нанотехнології, 3D-друк, BlockChain, Digital marketing, безпілотні засоби пересування та інші. За згадуванням у ЗМІ на першому і другому місці в рейтингу глобальних цифрових трендів знаходяться мобільний зв'язок і штучний інтелект. В останні роки штучний інтелект зробив приголомшливий стрибок у розвитку завдяки стрімкому зростанню комп'ютерних можливостей та доступності величезних обсягів інформації: від програмного забезпечення для створення нових ліків – до алгоритмів, здатних передбачити наші культурні уподобання [3, с. 16]. Високе місце електронної комерції в зазначеному рейтингу є наслідком підвищеної інвестиційної активності і великої кількості угод у цьому сегменті [4].

Отже, сьогодні діджиталізація виступає загальносвітовою тенденцією, своєрідним трендом економічного розвитку та спричиняє глибинні зрушення у міжнародних економічних відносинах. Звідси виникає нагальна потреба в модернізації галузей виробництва, розбудові цифрової інфраструктури, формуванні технологічної платформи для забезпечення інтеграції країни у єдиний цифровий простір. Для України саме діджиталізація має стати пріоритетним напрямом державної політики, реалізація якого дозволить: створити високотехнологічні виробництва, провести технологічну модернізацію промисловості, забезпечити стабільне економічне зростання, стимулювати інноваційне підприємництво та підвищити конкурентоспроможність національної економіки на світовому ринку.

Література:

1. Череп А., Воронкова В., Нікітенко В., Ажажа М., Муц Л. Цифрова культура (фінтех) як чинник підвищення ефективності економіки та бізнесу в умовах технологічної революції 4.0. *Eastern european conference of management and economics (Eecme 2019):* матеріали міжнародної науково-практичної конференції, м. Любляна, 24 травня 2019 р., Словенія, 2019. С. 93-97.

2. Digital Economy and Society Index Methodological note. URL: https://ec.europa.eu/information_society/newsroom/image/document/2018-20/desi-2018 methodology_E886EDCA-B32A-AEFB-07F5911DE975477B_52297.pdf. (дата звернення (20.01.2021).

3. Шваб Клаус. Четверта промислова революція, Формуючи четверту промислову революцію. Харків: Клуб сімейного дозвілля, 2019. 426 с.

4. Monitorynh hlobalnykh trendiv tsyfrovizatsii. URL: https://www.company.rt.ru/upload/iblock/d79/2018.pdf (дата звернення 22.01.2021).

ТЕНДЕНЦІЇ КІБЕРСТРАХУВАННЯ

Д. В. КОНДРАТЕНКО, канд. екон. наук, доц.,
доц. кафедри фінансів і кредиту
Харківський національний університет будівництва та архітектури, м. Харків

Кожна підприємницька структура, незалежно від розміру, в значній мірі залежить від технологій, комунікацій і взаємодії. У нинішньому цифровому ринку кібератаки становлять значну загрозу для бізнесу, що призвело до того, що кібербезпека неухильно піднімається на порядку денному пріоритетів

вищого керівництва. Очікується, що темпи впровадження технології залишаються невизначеними та можуть прискоритись у деяких галузях. Впровадження великих даних та електронної комерції залишається пріоритетом для менеджменту, також спостерігається значний інтерес до шифрування та штучному інтелекту. Автоматизація в тандемі з рецесією COVID-19 створює сценарій «подвійного збою» для бізнесу.

Інформаційні технології, що стрімко проникають в економічні й соціальні процеси, зумовлюють необхідність інноваційних змін на ринку страхування України і розвитку такого сегмента, як кіберстрахування, який забезпечує необхідний страховий захист і відшкодування суми збитку в розмірі, необхідному для компенсації витрат, пов'язаних із втратою баз даних страхувальників та їх подальшим відновленням у разі виникнення масштабних кібератак [1].

Індустрія кіберстрахування стрімко розвивається, стають більш тісними відносини між страховиками і страхувальниками. У міру розвитку ринку кіберстрахування галузі всіх типів усвідомлюють потребу в кібербезпеці, але страхувальників і страховиків турбують такі тенденції:

1. Постачальники керованих IT-послуг (MSP) піддаються все більш частим атакам, а це означає, що сотні тисяч підприємств, які покладаються на них, спостерігають збільшення часу простою системи, в деяких випадках з втратою конфіденційних даних і репутаційних збитків, пов'язаних з ними. Хакери також використовують MSP як плацдарм для за пуску атак програм-вимагачів проти підприємств, які обслуговують ці постачальники [2].

2. Зросла тяжкість фінансових наслідків використання програм-вимагачів. Викупи зросли з п'ятизначних цінників на мільйони, включаючи 10 мільйонів доларів, які виплатив Garmin. Нещодавній звіт Hiscox показує застраховані кіберзбитки в розмірі 1,8 мільярда доларів у 2019 році, що зростають на 50% за рік [3].

3. Уповільнення попиту на кіберстрахування. Незважаючи на безліч кібератак, компанії купують менше кіберстрахування або взагалі не купують, оскільки економічне напруження від Covid-19 змусило деяких дивитися на кіберстрахування як на розкіш. І хоча більша кількість атак може стимулювати попит, вони також створюють проблему з постачанням, роблячи страховиків обережнішими у забезпеченні покриття. Крім цього, відсутність історичних даних про втрати (внаслідок короткої історії сектору) додає ще один рівень непередбачуваності для страховиків.

4. Зростання ємності ринку кіберстрахування. Ринок кіберстрахування в даний час оцінюється на суму близько $ 2 млрд премій в усьому світі, причому американський бізнес складає приблизно 90%. Сьогодні менше 10% компаній купують кіберстрахування [4]. Клієнти ще не розуміють ризики, з якими стикаються їх організації. Головними перешкодами на шляху до продажу кіберстраховки залишається, як і в минулі роки: не розуміння страхового покриття і вартості страховки. Для страхувальників життєво важливо мати більш чітке уявлення про те, які кібератаки покриваються, а які ні. Крім того, індустрія кіберстрахування повинна продовжувати вдосконалюватися в поясненні ризиків, що призведе до більшої прозорості та зростанню ринку.

5. Кібербезпека і страхування розвиватимуть тісні партнерські відносини. Це створить цікаві можливості для обох сторін. Наприклад, якщо у компанії є хороші заходи кібербезпеки, вона, ймовірно, отримає страхові бонуси, аналогічні отриманню в автострахуванні (завдяки телематики водія). Кіберстійкість вимагає як кібербезпеки, так і кіберстрахування.

6. Освіта в області кіберстрахування буде продовжувати рости. Страховики повинні пропонувати доступні, легко засвоювані страхові продукти для тих, хто не так добре знайомий з кібербезпекою. Індустрії кіберстрахування належить виконати велику роботу, щоб внести ясність. Це включає використання простих термінів для позначення кожного типу конфіденційної інформації, будь то корпоративні файли, медичні записи або особисті дані. І фахівцям з безпеки, і страховикам необхідно розгорнути чітку систему обміну повідомленнями, яка точно показує, які ризики можуть бути у бізнесу і як вони можуть захистити себе. Крім того, всі зацікавлені сторони повинні спиратися на єдине джерело істини, вибудовуючи політику з урахуванням того, що технології і всебічна оцінка забезпечать максимальний захист. Страховики кіберстрахування, які будуть попереду всіх, – це ті, які пропонують корисні інструменти, розмовляють мовою непрофесіонала і співпрацюють з сектором кібербезпеки, даючи страхувальникам можливість більше дізнатися про кіберпростір, оскільки він відноситься до їх конкретного бізнес-сектору.

Ринок кіберстрахування характеризується постійно мінливим середовищем. Завтрашні кібератаки можуть виглядати не так, як сьогоднішні. Щоб страховики реагували на цю унікальну загрозу, їм доведеться змінюватися з часом, доки галузеві знання не стануть достатніми для того, щоб поводитися з кібер як зрілі класи бізнесу.

Література:

1. Ільчук В. П., Парубець О. М., Сугоняко Д. О. Інноваційні підходи до розвитку ринку кіберстрахування в Україні. *Ефективна економіка*, 2018, № 5. URL: http://www.economy.nayka.com.ua/pdf/5_2018/5.pdf (дата звернення: 17.01.2021).

2. Що найбільше лякає страховиків кібер-ризиків. URL: https://forinsurer.com/files/file00693.pdf (дата звернення: 17.01.2021).

3. Tom Johansmeyer. Cybersecurity Insurance Has a Big Problem. Harvard Business Publishing. 2021. URL: https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem (дата звернення: 17.01.2021).

3. Временко Л. В. Визначення та види кібернетичного ризику. *Ринок фінансових послуг: погляд у майбутнє: монографія,* ФОП Ямчинський О.В., 2019. С. 296-314.