**Нестеренко Олександр Васильович,** кандидат технічних наук, доцент, дійсний член Міжнародної академії інформатики, Заслужений працівник сфери послуг України, професор кафедри комп’ютерних наук, інформаційних технологій та системного аналізу, Національна академія управління

**КІБЕРБЕЗПЕКА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ БІЗНЕСУ**

Нещодавні прогнози компанії IDC (*FutureScape: Worldwide IT Industry 2018 Predictions, 31 осt 2017*) визначають десятку ключових подій у світі технологій, які вплинуть на кожну можливість бізнесу зростати і конкурувати протягом наступних років (принаймні до 2020) [1]. Прогнози базуються на найбільшому ІТ-зрушенні нашого часу - цифровому перетворенні (*Digital Transformation,* DX) сучасних підприємств і застосуванні цього явища для примноження інновацій в цифровій економіці. Поняття цифрової трансформації основане на тенденції швидкого переходу бізнесу у хмарні технології фази 2.0, де визнається кращою для екосистеми кожної компанії публічна хмара як єдина платформа, що буде підтримувати прискорення цифрових трансформацій промисловості («якщо ви не в хмарі, ви ізольовані від інновацій») на базі таких технологій, як штучний інтелект (*Artificial intelligence*, AI) і машинне навчання (Machine learning), Інтернет речей (*Internet of Things*, IoT), розширена (доповнена) реальність (*Augmented reality*, AR), віртуальна реальність (*Virtual reality*, VR) і блокчейн (*blockchain*).

За вказаними прогнозами у найближчі роки більше половини всіх підприємств у світі повністю сформулюють організаційні стратегії цифрового перетворення як нового ядра для тих, хто прагне конкурувати в цифровій економіці, і будуть в процесі реалізації цих стратегій. Завдяки цьому принаймні 50% світового ВВП буде «оцифрованим». 40% ініціатив цифрових трансформацій будуть використовувати послуги AI, зокрема нових промислових роботів. За рахунок диверсифікації людино-машинного (*human-digital*) інтерфейсу більш чверті працівників будуть використовувати AR, майже 50% нових мобільних додатків використовуватимуть голос як основний інтерфейс і біометричні датчики для ідентифікації і персоналізації.

Значна частина великих світових компаній (Global 2000), серед яких банки, підприємства роздрібні торговці, організації охорони здоров’я, будуть використовувати *blockchain*-послуги як основу для забезпечення цифрової довіри у глобальному масштабі. А майже 90% великих підприємств будуть отримувати дохід від послуг, що будуть надаватись на основі накопичених даних (*data-as-a-service*), таких як продаж необроблених даних, метрик, розуміння (знання) та рекомендацій, отриманих на основі технологій бізнес-аналітики (*Business Intelligence*, BI) та інтелектуального аналізу даних (*Data mining*, *Big Data*).

Оці перспективи значною мірою перегукуються з іншим трендом - настанням четвертої промислової революції (Індустрія 4.0), яка, за словами доктора Клауса Шваба, фундатора Давоського економічного форуму і автора цієї парадигми, «…йде на нас, як цунамі. Швидкість цієї революції є такою значною, що політичному суспільству важко або навіть неможливо встигати з необхідними нормативними і законодавчими рамками. Четверта революція характеризується роботизацією і кібер-соціалізацією, злиттям технологій і стиранням граней між фізичними, цифровими і біологічними сферами. Ця революція кардинально змінить те, як ми живемо, працюємо, відносимося один до одного. Подібного масштабу і складності змін людству ще ніколи не доводилося відчувати».

Багато що з обговорення питань про взаємовідношення між технологією і виробництвом – це розгляд проблем зіткнення зі штучним інтелектом. Поки що AI має відношення до аналізу великих даних, ідентифікації знань, безпеки даних, виявлення фальсифікацій у фінансовій діяльності, тощо. Але впровадження роботів у виробництві – це найочевидніший приклад появи нових небезпек: скорочення робочих місць, зростання соціальної напруги, відставання значної частини людства від розуміння технологічних новацій та їх опанування.

Чи варто боятися експансії «братів за розумом»? Час покаже, але сьогодні в умовах конвергенції комп’ютинга і комунікацій, коли «все буде з’єднано з усім» цифровими технологіями, необхідно звертати підсилену увагу на усе більшу небезпеку, яка надходить саме від людей, що промишляють у кібер-сфері [2].

Підвищення рівня використання у суспільстві нових технологій створює нові «робочі місця» для людей, що безпосередньо застосовують технологічні новації для шахрайства, зловживань і злочинності, і не лише щодо пересічних громадян, а й у напрямку здійснювання атак на критичні інфраструктури суспільства, на урядові і політичні інституції. Численні факти результативних кібератак за останні місяці (не роки!), є цьому яскравим підтвердженням.

Значною мірою кіберзагрози торкнуться також підприємств малого і середнього бізнесу (СМБ), які не в змозі вкладати чималі кошти у забезпечення кібербезпеки власної інформаційної інфраструктури, підтримувати інтеграцію кібербезпеки в корпоративне управління, керування ризиками та забезпечення відповідності (*Governance, Risk Management and Compliance*). Цифрова світова екосистема, і ЄС зокрема, надає можливості засвідчувати контракти та надавати послуги в режимі он-лайн, використовуючи електронний цифровий підпис, електронну печатку, BankID, Mobile ID тощо. Ці сервіси відкриють й новий вимір перед зловмисниками, що нишпорять мережами у пошуках прогалин у захисті важливих даних. В Україні також прийнято закон «Про електронні довірчі послуги», направлений на залучення до європейської моделі.

Кібербезпека зосереджується на особливих формах складних атак та охоплює їх технічний і соціальний аспекти, Тому підприємствам варто серйозно замислюватися над тим, що технології вже беруть їх у полон. Водночас державі необхідно орієнтуватися на програми та ініціативи ЄС у сфері кібербезпеки, що базуються на серії документів про впровадження європейської кібербезпеки, які залучають практичні настанови, що відповідають європейським вимогам і передовому досвіду згідно з діючими законами, стандартами та іншими настановами. З іншого боку, підприємства повинні орієнтуватися на нововведення, що передбачають глобальну досяжність публічних хмар, які, зокрема, пропонуються партнерствами світових брендів, як то SAP і Google, SAP і Microsoft, щоб повністю реалізувати вигоди від застосування *cloud*-платформ і пом’якшувати ризики несанкціонованого доступу до їх ресурсів [3,4]. Це, мабуть, єдине, що має бадьорити у наш час творчих, інноваційних підприємців.

1. IDC FutureScape Web conference // Електронний ресурс: https://www.idc.com/getdoc. jsp?containerId=IDC\_P37531
2. Нестеренко О.В. Безпека економіки знань // Formation of Knowledge Economy as the Basis for Information Society [Collected works] / by M.M. Yermoshenko, S.V. Onyshko, A.A. Oleshko, I.Y. Stuler etc. – Athens-Kyiv: International Academy of Information Science, 2017. – 15-18 pp.
3. Flexibility, Scalability, Speed: SAP and Google Announce Strategic Partnership // Електронний ресурс: https://news.sap.com/flexibility-scalability-speed-sap-google-strategic-partnership/
4. Microsoft and SAP join forces to give customers a trusted path to digital transformation in the cloud // Електронний ресурс: https://news.microsoft.com/2017/11/27/microsoft-and-sap-join-forces-to-give-customers-a-trusted-path-to-digital-transformation-in-the-cloud/