Mav Rodriguez. Cyber scammers refine phishing tactics with AI – Gallagher // KM Business Information Australia Pty Ltd (https://www.insurancebusinessmag.com/au/news/breaking-news/cyber-scammers-refine-phishing-tactics-with-ai--gallagher-569339.aspx). 21.03.2026).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«…У відповідь на масштабну кібератаку ФБР заблокувало домени, пов’язані з іранською групою кібершпигунів «Handala», зокрема ті, що використовувалися під час нещодавнього інциденту, спрямованого на зривання роботи компанії Stryker, яка займається медичними технологіями. Група «Handala» взяла на себе відповідальність за цю атаку, заявивши, що знищила понад 200 000 систем і викрала 50 терабайтів даних, що, за повідомленнями, мало значний вплив на інноваційний центр Stryker в Ірландії. Після злому, під час якого було використано вразливість Microsoft Intune, Агентство з кібербезпеки та безпеки інфраструктури США (CISA) випустило попередження для організацій щодо посилення захисту кінцевих точок шляхом впровадження принципів мінімальних привілеїв, використання багатофакторної аутентифікації, стійкої до фішингу, та вимагання схвалення кількох адміністраторів для змін у системі. Звіти про загрози описують Handala як групу «хактивістів», яка діє з 2023 року і відома використанням руйнівних тактик, таких як шкідливе програмне забезпечення типу

«wiper» для знищення даних компаній — саме цю техніку було застосовано під час атаки на Stryker». ***(Emma Woollacott. Stryker hackers struck by FBI in domain seizure campaign // Future US, Inc. (https://www.itpro.com/security/cyber-attacks/stryker-hackers-struck-by-fbi-in-domain-seizure-campaign). 20.03.2026).***

***

«Білий дім координує свої дії з FBI (Федеральне бюро розслідувань), NSA (Агентство національної безпеки) та CISA (Агентство з кібербезпеки та безпеки інфраструктури) з метою розслідування очевидного, надзвичайно складного злому несекретної системи спостереження FBI, інциденту, який викликає серйозну стурбованість адміністрації Трампа з приводу кібербезпеки та контррозвідки. Вперше виявлений 17 лютого і нещодавно розкритий Конгресу, злом був спрямований на систему, що містила конфіденційну інформацію правоохоронних органів, включаючи особисті дані осіб, що перебувають під слідством FBI, та метадані з пристроїв спостереження «pen register and trap and trace». Цей тип даних, що розкриває об'єкти спостереження FBI, є надзвичайно цінним для іноземних розвідувальних служб та злочинних організацій. Згідно з повідомленням Конгресу, хакери продемонстрували високу майстерність, використовуючи інфраструктуру комерційного інтернет-провайдера для обходу систем безпеки FBI — тактику, яку історично застосовували групи, підтримувані китайською та російською державами…

Хоча FBI не приписало цю атаку конкретному суб'єкту і все ще оцінює повний масштаб збитків, цей інцидент має схожість з нещодавніми масштабними шпигунськими кампаніями. Зокрема, глобальний злом телекомунікаційної мережі в 2024 році, здійснений китайською хакерською групою «Salt Typhoon», в результаті якого були скомпрометовані дані про прослуховування та комунікації високопоставлених американських чиновників, досі вважається дуже активною загрозою, а чиновники попереджають, що хакери так і не були повністю вигнані з уражених мереж. Цей останній злом FBI є другою великою кібератакою, що викрила конфіденційні дані правоохоронних органів з моменту повернення президента Трампа на посаду, після попереднього компрометації онлайн-системи управління справами федеральної судової влади…» ***(John Sakellariadis, Maggie Miller, Dana Nickel. White House assisting probe of 'sophisticated' hack into FBI surveillance system // POLITICO LLC (https://www.politico.com/news/2026/03/06/fbi-hack-white-house-nsa-cisa-00817072). 06.03.2026).***

***

«…3 та 4 березня в рамках великої скоординованої операції, що охопила 14 країн, міжнародні правоохоронні органи під керівництвом Міністерства юстиції США та за підтримки Європолу успішно ліквідували LeakBase, один із найбільших у світі ринків кіберзлочинності. З понад 142 000 зареєстрованих членів, відкритий веб-форум слугував величезним глобальним центром для кіберзлочинців, де вони могли купувати, продавати та обмінюватися викраденими особистими даними, банківськими реквізитами та хакерськими інструментами, що значно сприяло поширенню крадіжок особистих даних та шахрайства…

Під час масштабної операції влада конфіскувала домени та базу даних платформи, замінивши сайт офіційними банерами про конфіскацію, одночасно виконуючи ордери на обшук, арешти та допити в різних країнах, включаючи США, Великобританію, Іспанію та Австралію. Захопивши величезний масив цифрових доказів, включаючи приватні повідомлення, облікові записи користувачів та журнали IP-адрес, слідчі не тільки зруйнували важливу частину глобальної інфраструктури кіберзлочинності, але й отримали цінну інформацію, яка буде використана для розшуку інших підозрюваних і жертв, підкресливши важливу роль транскордонного співробітництва в боротьбі з сучасними цифровими загрозами». ***(David Unyime Nkanta. Global Cybercrime Hub LeakBase Taken Down in Massive 14-Country Police Operation // IBTimes (https://www.ibtimes.co.uk/global-law-enforcement-dismantles-leakbase-1783454). 05.03.2026).***

***

«У рамках скоординованої міжнародної операції правоохоронні органи США, Канади та Німеччини успішно ліквідували інфраструктуру управління чотирма великими ботнетами «Інтернету речей» (IoT), відомими під назвами Aisuru, KimWolf, JackSkid та Mossad. Використовуючи вразливі пристрої, такі як веб-камери, цифрові відеореєстратори та корпоративні маршрутизатори, включаючи ті, що традиційно захищені брандмауерами, зловмисники заразили понад три мільйони пристроїв по всьому світу, щоб створити прибуткову платформу «кіберзлочинність як послуга». Ця підконтрольна мережа здавалася в оренду іншим злочинцям і використовувалася для запуску руйнівних атак типу «розподілена відмова в обслуговуванні» (DDoS), пікова потужність яких досягала рекордних 30 терабіт на секунду. Ці масштабні об’ємні атаки були спрямовані на глобальні сервери, критичну інфраструктуру та інформаційну мережу Міністерства оборони США і часто використовувалися як засіб примусу для вимагання викупу у цільових організацій…

Щоб нейтралізувати загрозу, такі відомства, як FBI, DCIS (Служба кримінальних розслідувань Міністерства оборони), німецьке BKA (Федеральне кримінальне управління) та RCMP (Королівська канадська кінна поліція), провели одночасні операції з вилучення серверів і доменів, а також затримання підозрюваних, тим самим хірургічно розірвавши канали зв’язку між зараженими кінцевими пристроями та їхніми операторами. Ця успішна операція була активно підтримана коаліцією приватних технологічних та безпекових компаній, зокрема Akamai, AWS та Cloudflare, що підкреслює важливу роль обміну інформацією про загрози між державним та приватним секторами у виявленні та знешкодженні масштабних кіберзлочинних мереж…» ***(Guru Baran. Authorities Disrupt IoT Botnet Infrastructure Behind Record-Breaking 30 Tbps DDoS Attacks // Cyber Security News (https://cybersecuritynews.com/authorities-disrupts-iot-botnet/). 20.03.2026).***

***

«Правоохоронні органи США, Німеччини та Канади провели скоординовану операцію з ліквідації інфраструктури чотирьох великих ботнетів — Aisuru, KimWolf, JackSkid та Mossad — які загалом заразили понад

3 мільйони пристроїв по всьому світу, переважно пристроїв Інтернету речей (IoT), таких як веб-камери, цифрові відеореєстратори та Wi-Fi-маршрутизатори. За даними Міністерства юстиції США, ці ботнети використовувалися для здійснення сотень тисяч розподілених атак типу «відмова в обслуговуванні» (DDoS) проти цілей по всьому світу, включаючи веб-сайти Міністерства оборони, причому в деяких випадках оператори вимагали від жертв виплати викупу… Крім того, ресурси ботнету KimWolf здавалися в оренду як мережа проксі-серверів для приватного використання, що дозволяло третім особам анонімізувати свою діяльність через заражені пристрої без відома їхніх власників. Німецька поліція ідентифікувала двох підозрюваних адміністраторів ботнету в Німеччині та Канаді, провівши обшуки, в результаті яких було вилучено значну кількість доказів та криптовалюту на суму в десятки тисяч доларів. В операції брали участь майже два десятки провідних технологічних компаній, зокрема Amazon Web Services, Google, PayPal та Nokia, а також команда Europol PowerOff, яка з 2017 року бореться з кіберзлочинцями, що спеціалізуються на DDoS-атаках». ***(Maria Tsvetkova. US, Germany, Canada disrupt botnets that infected millions of devices // Reuters (https://www.reuters.com/business/media-telecom/us-says-it-disrupted-botnets-that-infected-over-3-million-devices-worldwide-2026-03-20/). 20.03.2026).***

***

Технічні аспекти кібербезпеки

Виявлені вразливості технічних засобів та програмного забезпечення

«У нещодавньому партнерстві з Mozilla у сфері безпеки, Anthropic виявила 22 окремі вразливості у Firefox, 14 з яких класифіковані як «високосерйозні». Більшість помилок було виправлено у Firefox 148 (версія, випущена цього лютого), хоча деякі виправлення доведеться чекати на наступний реліз.

Команда Anthropic використовувала Claude Opus 4.6 протягом двох тижнів, починаючи з движка JavaScript, а потім розширюючи його до інших частин кодової бази. Згідно з публікацією, команда зосередилася на Firefox, оскільки «це одночасно складна кодова база та один із найкраще перевірених та безпечних проектів з відкритим кодом у світі».

Примітно, що Claude Opus набагато краще знаходив вразливості, ніж писав програмне забезпечення для їх використання. Зрештою, команда витратила 4000 доларів США у вигляді кредитів API, намагаючись створити експлойти для підтвердження концепції, але досягла успіху лише у двох випадках.

Тим не менш, це нагадування про те, наскільки потужними можуть бути інструменти штучного інтелекту для проектів з відкритим кодом — навіть якщо

вони приносять потік поганих мердж-реквестів поряд із корисними». ***(Russell Brandom. Anthropic's Claude found 22 vulnerabilities in Firefox over two weeks // TechCrunch Media LLC. (https://techcrunch.com/2026/03/06/anthropics-claude-found-22-vulnerabilities-in-firefox-over-two-weeks/). 06.03.2026).***

***

«Компанія Cisco розкрила 48 вразливостей, що впливають на її екосистему брандмауерів, яка включає Adaptive Security Appliance (ASA), Secure Firewall Threat Defense (FTD) та Secure Firewall Management Center (FMC), з виправленнями для всіх проблем. Серед них значну увагу привернули дві критичні вразливості в веб-інтерфейсі FMC, кожна з яких отримала максимальний бал серйозності 10/10. Перша, CVE-2026-20079, дозволяє зловмисникам обійти аутентифікацію та отримати root-доступ за допомогою спеціально підібраних HTTP-запитів, а друга, CVE-2026-20131, є недоліком незахищеної десеріалізації, який може дозволити віддалене виконання коду та підвищення привілеїв. Нідерландський центр кібербезпеки попередив, що публічні експлойти для підтвердження концепції та масштабне зловживання цими критичними помилками, ймовірно, не забаряться…

Експерти підкреслюють серйозну небезпеку, яку становлять ці вразливості, зазначаючи, що компрометація FMC — «нервового центру» мережевої безпеки — може дозволити зловмиснику змінити правила брандмауера та одночасно вимкнути засоби контролю безпеки на декількох пристроях. Ця інформація з'явилася на тлі загальної тенденції до збільшення кількості атак на периферійні мережеві пристрої, які вже принаймні два роки є улюбленим вектором початкового доступу для державних акторів. Ці пристрої часто є «сліпою зоною» для захисників, оскільки вони знаходяться поза традиційними стеками безпеки кінцевих точок і працюють на непрозорій прошивці. Як підкреслюють експерти з безпеки, організації намагаються не відставати, тому для них надзвичайно важливо використовувати такі інструменти, як Cisco Software Checker, і негайно виправляти уразливі системи, оскільки незахищений брандмауер — це як «відчинені двері з килимком «Ласкаво просимо»…» ***(Nate Nelson. Cisco Drops 48 New Firewall Vulnerabilities, 2 Critical // TechTarget, Inc. (https://www.darkreading.com/vulnerabilities-threats/cisco-48-firewall-vulnerabilities-2-critical). 05.03.2026).***

***

«Підозра на атаку типу «wiper» проти медико-технічної компанії Stryker привернула значну увагу до можливого зловживання сервісом Microsoft Intune після того, як компанія повідомила про інцидент, який призвів до збою в роботі тисяч мобільних пристроїв та інших систем і зробив недоступними електронні системи замовлення. У поданому до регуляторних органів документі компанія Stryker підтвердила, що атака зачепила її середовище Microsoft, тоді як пов'язана з Іраном зловмисна група Handala взяла на себе відповідальність, заявивши, що викрала 50 терабайтів даних та знищила інформацію з тисяч серверів і мобільних пристроїв. За даними дослідників з Halcyon, атака, ймовірно, була спрямована на телефони та робочі станції, пов'язані з рядком Intune base-64, з

використанням корисних навантажень, що містили команди віддаленого стирання для видалення даних з уражених пристроїв. Експерти з безпеки зазначають, що для такої атаки зловмисникам, ймовірно, знадобилося б отримати права адміністратора Intune або глобального адміністратора…

Аналітики зазначають, що це не свідчить про наявність вразливості в самій системі Intune, а скоріше відображає використання методів «living-off-the-land», коли легітимні адміністративні інструменти використовуються зловмисно для обходу систем захисту. Подібні атаки, пов'язані з платформами управління мобільними пристроями, траплялися й раніше, і експерти наголошують, що організації можуть знизити ризик за допомогою таких заходів, як багатофакторна автентифікація для доступу до систем управління мобільними пристроями та вимоги щодо затвердження кількома обліковими записами для виконання руйнівних дій, таких як дистанційне стирання даних. Хоча Microsoft ще не прокоментувала деталі, підрозділ 42 компанії Palo Alto Networks висловив більш загальні застереження щодо руйнівних атак з видаленням даних, під час яких зловмисники використовують вкрадені легітимні облікові дані, а компанія Stryker наразі розслідує інцидент разом із сторонніми фахівцями з криміналістики та Агентством з кібербезпеки та безпеки інфраструктури США». ***(David Jones. Stryker attack raises concerns about role of device management tool // TechTarget, Inc. (https://www.cybersecuritydive.com/news/stryker-attack-device-management-microsoft-iran/814816/). 16.03.2026).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Після 25 років роботи над перетворенням Palo Alto Networks на гіганта в галузі безпеки з капіталом 125 мільярдів доларів, співзасновник Нір Зук робить ще одну нестандартну ставку на Cylake: платформу безпеки на базі штучного інтелекту, апаратного забезпечення та локальних серверів для урядів, оборонних підрядників, суверенних держав та інших клієнтів, що підлягають суворому регулюванню і не можуть переміщувати конфіденційні дані в хмару. Завдяки підтримці у розмірі 45 мільйонів доларів від Greylock — венчурного фонду, який фінансував Palo Alto — Зук стверджує, що галузь «переорієнтувалася» на хмарні рішення, залишивши приблизно третину критично важливих клієнтів «на 20 років позаду». Він дотримується тієї ж нестандартної позиції, яку зайняв у 2005 році, запустивши хмарну безпеку, наполягаючи на тому, що у 2026 році існуватиме значний ринок для локальних рішень…

Ашім Чандна з Greylock називає це можливістю на суму понад 100 мільярдів доларів і рекламує Zuk як магніт для талантів; серед співзасновників — колишній керівник інженерного відділу Palo Alto Вілсон Сю та співзасновник SentinelOne Уді Шамір. Зук каже, що клієнти давно говорили йому, що хочуть отримати можливості Palo Alto без хмари — прогалину, яку компанія, що працює виключно в

хмарі, не могла заповнити, — що спонукало його до цього кроку після того, як він пішов з посади технічного директора, а Palo Alto придбала CyberArk за 25 мільярдів доларів. Ця ставка зроблена на тлі зростання загроз, пов'язаних з штучним інтелектом, і бурхливого розвитку кіберринку (у 2025 році буде залучено майже 14 мільярдів доларів, що на 47% більше), оскільки експерти попереджають, що геополітичні конфлікти, такі як війна з Іраном, сприятимуть збільшенню кількості атак. 54-річний Зук каже, що його мотивацією є не гроші, а створення того, чого не роблять інші: «Я знаю, що там є ринок». ***(Ben Bergman. The billionaire founder of Palo Alto Networks started a new cybersecurity company. Here's why many people are calling it 'crazy.' // Insider Inc. (https://www.businessinsider.com/founder-of-palo-alto-networks-started-a-new-cybersecurity-startup-2026-3). 05.03.2026).***

***

«У сучасних високодинамічних цифрових середовищах, що характеризуються хмарними платформами, віддаленою роботою та додатками SaaS, традиційні інструменти моніторингу кібербезпеки, засновані на правилах, стають все більш недостатніми. Ці старі системи часто ізольовані, не можуть виявляти невідомі загрози та генерують величезну кількість сповіщень, багато з яких є помилковими, що викликає серйозну «втому від сповіщень» у аналітиків Центру операцій з безпеки (SOC). Щоб боротися з ескалацією масштабів і швидкості кіберзагроз, організації звертаються до моніторингу кібербезпеки на основі штучного інтелекту…

Моніторинг на основі штучного інтелекту використовує машинне навчання та розширену аналітику для постійного спостереження та інтерпретації телеметрії в мережах, кінцевих точках, поведінці користувачів та хмарній інфраструктурі. Замість того, щоб покладатися на статичні сигнатури, ці системи вивчають, як виглядає «нормальна» активність, що дозволяє їм виявляти аномалії в поведінці, які можуть вказувати на складні атаки, такі як латеральний рух або витік даних. Штучний інтелект покращує безпеку, пов'язуючи, на перший погляд, не пов'язані між собою події в різних системах в єдину хронологію, значно зменшуючи кількість помилкових спрацьовувань та виявляючи інциденти набагато швидше, ніж при ручному аналізі…

Ця зміна не тільки покращує виявлення загроз, але й трансформує роботу SOC, дозволяючи командам масштабувати моніторинг у складних гібридних середовищах без перевантаження. Завдяки автоматизації аналізу даних штучний інтелект дозволяє аналітикам зосередитися на важливих завданнях, таких як стратегічне планування та реагування на інциденти. Крім того, технологія рухається в напрямку прогнозного моніторингу, де штучний інтелект аналізує історичні дані та тенденції поведінки, щоб передбачити ризики та проактивно посилити захист. Такі платформи, як Seceon, є прикладом цієї еволюції, пропонуючи уніфікований інтелектуальний моніторинг, що забезпечує всебічну видимість та автоматизовану пріоритезацію загроз, гарантуючи, що організації будуть готові захищатися від дедалі складнішого кіберпростору майбутнього». ***(Anamika Pandey. AI-Based Cybersecurity Monitoring // Techstrong Group Inc.***

(https://securityboulevard.com/2026/03/ai-based-cybersecurity-monitoring/). 09.03.2026).

***

«…Запуск компанією Anthropic функції Claude Code Security — яка сканує код на наявність вразливостей і пропонує способи їх усунення — спочатку спричинив падіння акцій традиційних постачальників рішень у сфері кібербезпеки, таких як Palo Alto Networks і CrowdStrike, але ціни швидко відновилися, оскільки аналітики дійшли висновку, що цей вплив буде скоріше поступовим, а не руйнівним. Цей інструмент, який позиціонується як альтернатива статичному аналізу на основі правил, що базується на логічному міркуванні, є частиною Claude Code — провідного помічника з кодування на базі штучного інтелекту від Anthropic — і наразі перебуває на стадії раннього попереднього перегляду…

Експерти стверджують, що це рішення доповнює, а не замінює комплексні програми з безпеки додатків: йому бракує функцій корпоративного управління, безперервного сканування, звітності, що відповідає вимогам нормативних документів, та регресійного тестування, які пропонують такі визнані гравці, як Veracode та Checkmarx… Аналітики Forrester та IDC прогнозують обмежений тиск на бюджети та відсутність значних скорочень робочих місць, причому керівники служб інформаційної безпеки (CISO) швидше перерозподілять персонал на завдання з вищою доданою вартістю, ніж скорочуватимуть штат. Відносно невеликий розмір ринку статичного аналізу в поєднанні з тим, що Claude Code Security зосереджується на підвищенні довіри до коду, згенерованого ШІ, а не на завоюванні ринку тестування безпеки, свідчить про те, що загроза для існуючих гравців була переоцінена. Загалом, існує консенсус щодо того, що крок Anthropic прискорює безпечну розробку, не змінюючи при цьому фундаментально загальний ландшафт кібербезпеки». ***(David Meyer. After the Panic, the Reality of Claude Code Security // Information Security Media Group, Corp. (https://www.govinfosecurity.com/after-panic-reality-claude-code-security-a-30936). 06.03.2026).***

***

«Незважаючи на те, що «діоди даних» — апаратні пристрої, які забезпечують суворо односпрямований потік даних — часто залишаються в тіні таких популярних програмних рішень, як брандмауери та штучний інтелект, вони стають незамінними для захисту критично важливих корпоративних середовищ. На відміну від брандмауерів, що базуються на налаштовуваних програмних правилах, «діоди даних» забезпечують справжню сегментацію мережі на фізичному та протокольному рівнях, дозволяючи даним виходити із захищеної мережі, водночас фізично запобігаючи проникненню до неї будь-яких маршрутизованих даних, шкідливого програмного забезпечення або побічних переміщень. Стрімке зростання попиту на цю технологію, ринок якої, за прогнозами, подвоїться до 2034 року, зумовлене трьома основними факторами. По-перше, швидка конвергенція інформаційних технологій (IT) та операційних

технологій (ОТ) у промислових середовищах значно розширила площину атаки на підприємства…

По-друге, зловмисники все частіше націлюються на ці вкрай вразливі кіберфізичні системи, про що свідчать руйнівні інциденти, такі як атака з використанням програм-вимагачів на компанію Jaguar Land Rover у 2025 році, яка призвела до збитків у розмірі 2,5 мільярда доларів. Нарешті, глобальна хвиля модернізації нормативно-правової бази — включаючи американські рамки від NIST, CISA та TSA, а також сувору директиву ЄС NIS2 — тепер вимагає надійної та підтверджуваної сегментації мережі. Зокрема, NIS2 переносить відповідальність за кібербезпеку безпосередньо на керівництво компанії, що наражає керівників на особисту відповідальність, публічні санкції та заборону на управління у разі грубої недбалості. Отже, хоча діоди даних не є панацеєю від усіх кіберзагроз, їхня здатність забезпечувати незмінну, апаратну ізоляцію робить їх незамінним інструментом для захисту критичної інфраструктури, забезпечення безперебійності роботи та захисту керівників від регуляторних та юридичних наслідків». ***(Mario Fernandez. Data Diodes Have Become Essential to Modern OT Cybersecurity // Information Security Media Group, Corp. (https://www.inforisktoday.com/blogs/data-diodes-have-become-essential-to-modern-ot-cybersecurity-p-4063). 10.03.2026).***

***