MANAGEMENT AND MEASUREMENT OF DIGITAL RISK IN BUSINESS

УПРАВЛІННЯ ТА ВИМІРЮВАННЯ ЦИФРОВОГО РИЗИКУ У БІЗНЕСІ

Suntsova O.O.[1]

DOI: https://doi.org/10.30525/978-9934-26-351-4-9

Вступ. Існує багато дискусій щодо природи та поширеності цифрових загроз безпеці: поширеність та типи вразливостей; частота, серйозність та вплив цифрових технологій інциденти безпеки та ефективність різних практик безпеки. Ці суперечки відбуваються через низку концептуальних, методологічних та гносеологічних питань, з якими стикалися вимірювання явищ, пов'язаних з цифровою безпекою.

Цифрові опитування, як інструмент вимірювання цифрового ризику, представляють власні унікальні виклики, особливо коли вони розгорнуті для цілі вимірювання елементів, пов'язаних із цифровим ризиком безпеки. Існують поточні дебати, пов'язані з вимірювання цифрової безпеки, ризику цифрової безпеки та управління нею. Наведемо приклади загальних методологічних підводних каменів, які мали минули вимірювання. Роблячи це, узагальнимо проблеми, що стосуються вимірювання безпеки в цифровій економіці. Єдиним документом [1], який намагався визначити та описати основні загрози безпеки в цифровій економіці це ОЕСР Проект 2017 року [2], який прагнув вирішити та подолати основні цифрові загрози в бізнесі, досягти своєї мети щодо вдосконалення практики вимірювання та управління цифровими ризиками безпеки в бізнесі.

Концептуальні питання вимірювання цифрової безпеки

На концептуальному рівні термін «безпека» не часто є чітко визначеним у галузі цифрових технологій безпеки. Дискусії щодо безпеки іноді впадають у дихотомічні, двійкові концепції де щось вважається «захищеним» або «небезпечним» (DSTI / CDEP / GD (2018) [3; 4; 5]).

[1] Doctor of Economic Sciences, Full Professor,
State Tax University

Бракує значної частини нюансів, необхідних для формування такого розуміння в свою чергу, призвело б до ефективного управління ризиками, що призвело б до більшої безпеки.

Більш тонке розуміння розглядало б такі питання, як відносна безпека чогось (сутність або її діяльність), десь (контекст) проти якогось супротивника (включаючи навмисне та ненавмисне, а також людське та нелюдське – наприклад, природне – джерел загроз), серед інших питань. З'ясування цієї концептуальної двозначності – це перший крок до більш точного та корисного вимірювання цифрової безпеки, а, отже, і ефективне управління пов'язаними цифровими ризиками. Область управління цифровими ризиками безпеки також постійно змінюється. Багато що ще невідомо через динамічні явища, що досліджуються, і через обмеження здатність спостерігати та розуміти явища, що досліджуються, серед інших причин. Навіть коли дані збираються та аналізуються, тим самим даючи більше розуміння нинішнього стану справ, це розуміння може швидко знову застаріти завдяки до динамічного характеру явищ. Там, де є докази, часто виникають розбіжності щодо «правильного» способу формувати висновків та критеріїв, за якими можна робити висновки або оцінювати результати [6]. Наприклад, загальним твердженням є те, що інциденти цифрової безпеки зростають за частотою та тяжкістю.

Однак в 2015 році американський дослідник Дж. Жардін та інші [7] стверджували, що більш точна картина безпеки цифрового середовища вимагає відповідних статистичних даних – у тому числі мобільної вразливості, зловмисні веб-домену, експлойти нульового дня та інші веб-атаки – виражати як частку зростаючого розміру Інтернету («нормалізований»). Якщо висловитись таким чином, картина цифрових інцидентів, що виникає, складається з числа випадків, які можуть зростати повільніше, ніж кількість людей та пристроїв, що користуються Інтернетом [8]. Ще одним поширеним твердженням є те, що порушення та атаки на дані збільшуються за масштабами, частотою та тяжкістю. Однак команда дослідників на чолі з Дж. Едвардсом в 2014-му році проаналізували базу даних про зареєстровані порушення даних та їх результати. Вони виявили, що «…ні розмір, ні частота порушення даних не зросли за останнє десятиліття…» [9]. Автори стверджують, що гучні цифрові інциденти, які привертали увагу

останніх років можна пояснити важким розподілом статистики, що лежать в основі набору даних. Пізніше, в 2016-му, ці висновки підтримав А. Романоскі, який виявив, що «…вартість типового кіберінциденту [у нашій вибірці] менша ніж 200 000 доларів США (приблизно стільки ж, скільки річний бюджет фірми на IT-безпеку), і це становить лише 0,4% від їх передбачуваних річних доходів…» [10].

Такі висновки демонструють нюанси та складність оцінки справжньої тяжкості порушень даних, хоча це справедливо одна підгрупа всіх випадків цифрової безпеки. Ускладнення здатності робити висновки та приймати рішення на основі емпіричного дослідження – це обмеження використання минулого як орієнтира на майбутні результати. Це обмеження має особливу проблему в цифровому домені, враховуючи серйозність та вплив цифрових інцидентів в сукупності, які часто слідують розподілам з важкими хвостами, і саме цю особливість помітили та описали в своїх дослідженнях Талеб та Кірілло у 2015-му [11]. Поки один може розглянути твердження Джардін про те, що в середньому (тобто, більшість днів) утримується кіберпростір «Безпечніше», або висновки Едвардса та ін. та Романоскі щодо стабільної частоти та тяжкості минулих порушень даних, при важко розповсюдженому розподілі, можуть бути найгірші дні в майбутньому набагато гірше, ніж будь-коли раніше (робота Гартнер [12]).

Усі ці суперечки вказують на невід'ємні труднощі в ефективному вимірюванні, а потім у тлумаченні результатів аналізу галузі управління цифровими ризиками безпеки [13]. Є кілька простих відповідей, і там, де вони є, немає гарантії, що відповіді будуть залишатись «справжніми» в майбутньому. Щоб правильно виміряти та оцінити докази у цій галузі повинні зберігати відкритість і постійно переглядати припущення, що лежать в основі висновків.

Методологічні завдання для цифрових опитувань безпеки

Поєднання цих питань являє собою низку методологічних питань, пов'язаних спеціально з опитуваннями, які спрямовані на збір даних про елементи, пов'язані з цифровим ризиком безпеки та його управлінням. Опитування є одним із найпоширеніших джерел емпіричних даних використовується для формування політики. Вони базуються на питаннях, заданих людям (тобто, на зразку населення). Їх мета полягає в тому, щоб дізнатись про певні ознаки сукупності на основі вибірки

цієї сукупності шляхом статистичного висновку (OECD, 2012) [14]. Щороку публікуються нові звіти – на основі опитувань – із показниками, що охоплюють конкретні аспекти цифрової безпеки. Однак остаточні звіти для цих опитувань зазвичай не намагаються надати достатньо детальної інформації щодо своїх джерел даних або методології, мають обмежений обсяг і в географічному різноманітті, і може розроблятись або фінансуватися суб'єктами, що мають певні корисні інтереси. Хоча така статистика може бути корисною для певних вузьких цілей, вона часто не є такою достатньо надійною для використання розвитку громадської політики.

Є такі дві загальні слабкі сторони опитувань: проведення опитування може коштувати дорого і бути занадто трудомістким; а погано розроблені опитування, як правило, підтверджують існуючі уявлення та не дають можливості отримати нових уявлень (OECD, 2011) [15]. Окрім цього, при опитуванні керівництва має специфічний минулий ризик цифрової безпеки, коли як правило, результати страждають від специфічних недоліків у таких сферах: вибірки; забезпечення достатніх технічних знань респондентів; точне виявлення аварій та звітність; точне вимірювання / оцінка впливу; та відсутність загальних визначень, термінології та таксономії. Ці обмеження підривають корисність і порівнянність та надійність результатів опитування.

Вибірка та відбір

Для того, щоб зробити висновок за результатами опитування правильним, вибірка опитування повинна бути чітко визначеною указаною цільовою сукупністю, а потім надайте репрезентативну вибірку цієї сукупності [16]. В випадку, якщо цільовою сукупністю є загальна сукупність підприємств, але вибірка опитування не є репрезентативною для цієї сукупності, для компенсації можуть застосовуватися різні ваги для вибірки недоліків. Відбір респондентів для вибірки опитування повинен бути рандомізованим, щоб зменшити потенціал для реакції або упередженості вибору. Крім того, може бути присутнє упередження у відповіді, що впливає на результати, враховуючи те, що особи чи компанії, які не відповіли на опитування може суттєво відрізнятися з точки зору основних переконань від тих, хто закінчив опитування. Зразок кадру може бути упередженим з багатьох інших причин. Це могло б бути пов'язані із впливом зовнішніх сил, таких як висвітлення у ЗМІ, або

тому, що респонденти винагороджується грошовою сумою. Наявність великих вибіркових кадрів, з яких можна взяти репрезентативну вибірку з населення, таким чином вирішення питань відбору проб, може бути складним та затратним. Хоча національний статистичні управління, як правило, мають доступ до великих баз даних для випадкового відбору їх вибірки, багато приватних консультантів або постачальників послуг безпеки (які беруть на себе більшість із поточних загальнодоступні цифрові опитування ризиків безпеки) не мають доступу до таких великих зразків [17]. Це обмежує репрезентативність цих результатів опитування підгрупами загального бізнесу населення і має тенденцію до збільшення рівня помилок, що, в свою чергу, знижує здатність малювати точні та відповідні висновки за результатами опитування. Необхідні технічні знання Важливо забезпечити, щоб відповідна особа відповіла на інструмент опитування всередині цільове підприємство [18]. Хто вважається «відповідним», багато в чому визначається суб'єктом питання, що охоплюється інструментом обстеження, а також розмір та структура підприємства розглянутий [19].

Визначення відповідного респондента для цифрового опитування ризиків безпеки може початися з орієнтації на людей з певною роллю та / або рівнем стажу на підприємстві. Для вимірювання цифрової безпеки буде оцінюватись як економічний та соціальний виклик, респондент повинен мати розуміння ділової діяльності та економічних та соціальних ризиків, якими є саме його бізнес [20]. Ця особа також повинна розуміти технічні аспекти цифрової безпеки та розуміти та ідеально володіти знаннями про: людські ресурси та навчання; корпоративне управління; ризик управління; конфігурація мережі та комп'ютера; серед інших [21]. Ця людина повинна бути в достатньо старшій ролі, щоб мати змогу мати видимість на всьому підприємстві. Залежно від за розміром бізнесу ця особа може мати одне з таких посад: головний директор з ризиків; начальник / менеджер з управління ризиками; внутрішній ревізор; бухгалтер; комітет з управління ризиками (та аудитом); головний виконавчий директор; головний операційний директор; або головний фінансовий директор / менеджер.

Респондентом в ідеалі не був би той, хто відповідає лише за інформаційних комунікаційних технологій (ІКТ), якими ця людина, швидше за все, не володітиме достатніми знаннями про підприємницьку діяль-

ність та інші важливі для управління ризиками на підприємстві елементами. На практиці це визначення поняття «доречно» має певні обмеження. Деякі підприємства можуть не мати людини в одній із цих ролей для нормального опитування. Це, швидше за все, має місце у багатьох ФОПах і малих підприємствах, а також на деяких середніх підприємствах з низькою цифровою інтенсивністю. Великі фірми без існуючої культури та механізму управління ризиками також можуть не мати осіб з відповідним профілем для розгляду цифрової безпеки як бізнес-ризику. В таких випадках, найбільш відповідним респондентом, швидше за все, буде власник підприємства або хтось інший на керівній посаді.

Цифрове управління ризиками безпеки може включати концепції, яких певні респонденти можуть не розуміти. Такі поняття можуть бути технічними (наприклад, відмова в обслуговуванні, шкідливе програмне забезпечення) або пов'язаними з ризиками (наприклад, оцінка ризику, передача ризику). Крім того, термінологія, пов'язана з такими поняттями можуть бути не однорідними між секторами, країнами та культурами. Якщо відповідач недостатньо обізнаний у технічних концепціях або якщо опитування сформульовано таким чином, що загальний спеціаліст може не зрозуміти, постраждає надійність відповідей на опитування. Тому необхідно досягти рівноваги між респондентом, який має достатній стаж розуміти вразливість декількох доменів на підприємстві та мати достатні знання базових технічні концепцій, щоб мати змогу точно реагувати на інструмент опитування.

Один із способів потенційно пом'якшити цей ризик полягає у формулюванні інструменту опитування таким чином, щоб загальний спеціаліст міг зрозуміти питання, що означає уникнення надто технічної термінології або спеціалізованих знань домену.

Виявлення цифрових інцидентів та повідомлення про них

Існує низка методологічних питань, що стосуються самої фіксації повідомлень про події та інциденти цифрової безпеки. Звітність про їх вплив на діяльність підприємства є проблематичною в контексті якості проведених опитувань, деякі з яких були визначені в попередніх роботах ОЕСР (директива OECD, 2015b) [22]. Респонденти, швидше за все, занижують істину кількість інцидентів цифрової безпеки, які вони зазнають протягом певного періоду часу. Наприклад, протягом

одного року бізнес може зазнати певної кількості інцидентів цифрової безпеки, але банально не зрозуміти цього і не помітити, і тому не зафіксувати такі цифрові інциденти.

З величезної кількості всесвіту інцидентів бізнес може виявити не всі цифрові інциденти. Ці невиявлені випадки цифрової безпеки не враховуватимуться, коли респонденти відповідають на запитання пов'язані з минулими інцидентами. Тому потрібно урахувати при постановці питань те, аби якщо респонденти, які не вважають, що їх відповіді залишатимуться конфіденційними, то вони не можуть розкривати справжній обсяг або всі виявлені випадки (наприклад, через проблеми з репутацією). Точно невідомо, яка частка цифрових інцидентів залишається невиявленою. Деякі дослідження мають цитовані підрахунки, які свідчать про те, що ця цифра коливається від 60% до 89% випадків цифрової безпеки, які не повідомляються (таке стверджують у роботах команда науковців під керуванням професора Койлі) [23]. Якщо ці оцінки будуть прийняті, це означатиме, що значна частка всього всесвіту інцидентів є частиною «невідомого». Однак, на гносеологічному рівні, це може означати, що просто неможливо остаточно визначити частку випадків, які не виявляються, через природу явища та можливі методи дослідження [24].

Наслідки цих методологічних питань підтверджуються на прикладах, наведених нижче, які базуються на результатах попередніх опитувань. Спочатку розглянемо результати проведених досліджень ІКТ ОЕСР [25].

На рисунку 1 наведено порівняльну статистику міждержавних зв’язків щодо випадків порушення цифрової безпеки, виявлених підприємствами. Є сукупна різниця між країнами, у зв’язку з чим виникає питання щодо того, чи є частка підприємств, які зазнають цифрових атак та інцидентів, насправді вища в деяких країнах за інші, чи це просто пояснюється тим, що можливості виявлення цифрових інцидентів та атак вищі на підприємствах одних країнах в порівнянні з іншими.

Якщо більш докладно, можливо, виявляються та повідомляються лише деякі цифрові атаки та інциденти та лише ті, що є визначальними, тобто, є певний розмір підприємства та клас інциденту. У таблиці 1 наведені результати опитування, опублікованого в США. Результати вимірюються як частка всіх підприємств, які постраждали від розміру та інциденту клас. Зверніть увагу на широкі розбіжності не тільки між

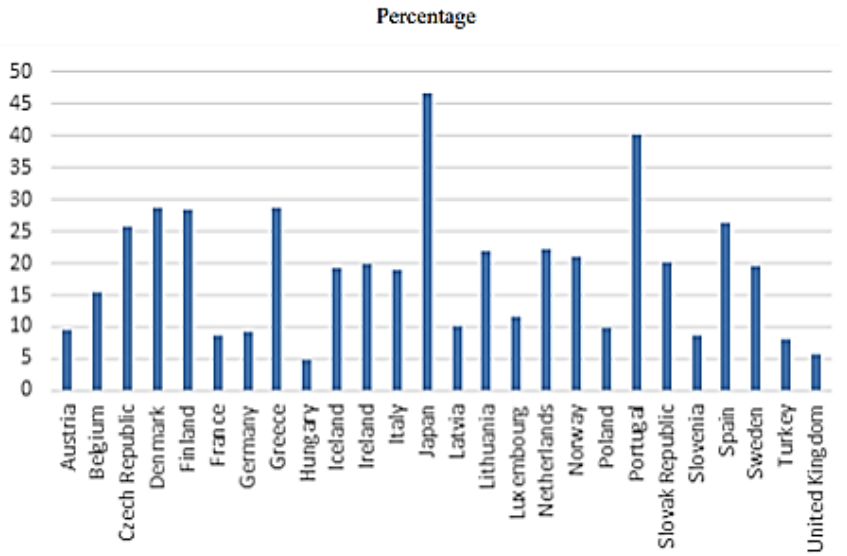

Рис. 1. Дослідження зафіксованих цифрових атак та інцидентів в бізнесі за 2021 рік

Джерело: OECD

різними класами інцидентів, але і розмірами підприємства-відповідача. Деякі інциденти частіше виявляються через їх різні впливи, ніж інші. Більше того, частка респондентів, яка, ймовірно, буде мати можливості виявляти певні класи інцидентів, також, ймовірно, відрізнятимуться між собою, а також приймаються до уваги підприємства різних розмірів. Все це у сукупності викликає питання щодо надійності та корисності результатів опитування.

Відразу зауважимо, що більшість із підприємств взагалі не повідомляють про випадки будь-якого класу виникнення у них цифрових інцидентів за попередній рік. З тих, що виявляли та повідомляли про інциденти, знову ж більшість повідомляє про 1-5 інцидентів загалом. Не зрозуміло який клас інцидентів виявляється та повідомляється, що ускладнює розуміння де пов'язані загрози та вразливості, що, в свою чергу, допоможе ефективно управляти відповідними ризиками.

Таблиця 1

Поширеність випадків комп'ютерної безпеки, США, за розміром бізнесу (чисельність персоналу)*

	Всі інциденти	Кібератаки	Кіберзломи	інші
Всі бізнеси	67	58	11	24
2-24	50	44	8	15
25-99	59	51	7	17
100-999	70	60	9	24
1000+	82	72	20	36

* Результати опитування, опублікованого в Австралії в 2009 р.

Потрібна подальша робота, щоб краще зрозуміти, де найбільше можна отримати надійні дані про випадки та чи можуть опитування надати корисні дані додаткові дані, рис. 2.

Вимірювання впливу інциденту цифрової безпеки, оцінка та звітність

Справжній фінансовий вплив інциденту цифрової безпеки важко точно оцінити і виміряти. На першому етапі важливо розрізняти

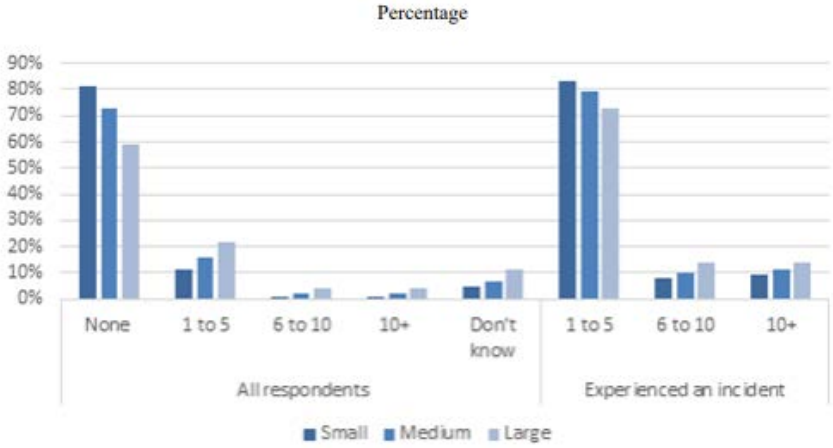

Рис. 2. Кількість випадків комп'ютерної безпеки за розміром бізнесу, Австралія (результати опитування, опублікованого в Австралії в 2019 р.)

прямі витрати, непрямі економічні втрати та альтернативні витрати. Коли трапляється інцидент цифрової безпеки, такий як порушення даних, виникають прямі витрати організації, що була атакована [26]. Ці витрати можуть включати ремонт мережі, найми консультантів з питань безпеки та придбання послуг кредитного моніторингу для постраждалих.

Прямі витрати мають перерозподільний характер, тобто вони представляють грошові кошти, сплачені або викрадені одним суб'єктом господарювання іншим. Це відрізняється від непрямих економічних втрат, які представляють собою втрату економічної діяльності або знищена економічна цінність.

Непрямі втрати від інцидентів цифрової безпеки є тими, які не можуть бути пов’язані виправданим ступенем точності безпосередньо з конкретним інцидентом (стверджується у дослідженні Гордона та Лоеба, 2006). До таких категорій, як правило, належать: втрата клієнта довіра / шкода репутації, зменшення використання цифрових технологій через відсутність довіри та альтернативні витрати та втрата продуктивності, пов’язані з необхідністю інвестування в нецифрову інфраструктуру (визначено командою науковців під керуванням професора Андерсона, 2012).

Існують також альтернативні витрати, пов'язані з прямими витратами через інциденти цифрової безпеки, інвестиції в превентивні заходи безпеки. Для приватних підприємств, а не для витрат кошти на консультантів з питань безпеки та профілактичні заходи, ці самі кошти могли бути інвестовано в діяльність, яка сприяє іншій діяльності, що приносить дохід, або заходи щодо підвищення продуктивності праці фірми. Ці поняття є не завжди диференційовано в цифрових дослідженнях безпеки, що призводить до неточних оцінок витрат / збитків від інцидентів. Витрати та збитки, як правило, складаються з багатьох категорій, кожна з яких має власного родича проблеми вимірювання.

Наведені нижче приклади, взяті з минулих опитувань, продемонструвати широкі розбіжності між різними методологіями витрат і збитків та, по суті, важливість чіткого визначення того, що вимірюється, таким чином, щоб це могло бути достовірно повідомленим відповідачем. Прямі витрати після інциденту, такі як найм консультантів або ремонт IT інфраструктури, можна порівняно легко оцінити через

наявність рахунків-фактур на ці послуги. Однак слід бути обережним у визначенні ключових термінів (наприклад, типу інциденту, категорії витрат / збитків, часовий масштаб), щоб отримати корисні, надійні та порівнювані результати.

Таблиця 2

Грошові втрати, спричинені інцидентами з комп'ютерною безпекою, за типом інциденту, Сполучені Штати*

	Не було втрат	Втрати у 1000-9000 дол. США	Втрати у 10000-99000 дол. США	Втрати у понад 100000 дол. США
Інциденти цифрової безпеки	10	51	27	13
Кібератаки	9	57	25	9
Комп'ютерні віруси	7	60	24	9
Відмова сервісів	19	52	24	6
Вандалізм чи саботаж ІС	11	59	21	9
Кібервзломи	6	26	38	30
Кіберкрадіжка даних, що містять комерційну таємницю	4	19	44	33
Кіберкрадіжка об'єктів інтелектуальної власності	9	17	36	38
Кіберкрадіжка персональних даних та особистості	11	31	29	29
Інші інциденти цифрової безпеки	20	49	25	7

* За даними аналізу OECD

Результати опитування, наведеного нижче, стосуються прямих збитків (хоча збитки не визначено явно) від інцидентів цифрової безпеки, що виникли на підприємствах Сполучених Штатів за 2022 рік.

Вони вказують, що більшість респондентів зазнали загальної втрати у 1000 доларів США – 9000 за попередній рік. Розподіл цих втрат серед населення включає а меншість підприємств, для яких збитків не було. Повідомлені збитки та їх розподіл істотно різняться між різними категоріями інцидентів, хоча різниці між різними категоріями не завжди чітко розмежовано.

Непрямі збитки від інциденту, такі як втрата доходу або вартість викраденого інтелекту

Однак у деяких випадках, хоча і не завжди, може бути важко оцінити майно, яке було втрачено при виникненні кіберінциденту. Для, наприклад, відокремлення частки падіння доходу через інцидент від тієї, яка була обумовлена більш широкими економічними умовами протягом певного періоду, не можливо зробити достатньо чітко (і якщо вплив очевидний, це може не обов'язково бути зрозумілим респонденту опитування). Навпаки, визначити непрямі витрати через переривання бізнесу порівняно легше щоб визначити, хоча, знову ж таки, ці витрати можуть бути не зрозумілі респонденту опитування. На малюнку нижче узагальнено результати опитування, проведеного у 2019 році. Результати такі, що малося на увазі включати всі витрати від певних інцидентів, які вплинули на підприємство респондента за попередній рік. Мабуть, найбільш значущий висновок із них є те, що більшість респондентів не понесли ніяких витрат, оскільки вони не понесли інцидентів (або їх не помітили чи умовчали з міркувань збереження репутації). Припускаючи, що ті, хто повідомив про витрати, справді зазнали інцидентів, розподіл звітних витрат охоплює всі смуги відносно однаково, хоча це не так чітко визначити, які підприємства понесли які витрати. Це важливо, враховуючи, що витрати є ймовірно суттєво різниться в залежності від розміру підприємства, галузі та цифрової інтенсивності

В ідеалі для оцінки непрямих збитків потрібно буде встановити контрфакт (тобто які могли б бути доходи, якби інцидент не стався). Це може бути можливо, якщо надходження від стабільної компанії, що працює у галузі багато років. Однак, насправді таке рідко буває. Більше того, багато інцидентів цифрової безпеки залучають або впливають на нематеріальні активи, які важко оцінити. Необхідна подальша робота для більш чіткої класифікації та вимірювання економічних наслідків

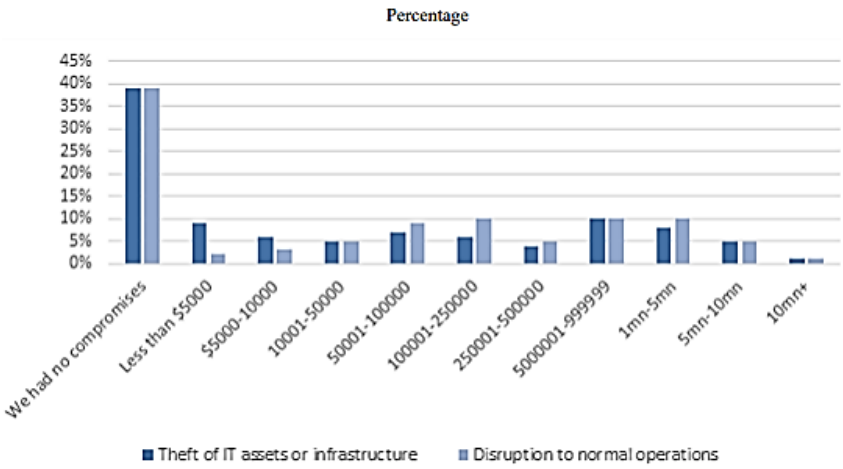

Рис. 3. Приблизно скільки шкоди або крадіжки ІТ-активів та інфраструктури / порушення нормальної діяльності коштувало вашій організації за останні 12 місяців?*

*Дані опубліковано у звіті цифрової економіки за 2019 рік по країнам ОСЕР

інцидентів цифрової безпеки, перш ніж з опитування можна буде вважати достатньо надійним та корисним інструментом, аніж використання моделювання (наприклад, метод Монте-Карло) яке може дозволити обмежені, імовірнісні кошториси, які слід розрахувати, але до цього часу були недостатньо використані в польових умовах, і тому майбутня робота може використовувати ці та інші аналітичні методи.

Визначення цифрового інциденту

При спробі порівняти результати в ході опитувань, окрім методологічних труднощів, деталізовані вище, основною перешкодою є відсутність консенсусу щодо визначень, типології та таксономії інцидентів цифрової безпеки, загроз та вразливостей, та багато інших аспектів. Три конкретні приклади виділяються із цифрового ризику безпеки та обстеження управління бізнесом, розглянуті на першому етапі: цифрова безпека, розмір підприємства та інцидент.

Цифрова безпека: існували великі розбіжності між опитуваннями щодо термінології, яка використовується для позначення цифрової

безпеки. Терміни «інформація», «Інтернет», «комп'ютер» або «кібер» по-різному використовувались разом із терміном «безпека». У деяких випадках визначення не було надано для терміну, що використовується, що ускладнює розуміння того, чого опитування стосуються, щоб зробити висновки та висновки з результатів та порівняти результати.

Розмір підприємства: для малого, середнього та великого бізнесу можуть використовуватися різні визначення в опитуваннях, де результати стратифіковані за розмірами підприємства. Це поширене питання у всьому світі для опитувань та статистичних даних, що стосуються бізнесу, і не обмежується лише цифровим ризиком безпеки опитування керівництва. Визначення МСП (малих і середніх підприємств) (або МСБ (малого і середнього бізнесу) в США) може бути визначене виходячи з річного доходу або країни. Поріг, на якому вважається бізнес є МСП відрізняється в різних країнах та в межах країн, за галузевим сектором. Більше того, деякі країни до МСП включають підприємства з нульовим співробітником (ФОП), а інші – ні. Деякі опитування виключають підприємства, у яких менше десяти працівників. Опитування по-різному стосуються підприємств, підприємств, фірм, установ тощо, і не визначають, що мається на увазі під термін, що використовується. Всі ці елементи перешкоджають перехресному опитуванню порівняння результатів.

Інциденти: Для позначення класів інцидентів з деякими використовувались дуже різні таксономії поєднання загроз, вразливостей, інцидентів та наслідків разом під широкими, всеохоплюючими умовами Наприклад, багато опитувань використовували термін «порушення» для позначення «Інцидент», загалом кажучи, коли термін «порушення» зазвичай використовується для позначення а підмножини випадків, що впливають на конфіденційність та, можливо, цілісність даних.

Найкращі опитування чітко пояснити респондентам, що означає кожен термін у глосарії. Однак не всі опитування надати глосарій, який ускладнює проблему, яку респонденти не розуміють технічні поняття, враховуючи, що самі терміни не є чітко визначеними. Це в свою чергу знижує надійність результатів таких опитувань. Відсутність чіткого визначення або а глосарій також перешкоджає можливості читачів інтерпретувати, що означають кінцеві результати опитування.

Загальна одиниця виміру повинна бути чітко названа під час опитування практики управління цифровими ризиками безпеки на підприємствах з метою отримання корисних, відповідних даних з інструмент опитування. Теоретично можливо, що деякі показники мають відношення до індивідуальний респондент, підрозділам або підрозділам у бізнесі або загальному бізнесі себе. Більше того, практики управління ризиками, а також абсолютний та відносний рівні безпека, ймовірно, буде відрізнятися залежно від одиниці виміру, про яку йдеться (наприклад практики підприємства в цілому порівняно з практикою окремого респондента). Висновок Ці обмеження, обмеження та проблеми є фоном для рішень, прийнятих у розробці системи вимірювань, показників та інструменту пілотного обстеження.

Система вимірювання цифрового ризику безпеки управління на підприємствах

Система вимірювань, розроблена для оцінки цифрової безпеки практики управління ризиками бізнесу (FERMA) – є інструментом опитування, який використовується для основи для збору даних, які можуть:

– допомогти компаніям порівняти свій відносний ризик цифрової безпеки практика управління проти однолітків;

– допомогти інформувати державну політику, яка має на меті підняти рівень зрілості підприємств з управління ризиками цифрової безпеки.

Структура була розроблена протягом майже двох років спільною робочою групою, до складу якої входять делегати робочих груп SPDE та MADE; делегати цих Робочих груп; а також вказівки інших експертів з ОЕСР країн. Проект був спочатку запропонований як результат першої фази проекту ОЕСР. На другому етапі було розглянуто структуру та показники, а потім все доопрацьовано на основі відгуків. Потім проект спільного інструментарію був розроблений спільним завданням силами ОЕСР та Cetic.br, а згодом піддана когнітивному тестуванню Cetic.br.

Після переглядів, що базуються на відгуках, до третьої фази залучався пілот інструменту обстеження FERMA. Пілот надає додатковий зворотний зв'язок з місця роботи щодо запитань та понять, які вони включають, а також корисність та придатність даних, зібраних для кожного з показників. У міру розвитку технологічних та політичних пріоритетів розвиваються уроки пілотного опитування враховуючи, опиту-

вання потрібно переглянути та адаптувати. В деяких випадках, країни можуть вибрати додавання нових індивідуальних показників на основі потреб політики або контекстуальні законодавчі та нормативні вимоги, за винятком технічних умов та / або надання подальша конкретність на основі потреб політики або відносної зрілості респондента.

Однак це не повинно впливати на міжнародну порівнянність результатів. Вимірювання FERMA значною мірою спиралися на Принципи ОЕСР, що містяться в Рекомендація ОЕСР щодо управління ризиками цифрової безпеки для економічних та соціальних питань («Рекомендація щодо безпеки»). Представлення консенсусу ОЕСР країн щодо того, що становить бажану практику щодо ризику цифрової безпеки, Рекомендація з безпеки забезпечує надійну основу, на якій слід розробити показники для оцінки цифрових практик управління ризиками безпеки бізнесу.

Структура застосовує модульний підхід згідно з рамками «модельного опитування» ОЕСР (Рекомендація ОЕСР, 2011). Щоб бути в цілому корисним, модельне опитування ОЕСР включає окремі, автономні модулі, що забезпечують гнучкість та пристосованість до швидко мінливого середовища. Основні модулі можуть бути додані до існуючих національних опитувань або адмініструватися як самостійне опитування FERMA, тоді як додаткові модулі можуть використовуватися за потребою країн. Цей підхід дозволяє широко виміряти основні поняття на міжнародно порівнянному рівні, дозволяючи країнам адаптувати частину вмісту, який вони збирають, для задоволення конкретних потреб країн.

Наведемо повну структуру вимірювань FERMA, яка складається з шести модулів та вісімнадцяти показників. Кількість Показники відрізняються залежно від модулів, як і кількість запитань для збору даних кожен показник за допомогою інструменту опитування. Кожен індикатор прагне виміряти відсоток від загальної кількості підприємств (респондентів).

Модуль А: Демографія

Обґрунтування: Модуль А включає показники та запитання, що дозволяють розшарувати вибірки та подальший аналіз на основі підгруп підприємств.

Показник А1: реєструє географічне розташування підприємства та географічне розташування материнської компанії у випадку, якщо відповідач є дочірньою компанією.

Показник A2 і A4: реєструє розмір підприємства за штатним штатом (показник A2) або за річним оборотом (показник A4). Порогові значення для чисельності персоналу дозволяють бути розділеними на основі конкретного визначення країни, про яку йде мова. Поле для річного товарообігу забезпечує постійну змінну, що дозволяє встановлювати порогові значення де завгодно.

Показник A3: Визначає економічну діяльність (тобто галузь промисловості) респондента підприємство, засноване на ISIC rev. 4 стандартні.

Показник A5: Вимірює цифрову інтенсивність (або залежність) підприємства респондента. Це важливо, оскільки наступні модулі пов'язані з цифровим ризиком безпеки. На практиці управління відповідним підприємством можна оцінити в контексті (тобто, якщо підприємство не використовує багато цифрових технологій, а наступні відповіді, які припускають низькі практики управління цифровим ризиком безпеки / зрілість становлять відносно меншу стурбованість).

Модуль B: Управління ризиками цифрової безпеки

Обґрунтування: Модуль B призначений для оцінки того, чи має підприємство відповідну цифрову система управління ризиками безпеки. Такий каркас є вимогою до ефективного управління ризиками цифрової безпеки, особливо для відносно великих організації, в яких часто потрібна складність управління цифровими ризиками безпеки прийняття офіційних рішень. Те, що цей модуль з'являється, відображає міркування управління як загальної концепції, яка зачіпає всі аспекти та є визначальним фактором успішного управління ризиками цифрової безпеки на підприємстві.

Показник B1: Розподіл відповідальності на конкретні ролі на підприємстві є а наріжний камінь ефективного управління ризиками цифрової безпеки. Це відображено в Принципі 2 принципів OECP та у FERMA / Європейській конфедерації внутрішніх інститутів Аудиторський звіт (ECIIA) щодо корпоративного управління та кібербезпеки (2017). Для цього показник B1 та пов'язані з ним питання намагаються з'ясувати, чи є у підприємства роль / відділ, присвячений загальному управлінню ризиками; чи ця роль / відділ також відповідає за управління ризиками цифрової безпеки; і який відділ конкретно відповідає за управління ризиком цифрової безпеки та визначення допустимого рівня ризику цифрової безпеки за кожну ділову діяльність.

Показник B2: Структура управління, як правило, відображається в корпоративній або організаційній політиці або документі управління. Такий каркас може приймати якомога більше форм, оскільки існують культури та стилі управління організацій (OECD, 2015a). Для цього показник B2 та пов'язані з ним питання (B2a, B2b, B2c) мають на меті визначити, чи є політика – письмова або усна і чи діє вона на підприємстві, і якщо так, то що вона охоплює.

Показник B3: Рекомендація ОЕСР щодо безпеки наполягає на забезпеченні ефективної цифрової безпеки управління ризиками вимагає постійного перегляду цифрового ризику безпеки як частини поточного процесу оцінки (там же). Дійсно, Принципом 5 Рекомендації є «оцінка ризику і цикл лікування », що відображає його важливість у загальній безпеці Рекомендацій ОЕСР. З цієї причини індикатор B3 намагається визначити, чи існує процес для моніторингу та аналізу управління цифровими ризиками безпеки в межах підприємства; які практики моніторингу виконуються та, у випадку, якщо вони є, як часто такі практики трапляються.

Показник B4: Рекомендація ОЕСР щодо безпеки, згідно з Принципом 4 «Співпраця», каже, що співпраця, «повинна відбуватися урядами, державними та приватними організації» (там само). Ця співпраця є «важливою для заходів безпеки, інновацій та заходи щодо готовності, які мають бути повністю реалізовані» (там само). Причина, з якої це важливо, полягає в тому, що ефективне управління цифровими ризиками безпеки вимагає взаємодії між технічною стороною управління підприємством (наприклад, команда ІКТ) та діловою стороною управління підприємством, і що саме це підтримує (наприклад, виконавча команда, відділ управління ризиками тощо). Тільки разом ці дві сторони можуть приймати рішення, які врівноважують потребу в безпеці з необхідністю сприяння економічної діяльності і, отже, економічному процвітанню відповідного підприємства. З цієї причини показник B4 намагається визначити, чи відбувається взаємодія в структурованому шлях між персоналом, відповідальним за управління бізнесом, та ІКТ при оцінці цифрових технологій ризик безпеки.

Модуль C: Практика оцінки цифрових ризиків безпеки

Обґрунтування: Постійна оцінка ризику та кіберлікування є важливими для забезпечення відповідності рішень, пов’язаних із безпе-

кою, та їх співвідношенням з ризиком та економічними та соціальними активностями. З цієї причини модуль С націлений на вимірювання певних практик цифрової економічної безпеки, які становлять відповідний процес оцінки ризику.

Показник С1: Рекомендація ОЕСР з безпеки вимагає наближення економічного ризику до цифрового ризику, а не лише розглядати його як технічну проблему, яка вимагає певних технічних рішень. Для цього потрібно, щоб цифровий ризик «був невід'ємною частиною загального процесу управління ризиками та прийняття рішень в організації» (OECD, 2015a). З цієї причини показник С1 намагається визначити, чи існує загальний ризик процесу управління на підприємстві та, якщо так, чи цифровий ризик безпеки процесу управління є частиною цього загального процесу.

Показник С2: Оцінка цифрового ризику безпеки в ідеалі повинен складатися з трьох етапів. Ризики слід визначити, проаналізувати та оцінити. З цієї причини індикатор С2 прагне визначити не просто чи виконуються ці три етапи в якійсь формі в межах підприємства, але і хто в межах підприємства або за його межами виконує завдання, які кожен з цих етапів передбачає. Більше того, в Рекомендації з питань безпеки ОЕСР сказано, що цей процес повинен бути безперервним / постійним. З цієї причини питання в інструменті опитування намагається визначити, як часто підприємство оцінює можливі наслідки інцидентів безпеки цифрових технологій, які можуть вплинути на діяльність підприємства. Цей конкретний елемент (тобто можливий наслідок інцидентів цифрової безпеки) було обрано внаслідок динамічного характеру цифрових загроз і вразливостей, які вимагають більшого циклічного моніторингу, ніж інші елементи завдяки своїй динамічній природі.

Модуль D: Цифрові практики зменшення ризиків безпеки

Обґрунтування: Зниження ризику є однією з чотирьох широких категорій варіантів лікування ризику, тобто це ті структури у складі підприємства, хто відповідає за управління ризиками в бізнесі, і які можуть вибирати, коли лікувати ризик.

Показник D1: Зниження ризику має бути спрямоване на зниження цифрового ризику безпеки до прийнятного рівня, визначеного в оцінці ризику. Питання D1a має на меті визначити, чи існувала якась практика зниження цифрового ризику безпеки завдяки оцінці ризику. Щоб

зменшити ризик, можуть бути обрані та застосовані заходи безпеки, при цьому інновації можуть розглядатися як щодо заходів безпеки, так і діяльності, про яку йдеться; і заходи щодо готовності та безперервності можуть бути визначені та застосовані у випадку інциденту (OECP, 2015a). Цей показник має на меті визначити, чи є якась із цих трьох форм ризику на відповідному підприємстві за попередні дванадцять років і чи застосовувались практики їх зменшення.

Показник D2: Відповідно до Принципу 4 «Співпраця» Рекомендації OECP щодо безпеки, «Оскільки зацікавлені сторони є взаємозалежними та залежними від цифрового середовища, співпраця є надзвичайно важливою (там же)». Одним із способів оперативної реалізації цієї співпраці є форма обміну інформацією між зацікавленими сторонами. Таким чином, індикатор D2 прагне визначити, чи має підприємство спільну інформацію про цифрові загрози безпеці, вразливість, інциденти, практика управління ризиками або заходи безпеки з будь-ким із числа зовнішніх зацікавлених сторін.

Модуль E: Практика передачі цифрових ризиків безпеки

Обґрунтування: Передача ризику є однією з чотирьох широких категорій варіантів, які відповідальні для управління ризиками всередині підприємства при виборі лікування ризику. Передача ризику включає, «переміщення небажаних наслідків невизначеності на цілі діяльності когось іншого»(там само).

Показник E1: Один із найпоширеніших способів передачі ризику іншій зацікавленій стороні укладається за контрактом, зокрема через страхування. Індикатор E1 вимірює безпосередньо чи має підприємство-респондент якийсь діючий страховий поліс, який охоплює цифровий ризик безпеки.

Показник E2: У багатьох країнах OECP купівля і акцептування підприємствами страхових полісів, які охоплюють ризики цифрової безпеки залишаються на відносно низькому рівні. Політики в таких країнах часто прагнуть зрозуміти, чому цей показник низький, як основа для цього впроваджувати заходи, які могли б полегшити ці відчутні перешкоди. Отже, показник E2 намагається визначити причину, чому респонденти не мають такого страхового полісу.

Показник E3: Страхові поліси, що покривають ризики цифрового ризику безпеки (іноді «кіберстрахування») мають багато форм. Іноді

вони є «самостійні» політики (тобто політики, що охоплюють лише ризики цифрового ризику безпеки) та інші, коли вони включаються в існуючі страхові лінії (наприклад, директори та офіси [D&O] або [P&C]) (Романоуський та ін., 2017). Індикатор E3 та пов'язані питання намагається визначити, який ризик охоплюється підприємством єдиним або потенційно численними страховими полісами, які можуть покривати такі ризики.

Показник E4: Страхування є однією з форм багатьох механізмів передачі ризиків. Індикатор E4 визначає, які ще загальновживані договірні та позадоговірні механізми передачі ризику використовуються підприємством респондента.

Модуль F: Поінформованість та навчання щодо управління цифровими ризиками безпеки

Обґрунтування: «Управління ризиками цифрової безпеки вимагає спочатку зрозуміти, чи такий ризик існує» (там же). Тому обізнаність є основою для всіх інших Принципів ОЕСР. Зацікавлені сторони, які не знають про існування ризику, в кінцевому підсумку мимоволі приймають ризик, а не оцінюють потім лікування. Поінформованість – це перший крок на шляху до відповідальності (Принцип 2 Керівного принципу Рекомендації ОЕСР щодо безпеки). Здатність приймати відповідальні рішення (тобто ефективне управління ризиком) вимагає для цього навичок. З цих причин цей модуль вимірює різні практики, включаючи навчання, для створення та / або підвищення обізнаності про ризик цифрової безпеки та управління ним на підприємстві.

Показник F1: Поінформованість може бути підвищена однією з багатьох конкретних практик (наприклад, семінари, конференції тощо). Навички набуваються різними засобами, включаючи освіту, навчання, досвід тощо. Показник F1 має на меті визначити, яка з цих практик та які кошти на це існують на даному підприємстві. Він також прагне визначити, хто отримує підвищення рівня обізнаності або навчання, враховуючи, що різні рівні обізнаності та різні види навички (набуті за допомогою навчання) потрібні людям, щоб виконати свою роль у ефективному управлінні цифровим ризиком безпеки. Особливо це стосується директорів та керівників напрямків бізнесу, що є дуже важливо в цьому плані. Без обізнаності та здатності ефективно управляти ризиком у керівного складу підприємства, зусилля зробити це

«знизу» менш вірогідні (FERMA & ECIIA, 2017 та ВЕФ, 2016). З цієї причини останнє питання в інструменті опитування намагається з'ясувати, чому не проводилось навчання для людей у цих ролях (у випадку, якщо таких навчань не було).

Пілотне опитування та його результати

Тут міститься аналіз відповідей на пілотне опитування, проведене в спільно з FERMA у період з липня по вересень 2021. FERMA об'єднує 22 асоціації з управління ризиками у 21 європейській країні. Їх членство забезпечує доступ до цільової групи з 4800 осіб, що займаються ризиком, по всій Європі. Всередині підприємства, менеджери ризиків несуть відповідальність за розуміння ризиків, які можуть вплинути на ризики підприємства здатності досягати своїх цілей і згодом реалізувати скоординований набір практик та методів лікування (контролю) цих ризиків (ISO, 2009). Це означає, що вони володіють розумінням економічних компромісів, пов'язаних із практикою безпеки в межах підприємства. Рекомендація OECP з безпеки 2015 року зосереджена на: «Економічні та соціальні цілі державних та приватних організацій та необхідність прийняття підходу, заснованого на управлінні ризиками. Замість того, щоб розглядати цифровий ризик як суто технічну проблему, що вимагає технічних рішень, цифровий ризик повинен підходити до них як до економічного ризику; отже, він повинен бути невід'ємною частиною загального процесу управління ризиками та прийняття рішень в організації».

Опитування ризикменеджерів дозволило визначити, якими способами та якою мірою Рекомендації OECP з безпеки в даний час введені в дію в рамках цільових підприємств з ризиком. У випадку, якщо у підприємства не було менеджера з управління ризиками, запитуваний респондент опитування включав: внутрішнього аудитора; бухгалтера; аудитор, голову / члена Керівного комітету; головного виконавчого директора; начальника операційного відділу; або фінансового директора. Зверніть увагу, що жодна з цих ролей не є технічною / IT-роллю. Це відображає позицію Рекомендації щодо підходу до ризику цифрової безпеки як до саме економічного ризику, а не як до технічного.

Однак підхід, прийнятий для пілотного проекту FERMA, має недоліки. У тому випадку, якщо цифрові практики управління ризиками безпеки не інтегровані в загальну структуру підприємства структу-

рою управління ризиками (тобто це трактується як технічний ризик), цільова група ризикменеджерів не зможуть точно відповісти на запитання, оскільки вони вимагають розуміння рішень щодо технічної безпеки, прийнятих в IT-відділі. Як результат цього, навіть серед відносно складного населення з точки зору управління ризиками, значна частина підприємств все ще не інтегрує цифрові технології безпеки в загальну систему управління ризиками. Більш вичерпною практикою цифрового управління ризиками безпеки на підприємствах є включення обидвох перспектив менеджерів з управління ризиками та IT-перспектив. Більше того, значна частина респондентів, доступних через FERMA, є великі підприємства. Цей проект OECP спочатку прагнув отримати уявлення про цифрові технології практики управління ризиками безпеки МСП. На жаль, такого розуміння бути не могло отримано від цільової сукупності пілота. Інструмент пілотного опитування відображає характеристики цільової сукупності в тому, що вона використовує відносно вдосконалене управління ризиками поняття та терміни. Цей словник не підходить для цільової групи що містять більшу частку МСП. Надалі використовувалася система вимірювань для проектування інструменту пілотного обстеження можна було б використати для розробки переглянутого інструменту для опитування МСП.

Аналіз результатів пілотного опитування надається з метою визначення сильних і слабких елементів інструмента пілотного обстеження FERMA, так як пропонується аномальні або незвично узгоджені закономірності в повних відповідях. Аналіз розділений на дві частини. У першій частині розглядаються повні відповіді, а в другій коротко вивчаються неповні відповіді.

Мета цього аналізу – не надати репрезентативну статистику щодо поточної цифрової інформації щодо практик управління ризиками безпеки підприємства. Зокрема, населення не є представником загальної сукупності підприємств; респонденти були не вибрані випадковим чином. Для того, щоб мати оцінки для всієї сукупності підприємств, інформацію для цільової сукупності – необхідний зразок. Сюди входить кожна одиниця популяції, що представляє інтерес, доступна для відбору з імовірністю більшою за нуль. Таке обстеження слід проводити, застосовуючи імовірнісний підхід, який дозволяє рандомізований вибір підприємств.

Протягом аналізу висловлюються пропозиції щодо подальших ітерацій опитування інструмент може бути спрямований таким чином, щоб забезпечити якісніші відповіді та дані. Як загальна пропозиція та з метою покращення якості процесу збору даних у майбутньому важливо, щоб під час збору даних створювалися звіти про польовий контроль процесу. Сюди входять, але не обмежуючись: посібники з виїзного навчання для інтерв'юерів, інструкції для респондентів та рецензентів.

Результати

FERMA розпочала розповсюдження пілотного опитування тринадцяти асоціаціям добровольців-членів 11 липня 2018 р. Асоціації передали пілотне опитування своїм відповідним членством в різні дати, частково через наближення святкових канікул. Одержувачі різнились асоціаціями та країнами, деякі з них вирішили надіслати опитування всім членам (наприклад, AIRMIC у Великобританії), тоді як інші воліли надсилати його певним (наприклад, GVNW у Німеччині надсилається лише великим підприємствам). Асоціації та їхні члени не мали однакових часових вікон та тривалості часу, на який відповідали опитування. Нагадування про розповсюдження опитування серед учасників були надіслані в середині серпня, кінці серпня та середині вересня. Загалом було отримано 80 заповнених відповідей у всіх країнах. Основна маса відповідей надійшли від підприємств Бельгії (16 відповідей), Фінляндії (15 відповідей) та Франції (14 відповідей). Рівень відповідей різнився в різних асоціаціях з найбільш високим у BELRIM (Бельгія) – 18%. Загальний коефіцієнт відповіді становив приблизно 3%, це дещо пригнічується помітною відсутністю відповідей від AIRMIC (Об'єднане Королівство), що становило майже 50% респондентів опитування (1058 з 2602 одержувачів). Видалення AIRMIC із загальної кількості призводить до загальної кількості відповідей до 5%, яка все ще залишається низькою.

Модуль А: Демографія

Показники А2 та А4 збирають дані про розмір підприємства респондента за кількістю працівників та дохід. За обома показниками переважна більшість респондентів вважатимуться великими підприємства (90% як за штатом, так і за річним оборотом) 7. Індикатором А3 збирається інформація про основну галузь підприємства. Найбільша частка

респондентів належать до обробної промисловості (24%), за якою слідують фінансова та страхова діяльність (16%), а також транспортування та зберігання (13%).

Показник A5 вимірює цифрову напруженість підприємства респондента. Оцінено дев'ять різних технологій / застосувань технології, результат дає короткий огляд ступеня до на які покладається підприємство і, отже, має управляти ризиком, пов'язаним із цифрові технології, про які йдеться. У всіх респондентів цифрова інтенсивність когорти є відносно високим, що можна було б очікувати, враховуючи розмір відповідних підприємств.

Середня кількість використовуваних технологій становить 7,8 із медіаною 8. Усі респонденти мали веб-сайт і майже всі (98%) мали інтранет. Електронна комерція була найменш помітним використанням цифрової технології (73%). Цікаво, що широкосмуговий зв'язок (76%) також не використовувався настільки широко, як можна очікувати, враховуючи широку доступність широкосмугового Інтернету в Європі країни, де базуються ці підприємства. Висока частота випадків «не знаю» як відповідь на цей конкретний варіант (21%) свідчить про те, що може виникнути потреба у чіткому визначенні що становить широкосмугове з'єднання. Можливо також, що це питання може бути зайвим, враховуючи, що всі інші технології потребують доступу до Інтернету (широкосмуговий чи ні) і тому слід припустити, що певна форма підключення до Інтернету (широкосмугова чи ні) існує. Ключовий елемент, який відсутній у демографічному розділі, пов'язаний із визначенням ролі відповідача на своєму підприємстві. Хоча для цього пілота це потенційно менше проблем опитування з FERMA завдяки великим підприємствам-респондентам та пов'язаним з ними вищим ймовірність відповідача відповідати за управління ризиками, його слід виправити у майбутніх ітераціях інструменту опитування, особливо у тому випадку, якщо збільшиться кількість МСП присутній у вибірці сукупності.

Модуль B: Управління ризиками цифрової безпеки

Більшість (85%) респондентів мали відділ або працевлаштовану особу головним чином відповідає за загальне управління ризиками на підприємстві. Однак з цього підмножини8, лише третина (32%) мала цю особу чи відділ, відповідальний за управління цифровим ризиком безпеки підприємства. Натомість, головний інформаційний дирек-

тор або IT-менеджер (43%) або начальник Цю відповідальність взяв на себе службовець з питань інформаційної безпеки (38%). Навпаки, начальник Виконавчий директор (33%), швидше за все, був відповідальним за прийняття прийнятного рівня ризику цифрової безпеки для кожної ділової діяльності, за яким слідує головний інформаційний директор або IT-менеджер (19%). У невеликій кількості випадків Рада директорів (4%) була відповідальний, який було введено вручну через «Інше (будь ласка, вкажіть)».

Переважна більшість респондентів (84%) мали або письмове, або неписане цифрове забезпечення політика. З цього підгрупи, переважна більшість (90%) мали письмову політику цифрової безпеки. З огляду на таку високу пропорцію, в майбутньому може бути доцільнішим лише задавати питання пов'язаний із типом політики з додатковою опцією відповіді «Не мати політики». Фактичний зміст цієї політики суттєво різнився, що дає деякі цікаві факти прозріння. Майже всі (91%) розподілили ролі та відповідальність за ризик цифрової безпеки управління на підприємстві, а також охоплення підвищення обізнаності та навчання (93%). Передача ризику навряд чи з'явиться в цих політиках (37% відповідають «Так») пропонують високу частку «Не знаю» (15%) для цього та для «процесів лікування ризику» що ці варіанти відповідей, можливо, не були добре зрозумілі респондентами. варіант відповіді «процес лікування ризику» може бути зайвим, враховуючи те, що інші наступні варіанти містять елементи такого процесу (наприклад, «рішення щодо заходів цифрової безпеки», «передача ризику»). Іншим способом інтерпретації даних, зібраних за цим показником, є врахування «глибини» політики безпеки. Глибину можна було виміряти, враховуючи, скільки практик в рамках опитування було наведено дев'ять варіантів, охоплених політикою в цій когорті інструмент. Якщо вимірювати таким чином, середня та середня кількість охоплених практик становить приблизно 6,6 з максимум 9 із стандартним відхиленням 2,7 для зразка 80 респондентів. Це свідчить про те, що підприємства цієї когорти мали відносно глибоку безпеку політики вкрай ймовірних випадках, коли на початку у підприємства була така політика.

Результати для показника B3, який намагається виміряти частоту певного моніторингу діяльності, може бути важко візуально інтерпретувати. Рівномірність відповідей у різних діяльність свідчить про те, що

респонденти обрали однакову відповідь у всіх заходах моніторингу не розрізняючи між собою. Тим не менше, з тих, хто брав участь у цій діяльності, більшість робили це щорічно. Незначна частина не проводила жодного моніторингу діяльності. У наступних ітераціях опитування може бути кращим дозволити респондентам відповісти негативно на запитання B2a (яке задає питання про наявність письмової чи неписаної політики) потім згодом мати змогу відповісти на питання B3. Можливо, що респондент підприємство не має письмового або неписаного плану, але все ще проводить певний моніторинг діяльності. Виключаючи цих респондентів за проектом, інформацію від цих підприємств (що становило 15% від загальної кількості в пілоті) не може бути захоплено.

Більшість респондентів (70%) організовували фізичні або віртуальні зустрічі із відповідальним персоналом управління бізнесом та ІКТ для визначення ризику цифрової безпеки в порівнянні з попереднім рік. Тільки 10% не знали, хоча 20% не знали. Це питання корисне, як може бути порівняно з наступними питаннями, що стосуються внутрішньої та зовнішньої співпраці та спілкування як перевірка узгодженості відповідей. Модуль C: Практика оцінки цифрових ризиків безпеки Значна частина (81%) респондентів мали регулярний загальний процес оцінки ризику яким була викрита підприємницька діяльність підприємства. З цього підмножини11 знову більшість (88%) інтегрували ризик цифрової безпеки в загальну оцінку ризиків. Була цілком така угода про розбіжності з точки зору особи, яка здійснює діяльність, що становить цифрова оцінка ризику безпеки. Це позитивна риса цього питання, як це демонструє багатогранний характер цифрового ризику безпеки та управління ним. Примітно, комбінація менеджерів бізнесу, IT-менеджерів або ризик-менеджерів виконували різні види діяльності. Дуже мало хто передає будь-яку з цих видів діяльності на зовнішнє замовлення, що може бути пов'язано з відносно великими підприємства-респонденти. Показник відносно низької частоти відповідей «Не знаю» що це чітко сформульоване питання з досить чітко окресленою та чітко визначеною відповіддю варіанти.

Також спостерігались великі розбіжності щодо частоти оцінювання з урахуванням можливих наслідків інцидентів цифрової безпеки, які можуть вплинути на діяльність підприємства. Знову ж таки, це позитивна риса питання, як це демонструє нюанс щодо способів управ-

ління різними підприємствами цифрової безпеки ризик. Більшість (58%) застосовували цю практику щороку. Незначна частина (14%) не знала і ще менша частка (6%) вводить власну частоту. Їхні відповіді («Раз на два місяці», «раз на півроку», «раз до цього часу», «постійно» та «спеціально»)) розглядаються як додаткові варіанти в майбутніх ітераціях інструменту опитування.

Модуль D: Цифрові практики зменшення ризиків безпеки

Протягом попереднього року більшість (81%) респондентів застосовували цифрові заходи безпеки в результаті оцінки цифрової безпеки. 8% не знали, тоді як 11% не знали. Це важливо, оскільки цей колектив 18% згодом не повинен був відповісти на наступне питання, яке задає питання про те, які заходи цифрової безпеки існували. Є хороший ймовірність існування таких заходів, хоча вони не були запроваджені через оцінка цифрової безпеки. Отже, ця частина їх управління цифровими ризиками безпеки процес не фіксується. Це слід змінити в наступних ітераціях опитування інструмент. Що стосується цілей самих заходів, між ними спостерігались великі розбіжності респонденти. Не дивно, що всі (100%) мали вжиті заходи з метою захисту діяльність проти потенційних загроз. Така переважна більшість може це припустити цей варіант має лише низьку корисність, але він встановлює еталон порівняння з іншими варіантами може бути оцінено. Цікавіше, що менше половини (42%) мали такі заходи мав на меті змінити ділову активність, тоді як більшість (80%) мали такі заходи спрямований на подолання інцидентів. Проблема з перекладом цього питання на програмну платформу, що використовується для Пілотне опитування полягало в тому, що респонденти були змушені надати відповідь на четвертий варіант ('Інше (вкажіть будь ласка)'). Розгублені респонденти відповіли «Не знаю» на цей варіант (75%), враховуючи, що їх змушували надавати інші варіанти, коли таких варіантів немає існував. Це питання повторюється у низці наступних питань у пілотному опитуванні. Можливо, ради простоти перефразуйте це питання, щоб запитати про що існували такі заходи (наприклад, ті, що передбачали захист від потенційні загрози, ті, що передбачають зміну ділової діяльності тощо), а не запитання для цілей заходів.

Існували великі розбіжності щодо частки респондентів, підприємства яких ділилися різними формами інформації із зовнішніми заці-

кавленими сторонами. Порівняно з 70% респонденти, які внутрішньо обмінюються інформацією між керівництвом та ІТ щодо цифрового ризику експозиція (показник В4), найвищі пропорції, з якими обмінювалася пов'язаною інформацією зовнішніми зацікавленими сторонами були «постачальники ІТ» (48%) та «постачальники страхових послуг» (45%). Тільки 8% респондентів поділилися інформацією з «Центрами обміну та аналізом інформації» 15. найменш імовірно, що зовнішні зацікавлені сторони отримували інформацію були «клієнтами» (22%). Це запитання виконує кілька корисних завдань, оскільки воно одночасно дає корисну інформацію та може також використовуватись як перевірка відповідей на інші запитання. Наприклад, більшість (45%) поділилися інформацією із постачальниками страхових послуг та, пізніше в ході опитування, подібною більшістю (55%) відповідають, що вони мають страховку, яка покриває ризик цифрової безпеки. Проблему з цим запитанням можна побачити у високій частці відповідей «Не знаю». З'ясування того, чому респонденти не знають відповідей на ці запитання, і чи є це можуть бути подолані в майбутніх змінах конструкції приладів обстеження, можуть бути розглянуті. це є можливо, що інформацією обмінюються люди з ІТ-відділу, але не з тими, хто працює в відділ управління ризиками (хто є бажаними респондентами пілотного опитування). Більше того, обов'язкова відповідь «Інше (будь ласка, вкажіть)» дала дві пропозиції, що може бути доречним для майбутніх ітерацій інструменту опитування: «інвестори / акціонери» та «рейтингові агентства». Однак це буде доречним лише у випадку, якщо існує висока частка підприємств, що публікуються в списку, серед населення респондентів.

Модуль Е: Практика передачі цифрових ризиків безпеки

Здається, підприємства-респонденти потрапляють в одну з двох широких груп: 1. ті, що (є усвідомлюючи, що вони) беруть участь у передачі ризику; або 2. ті, що цього не роблять. Подібні більшості респонденти використовували страхування (55%), інші юридичні договори (53%) або аутсорсинг (59%) передати цифровий ризик безпеки. Лише незначна частина (21%) використовувала гарантії для передачі ризику. Порівняно велика частка (26%) не знала, чи використовуються гарантії, які, можливо вказує на неоднозначність у визначенні цього терміну для респондентів.

З тих, хто не мав страховки, яка покривала б цифрові ризики безпеки, найпоширеніша Причинами цього не було те, що наявна політика не забезпечувала достатнього охоплення (50%). Дуже мало (3%) зазначили, що їм невідомо, чи існує таке покриття такого висвітлення не було в їхній країні. Багато респондентів мали кілька причини відсутності такого страхування (середнє = 2,13, медіана = 2, n = 30). Це підтримує поточний дизайн запитання, який дозволяє отримувати декілька відповідей, а не обмежувати відповіді на найважливіший. Двоє респондентів, коли їх змусили відповісти обов'язковий параметр «Інше (будь ласка, вкажіть)», вказував, що вони зараз проводять аналіз їх потреби та планується прийняти рішення протягом наступного року.

Серед тих, хто мав страховку, яка покривала ризики цифрової безпеки, фактичне покриття Ця політика була відносно однаковою. Дуже висока частка респондентів страхові поліси, які охоплювали варіанти, передбачені в інструменті опитування. Це може бути через відносно однаковий характер страхових полісів з точки зору покриття, яке вони зазвичай забезпечують. Попередмінно це може бути пов'язано з невеликою кількістю відповідей та деякими неоднозначність між деякими варіантами відповіді. Наприклад, може бути незрозуміло, наскільки «фінансовим збитки» відрізняється від «крадіжки та шахрайства». Найбільші розбіжності спостерігались у «репутації» збитків, що узгоджується з галузевою практикою, щоб зазвичай не покривати такі збитки.

Модуль F: Поінформованість про цифрове управління ризиками безпеки та навчання

В цілому значна частина когорти виконала низку поінформованості та навчання практики. Найчастіше ризики цифрової безпеки обговорювались на зустрічах бізнес-підрозділів (69%), після чого обов'язкове або факультативне навчання (61%) та включення посилань на ризик цифрової безпеки в трудових договорах (44%). Дуже мало (22%) забезпечили ефективність заохочення працівників, чиї дії знижують ризик цифрової безпеки. Варіація в відповіді на різні варіанти свідчать про те, що це корисне питання для розкриття різні практики управління цифровими ризиками безпеки на підприємствах.

З тих, хто проводив або обов'язкове, або факультативне навчання, майже всі надавали його директори (89%), керівники бізнес-ліній (95%), співробітники відділу безпеки (91%) та IT персонал відділу

(95%). Дуже мало (18%) надавали будь-яку форму навчання зовнішнім підрядники, хоча більша частка (31%) не знали, що говорить про те, що це може не є особливо значущим варіантом і може бути вилучений у наступних ітераціях інструмент опитування.

Заключне питання в інструменті опитування задає тим, хто не пройшов навчання Чому це так. Впали лише чотири респонденти ця підгрупа та їх відповіді мало що говорять про причини відмови від навчання. Це припускає, що це питання зайве і може бути вилучене з майбутніх ітерацій цього інструмент опитування.

Неповні відповіді

Тут подано короткі уявлення щодо відносно великої кількості неповних відповіді на пілотне опитування. Мета полягає у визначенні причин, чому ці відповіді не були завершено. Сподіваємось, що це послужить засобом для внесення змін до обстежити дизайн приладів у майбутньому і тим самим зменшити частоту неповних відповіді. Загалом було 311 неповних відповідей. З них 311 290 натиснули та увійшли до портал опитування, але не зареєстрував жодної відповіді на запитання. Ці респонденти можуть побачили очікуваний час на заповнення опитування (10-15 хвилин) і вирішили на цей момент у них не було такої кількості часу, щоб заповнити опитування. З решти 21 респондентів, які відповіли принаймні на одне запитання, 8 кинули в точно такий же момент: питання B1a. Ще 3-4 висадки або безпосередньо перед, або просто після цього питання. Ці питання відразу пішли за демографічним модулем, який закінчується низкою питань, спрямованих на оцінку цифрової інтенсивності / залежності від підприємство. Тобто у цих респондентів не було достатньо часу, щоб дістатися до основні питання в інструменті опитування.

Хоча неможливо визначити, скільки часу ці респонденти витратили на своє неповні відповіді на опитування, цей результат може припустити, що інструмент опитування такий, як він стенди занадто довгі, з точки зору часу, необхідного для відповіді, для добровільних відповідей без будь-яких форма компенсації. Здебільшого (72%) ці респонденти працюють на підприємствах з більш ніж п'ятьма тисячами працівників. Менеджер з управління ризиками на такому підприємстві, ймовірно бути натиснутою на час і, як результат, з більшою ймовірністю відповісти на коротке та стисле опитування інструмент. Не було

помітного переважання з точки зору географічного розташування Росії ні підприємство, ні його галузь. Якщо справді це момент, коли значна частина потенційних респондентів вирішує цього не робити продовжуючи опитування, це свідчить про те, що в майбутньому можна отримати більше відповідей використовуючи усічений інструмент опитування з максимум 5-7 питань.

Рекомендації щодо подальшого вдосконалення

Тут міститься рекомендації щодо подальшої роботи з метою вдосконалення вимірювання практики управління цифровими ризиками безпеки бізнесу. система вимірювань та інструмент обстеження, розроблені протягом цього OECP проект являють собою основні кроки вперед. Тим не менше, існує багато способів, за якими буде майбутнє зусилля можуть спиратися на ці інструменти, щоб продовжувати вдосконалювати вимірювання в цій галузі.

Покращення рівня відповіді на майбутні інструменти опитування

Рівень відповіді на пілотну програму опитування істотно різнився в залежності від ризику асоціації управління. Найвищий рівень відповіді спостерігався у BELRIM (Бельгія) з 18%. Загальний коефіцієнт відповіді становив приблизно 3%, що збільшується до 5% AIRMIC (Великобританія), який становив майже 50% респондентів опитування (1058 з 2602 одержувачів), видаляється. Є багато причин, чому рівень відповіді різнився, і, в деяких країнах був низьким. Перша і, ймовірно, найбільш суттєва причина була через пілота під час канікул у Європі. Само собою зрозуміло в ідеалі майбутні обстеження слід проводити в періоди року, коли респонденти частіше працюють, а тому частіше відповідають на опитування. Тим не менше, на рівні проектування обстеження можуть бути вжиті додаткові заходи для збільшення ймовірність виконаних відповідей незалежно від пори року, протягом якого проводилось опитування здійснюється. Вони пояснюються нижче та включають: зменшений перелік «ключових» показників; доповнення або вилучення питань або варіантів відповідей; та спрощена мова для непрофесійних респондентів.

Скорочений перелік «ключових» показників

Структура вимірювань навмисно обширна. Дотримуючись формату опитування моделі дозволяє підбирати або відкидати модулі, що стосуються конкретних проблем, залежно від потреб політики

у країнах ОЕСР. Однак, політики можуть хотіти мати мале знімки багатьох питань, що не є те, що модель форматування опитування легко дозволи. Більше того, велика кількість неповних відповідей пілота свідчить про це поточний інструмент повного опитування вимагає занадто багато бажаного часу респондентів їх повністю та / або точно заповнити. Щоб подолати цю ситуацію, можливо, можна вибрати один або кілька показників із кожен модуль та об'єднайте відповідні запитання у зрізаному інструменті опитування. вибір цих «ключових» показників повинен бути предметом більш суворого обговорення та результат, швидше за все, зміниться залежно від контексту-конкретних інтересів політиків розглянутий. Тим не менше, нижче пропонується набір показників, на які можуть претендувати усічений набір ключових показників.

Додавання або видалення запитань або варіантів відповідей

Аналіз визначив ряд можливих змін зроблений на основі відповідей пілоту для вдосконалення інструменту обстеження. Дещо додаткові варіанти відповіді можуть бути додані до певних питань, наприклад питання D2 міг скористатися опцією «акціонери», «інвестори» та / або «рейтингові агентства». Зміни такі, як це, слід робити відповідно до вірогідної сукупності респондентів. Наприклад, вищезазначені доповнення були б більш доречними, якщо б населення Росії респонденти складають значну частину публічно торгуючих компаній. Ще одне корисне доповнення може бути внесено в модуль А і може включати запитання респонденту, яку роль вони відіграють у своєму підприємстві. Це було б корисно для кращого інтерпретація результатів майбутніх опитувань, якщо вони включатимуть більше МСП чи охоплюватимуть більші компанії, які можуть не мати добре розвиненого відділу управління ризиками. Іншим варіантом може бути створення форка, за допомогою якого респонденти можуть мати ускладнене розуміння управління ризиками спрямоване одним шляхом, аналогічним чином складний словник управління ризиками, який використовується у питаннях, тоді як тих, що цим не є спрямували на шлях з більш простою, не фаховою лексикою. Останнім доповненням можуть бути питання, які викликають більш ґрунтовне розуміння того, чому підприємства здійснюють певну діяльність. Такі запитання можуть дати відповідне розуміння для розробка полі-

тики, спрямованої на підвищення обізнаності, навчання, страхування або інші практики управління ризиками.

З точки зору елементів, які слід вилучити з інструменту опитування, найважливіший з них буде обов'язковою опцією відповіді «Інше (будь ласка, вкажіть)», яка з'являється у запитаннях D1b, D2, E2, E3, E4 та F1c. Примушення респондентів відповісти на цей варіант, коли можуть не мати будь-якої іншої практики, щоб відповісти, додає значний і непотрібний час і зусилля навантаження. Це був артефакт програмного забезпечення, яке використовувалося для проведення пілота, хоча його слід відзначити присутність у тому випадку, якщо майбутні роботи намагатимуться спиратися на пілотне опитування інструмент у його поточному вигляді. Заключне запитання в інструменті опитування (F1c) задає питання навчання не проводилось для директорів чи керівників підприємств. Дуже мало респондентів (4 з 80 повних відповідей) повинні були відповісти на це питання, а коли вони відповіли, то відповіді між різними варіантами відповідей були відносно послідовними (тобто «ні», у тому числі для обов'язковий параметр. Якщо це питання потрібно зберегти, варіанти для відповіді, можливо, доведеться переглянути. У будь-якому випадку, враховуючи, що це питання було актуальним для так мало респондентів, можливо, його можна буде видалити без надмірної втрати корисності.

Спрощена мова для респондентів, які не є експертами

Бажаним респондентом інструменту пілотного опитування були менеджери ризику та вибірка населення через FERMA включало відносно велику кількість менеджерів ризику. Якщо інструменти опитування були надіслані вибірковій сукупності компаній, що включали більше МСП було б менш імовірно, що це зробив би конкретний менеджер з управління ризиками або відділ управління ризиками існувати. Це означало б, що респондент може мати проблеми з розумінням ризику словниковий запас управління, що використовується в інструменті опитування, та якість наступного відповіді будуть страждати. Корисна майбутня робота перекладе терміни управління ризиками на терміни, які були б більш доступними для не експертної аудиторії. Це дозволило б мати майбутнє інструмент опитування, який слід розробити для більшості населення підприємств. Однак, інструмент

опитування, спеціально націлений на менеджерів ризику, як і раніше залишатиметься корисним населення займає стратегічне становище на багатьох підприємствах, коли йдеться про ризик управління. Найкращим способом впоратися з цією ситуацією може бути впровадження «форкового підходу» в Модулі А, як пояснено вище.

Перехід від вимірювальної практики до моделі зрілості

Структура, розроблена в ході цього проекту, спочатку була задумана як спосіб для кращого вимірювання практики управління цифровими ризиками безпеки бізнесу, особливо МСП. Практики в сукупності дають короткий огляд загальної зрілості відповідного бізнесу (тобто зрілість як сукупність окремих практик). С рамки, що існують, і багато розумінь було зібрано протягом за два роки стало очевидним, що корисним внеском може бути адаптація або розширення цієї основи, яка б стала моделлю для оцінки цифрового управління ризиками безпеки зрілість бізнесу. Така модель може застосовувати ваги певні практики або рангові практики з точки зору певної метрики, такі як бажаність, важливість, ефективність тощо з огляду на цифрову інтенсивність, розмір та галузь підприємства, про яке йде мова. Однак процес розробки цієї моделі повинен був би уникнути ситуації, коли а з'являється нормативний погляд на те, що являє собою «зріле» чи «не зріле», що може призвести до генеруються дані, що підтверджують заздалегідь визначену концепцію зрілості. Можна провести порівняльний аналіз, за допомогою якого здійснюється управління цифровим ризиком безпеки практики підприємств зі схожими характеристиками (наприклад, однаковий розмірний клас, галузь та/або цифрові показники інтенсивності) оцінюються за рівних. Самі фактичні практики, і незалежно від того, представляють вони належний або необхідний рівень зрілості, це може бути визначається для окремих підприємств або від країни до країни. Якби цей показник зрілості поєднувати з інформацією про фактори ризику (тобто загрози, вразливості та інциденти), потенційно з інших надійних джерел (наприклад, антивірус компанії, постачальники технологій, комп'ютерні групи реагування на надзвичайні ситуації тощо), то політики змогли б скласти дуже детальне та складне уявлення про те, як добре підготовлений бізнес повинен ефективно управляти ризиками цифрової безпеки як цими ризиками еволюціонувати.

Розробка глибинних заходів

Ряд питань піддаються розробці глибинних вимірів певні аспекти, пов'язані з управлінням цифровим ризиком безпеки респондента підприємство. Термін «міра глибини» використовується для позначення заходів, що дозволяють оцінити витонченість конкретних практик на самому підприємстві. Це на відміну від чого можуть бути названі «показниками чисельності населення», які більше призначені для оцінки практики підприємство порівняно з деяким більшим населенням. Наприклад, дані, зібрані за допомогою питання A4, яке пов'язане з показником A5 «частка підприємств за цифровою інтенсивністю», забезпечити потенційну міру «глибини» цифрової інтенсивності респондента дев'ять різних цифрових технологій або їх використання. Так само питання B2c, що пов’язано з показником B2 частка підприємств, у яких діє політика Управління ризиками цифрової безпеки, збирає дані про дев'ять елементів політики цифрової безпеки може покрити. «Глибину» обох показників можна виміряти, виходячи з кількості елементи, якими підприємство володіє / використовує / включає їхню політику як частку сукупність можливих елементів.

Вимірювання інцидентів та їх економічний вплив

На попередньому етапі була розглянута можливість спеціального проекту модуль для збору даних про частоту та типи інцидентів цифрової безпеки, понесених підприємства респондента, а також оцінка їх економічного впливу. Це було вирішено не йти цим шляхом на цьому етапі, враховуючи суттєві методологічні проблеми, які страждають вимірювання в цій області (див. кінець першого розділу цього звіту для пояснення ці питання). У майбутній роботі можна було б переглянути методології, що використовуються в різних варіантах джерела даних для вимірювання інцидентів та їх економічного впливу. Такі джерела даних могли б включати минулі та існуючі опитування, постачальників антивірусів та безпеки, комп’ютерні аварійні ситуації групи реагування та національні системи повідомлень про інциденти як наслідок Директива GDPR / NIS в ЄС та зобов'язання щодо звітності, створені відповідно до подібних обов'язкових вимог вимоги щодо звітності в інших країнах OECP. Наявна робота OECP (2015b), IRT-System X (2016) та CRO Forum (2018) можуть надати корисні відправні точки.

Моделювання впливу цифрових бізнес-активів на економічне зростання країни за J-кривою продуктивності

Інформаційні технології загального призначення, в тому числі використання штучного інтелекту в бізнесі та інші цифрові бізнес-активи та їх перерозподіл за допомогою фінансових технологій, вимагають значних додаткових інвестицій, включаючи спільне інвестування, залучення додаткових фінансових ресурсів на винайдення нових цифрових бізнес-активів, цифрових бізнес-продуктів, бізнес-моделей і людського капіталу. Ці додаткові інвестиції зазвичай є нематеріальними і погано оцінюються в національних рахунках, навіть якщо вони створюють цінні активи для фірми. В такому випадку, зважаючи на складність їх обліку та статистичного представлення – виникає проблема і в розробці адекватної економіко-математичної моделі оцінювання їх впливу на темпи економічного зростання певної держави. Тому розроблено модель, яка показує, як недостатнє відображення в облікових реєстрах та національних рахунках саме діджиталізованих бізнес-активів призводить до недооцінки зростання продуктивності в перші роки нового такого цифрового бізнес-активу, і як пізніше, коли вигоди від нематеріальних інвестицій будуть отримані та визначені, зростання продуктивності буде переоцінено на вплив цих раніше не облікованих цифрових активів. Ця економіко-математична модель генерує J-криву продуктивності, яка може пояснити зниження продуктивності, яке часто супроводжує появу нових інформаційних технологій, які використовуються в бізнесі, а також підвищення продуктивності пізніше після застосування на практиці таких цифрових активів.

Наявність такого роду нематеріальних інвестицій як цифрові бізнес-активи та фінансові технології є однією з причин, чому може виникнути парадокс Солоу, а саме, коли з'являється чи застосовується новий вид цифрових бізнес-активів чи фінансових технологій, настане період, можливо, досить тривалий, протягом якого виміряні ресурси будуть спрямовані, а вимірюваний їх вплив на економічне зростання певної країни упущений, коли створення нових, невиміряних витрат, які доповнюють вже виміряні та обліковані нематеріальні активи. Наприклад, інформаційні технології, новітні цифрові бізнес-активи, фінансові технології, які активно рухають британську промисловість призвели до так званої «паузи Енгельса», тобто мало не півстолітнього

періоду виключного накопичення капіталу, промислових інновацій та стагнації заробітної плати (Е.МаГреттен [27]). Пізніше, коли відбулась тотальний перехід на Індустрію 4.0 та 5.0, промисловості цієї країни знадобилося ціле покоління, щоб природа заводських макетів була заново винайдена, щоб повністю використати переваги нової технології [28; 29]. Солоу висвітлив подібне явище приблизно через два десятиліття в епоху ІТ, де вимірювальний аспект цього явища названо J-кривою продуктивності. Оскільки фірми приймають у роботу свого бізнесу нові і нові цифрові бізнес-активи та фінансові технології, зростання загальної факторної продуктивності спочатку буде недооцінене, оскільки капітал і праця використовуються для накопичення невиміряних запасів нематеріального капіталу у нових формах цифрових бізнес-активів (діджиталізовані активи). Пізніше виміряне зростання продуктивності переоцінює справжнє зростання продуктивності, тому що послуги капіталу, що надходять із цих прихованих нематеріальних запасів у вигляді діджиталізованих активів, дають вимірюваний вплив на економічне зростання тієї чи іншої країни. Таким чином, похибка в виміряному зростанні загальної факторної продуктивності має форму J-кривої, спочатку спадає, тоді як норма інвестицій в невиміряний капітал перевищує ставку інвестицій в інші типи капіталу, а потім зростає, оскільки зростаючі нематеріальні запаси у нових формах діджиталізованих активів починають робити внесок у вимірюване виробництво. У довгостроковій перспективі, коли нематеріальні інвестиції та запаси капіталу досягають стабільних темпів зростання, скоригована на прибуток вартість невиміряних потоків нематеріального капіталу у формі цифрових бізнес-активів та фінансових технологій (які знаходяться в очікуванні) наближається до вартості початкових невиміряних інвестицій. Це означає, що деякі впливи помилкового вимірювання на зростання продуктивності можуть зберігатися навіть у довгостроковій перспективі.

Удосконалимо підходи Бріньольфссона [30; 31]. Припустимо, що сукупна (економічна чи галузева) виробнича функція є добутком нейтральної за Хіксом загальної факторної продуктивності A та функції $F(\cdot)$, яка слабо зростає і має постійну віддачу від масштабу у витратах K і L (кожен потенційно є векторами). Далі припустимо, що ринки є абсолютно конкурентними. Тоді

$$Y = A\mathrm{F}(K, L) \quad (1)$$

де Y – це випуск продукції (ВВП), який можна або спожити, або інвестувати як капітал. Якщо гнучкі ціни на капітал і фактори факторів r і w дорівнюють сукупній вартості граничного продукту капіталу та праці, ми маємо наступне (g означає зростання ставка):

Тепер припустимо, що існують невиміряні нематеріальні капітальні інвестиції та потоки капітальних послуг, такі як цифрові бізнес-активи та фінансові технології, але вони випливають із накопичених нематеріальних запасів. Незважаючи на те, що вони не виміряні, ці нематеріальні активи є справжніми результатами, коли вони створені як інвестиційні товари, і, коли вони впроваджені, то однозначно входять до функції сукупного виробництва. Використовуючи A^* для позначення виробничої функції, яка включає невиміряні запаси нематеріального капіталу, ми маємо

$$Y + \phi I_{\mathrm{da}} = A^*\mathrm{F}^*(K, \mathrm{DA}, L) \quad (2)$$

Ми можемо записати зростання загальної факторної продуктивності в цій нематеріально-інклюзивній економіці так:

$$g_a = \left(\frac{Y}{Y + fI_{da}}\right)\left(g_Y - \left(\frac{rK}{Y}\right)g_K - \left(\frac{r_{da}DA}{Y}\right)g_{da} - \left(\frac{wL}{Y}\right)g_L\right) + \left(\frac{fI_{da}}{Y + fI_{da}}\right)g_I \quad (3)$$

Різниця між залишками Солоу, що випливають із цих двох контекстів вимірювання, з'ясовує джерела невірного вимірювання зростання продуктивності, коли існують нематеріальні активи, але застосовуються стандартні методи вимірювання. Зміна термінів дає вираз, який пропонує інтуїтивне розкладання того, як нематеріальні активи призводять до різниці між виміряним і фактичним зростанням продуктивності:

$$\Delta = g_a - g_{a^*} = \left(\frac{\phi I_{da}}{Y + \phi I_{da}}\right)\left(g_Y - \left(\frac{rK}{Y}\right)g_K - \left(\frac{wL}{Y}\right)g_L - g_{I_{da}}\right) + \left(\frac{Y}{Y + \phi I_{da}}\right)\left(\frac{r_{da}DA}{Y}\right)g_{da} \quad (4)$$

Перший доданок у правій частині (6) є неправильним вимірюванням продуктивності через той факт, що стандартний показник зростання продуктивності не враховує нематеріальні інвестиційні товари як випуск, коли вони виробляються.

$$Y_t = (1 - \eta_t)Y_t^* \quad (5)$$

$$\eta_t = \frac{\phi_t IDA_t}{Y_t + \phi_t IDA_t} = \frac{Y_t^* - Y_t}{Y_t^*}$$

Це призводить до того, що виміряне зростання продуктивності занижує справжнє зростання продуктивності (тобто робить Δ від'ємним). Другий термін відображає перевищення справжньої продуктивності через той факт, що стандартний залишковий показник Солоу приписує продуктивності результати, отримані нематеріальними ресурсами, а не ці витрати. Цей термін зважується за часткою виміряної продукції в загальному випуску. Чи є Δ додатним чи негативним, залежить від відносного розміру цих двох членів.

$$\Delta = \left(\frac{dY}{Y} - \frac{dY^\star}{Y^\star}\right) + \left(\left(\frac{rK}{Y^\star}\right)\left(\frac{dK}{K}\right) - \left(\frac{rK}{(1-\eta_t)Y^\star}\right)\left(\frac{dK}{K}\right)\right) +$$

$$+ \left(\left(\frac{wL}{Y^\star}\right)\left(\frac{dL}{L}\right) - \left(\frac{wL}{(1-\eta_t)Y^\star}\right)\left(\frac{dL}{L}\right)\right) + \left(\frac{r_{DA}DA}{Y^\star}\right)\left(\frac{dDA}{DA}\right)$$

Реранжуючи з рівняння (5) отримаємо:

$$\Delta = -\eta_t \left(\left(\frac{dK}{Y}\right)g_K + \left(\frac{wL}{Y}\right)g_L\right) + (1-\eta_t)\left(\frac{r_{DA}DA}{Y}\right)g_{DA} + g_{(1-\eta_t)} \qquad (6)$$

Підставляючи ці відповідні вирази і перераховуючи Δ, як у (6), виходить:

$$\Delta = \left(\frac{Y}{Y+\phi I_{DA}}\right)\left(\left(\frac{r_{DA}DA}{Y}\right)\left(g_{DA} - g_K\right) - \left(\frac{\phi I_{DA}}{Y}\right)\left(g_{I_{DA}} - g_K\right)\right) +$$

$$+ \left(\frac{\phi I_{DA}}{Y+\phi I_{DA}}\right)\left(g_Y - \left(\frac{wL}{Y}\right)g_L - \left(1 - \frac{wL}{Y}\right)g_K\right) = (1-\eta)\left(\frac{r_{DA}}{Y}\right)\left(g_{DA} - g_K\right) + \eta\left(g_A - g_{I_{DA}}\right) \qquad (7)$$

А рівняння загального економічного зростання продуктивності тепер буде таким:

$$g_{A^*} = \left(\frac{Y}{Y+\phi I_{DA}}\right)\left[g_Y - \left(\frac{wL}{Y}\right)g_L - \left(1 - \frac{wL}{Y}\right)g_K - \left(\frac{r_{DA}DA}{Y}\right)\left(g_{DA} - g_K\right) + \left(\frac{\phi I_{DA}}{Y}\right)\left(g_{I_{DA}} - g_K\right)\right] \qquad (8)$$

Рівняння (7) і (8) описують розбіжності, використовуючи *Y* як виміряний випуск товарів, робіт та послуг у країні і *gY* як виміряний приріст виробництва в цій країні.

Щоб коригувати виміряне зростання продуктивності для цифрових бізнес-активів та фінансових технологій (складових нематеріальних активів) на практиці, потрібно оцінити нематеріальні інвестиції. З точки зору рівняння (9), нам потрібна міра вартості нематеріальних інвестицій ϕIDA.

$$g_Y = \left(\frac{wL}{Y}\right) g_L + \left(1 - \frac{wL}{Y}\right) g_K - \left(\frac{\phi I_{DA}}{Y}\right)\left(g_{I_{DA}} - g_K\right) + \left(\frac{Y + \phi I_{DA}}{Y}\right) g_{A^*} \quad (9)$$

і темпи зростання інвестицій $gIDA$ можна взяти з ряду спостережуваних інвестицій та ВВП. Одним із способів оцінки нематеріальних інвестицій є припущення, що кожна одиниця виміряних інвестицій є спостережуваним компонентом об'єднаної інвестиційної одиниці, яка також включає нематеріальні активи. Неоцінені нематеріальні корелюють активи на фірмі.

Регресія ринкової вартості на рівні фірми для вимірюваних видів капіталу, які, як очікується, будуть мати сильну кореляцію з прихованими нематеріальними активами, може кількісно визначити цю нематеріальну тіньову вартість.

$$\text{ВВП}_{ijt} = \beta_0 + \beta_1 \text{ЗагальніАктиви}_{it} + \beta_2 \text{капіталовкладенняДА}_{it} + \eta_{it} + \varepsilon_{it}$$

Щоб оцінити величину нематеріальних інвестицій у формі цифрових бізнес-активів та фінансових технологій, використовуємо підхід для отримання тіньових значень нематеріального капіталу шляхом порівняння спостережуваних інвестицій фірм з їх ринковою капіталізацією. Використовуємо їх для створення оцінок часових рядів окремих нематеріальних запасів, пов'язаних з інвестиціями в цифрові бізнес-активи та фінансові технології протягом 1961–2020 років за даними офіційної статистики за національними рахунками різних країн. Таким чином отримано базові показники продуктивності, чисті запаси капіталу для вимірюваних різновидів капіталу, включаючи цифрові бізнес-активи та фінансові технології, а також інвестиції цих різновидів капіталу, ринкову вартість фірми *i* в галузі *j* на момент *t*.

Розроблена модель може використовуватись для емпіричного аналізу історичних ролей нематеріальних активів, пов'язаних з дослідженнями та розробками, програмним забезпеченням та комп'ютерним обладнанням та іншими цифровими бізнес-активами та

фінансовими технологіями. Під час апробації розробленої моделі спостерігається значні й постійні ефекти J-кривої продуктивності для програмного забезпечення та фінансових технологій, та для комп'ютерного обладнання в меншій мірі. Скоригований показник нематеріальних активів на оцінену вартість цифрових бізнес-активів та фінансових технологій, які не обліковуються, на 11,3% вищий, ніж офіційні показники на кінець 2020 року, і на 15,9% вищий за офіційні показники на кінець 2021 року. В розробленій моделі також оцінено вплив результатів використання такого діджиталізованого бізнес-активу як штучний інтелект, та яким чином штучний інтелект пов'язаний із оцінкою нематеріального капіталу і як він зараз може впливати на виміряну продуктивність. В результаті апробації розробленої в даній статті моделі отримано результат, що і активи, пов'язані із використанням штучного інтелекту в бізнесі є незначними, але такими, які постійно зростають.

Список використаних джерел:

1. OECD Working Party on Indicators for the Information Society. OECD Working Party on Indicators for the Information Society. Information Economy Product Definitions based on the Central Product Classification System (version 2). 2008. URL: http://www.oecd.org/science/sci-tech/42978297.pdf (дата звернення: 08.08.2023).

2. Inaba T., Squicciarini M. ICT: A new taxonomy based on the international patent classification. *OECD Science, Technology and Industry Working Papers*. 2017. No. 2017/01. DOI: https://doi.org/10.1787/ab16c396-en (дата звернення: 10.08.2023).

3. OECD. Trade Facilitation and the Global Economy. Paris : OECD Publishing, 2018. DOI: https://doi.org/10.1787/9789264277571-en (дата звернення: 03.08.2023).

4. OECD. Services Trade Policies and the Global Economy. Paris : OECD Publishing, 2017. DOI: https://doi.org/10.1787/9789264277571-en (дата звернення: 10.08.2023).

5. Ferencz J. The OECD Digital Services Trade Restrictiveness Index. *OECD Trade Policy Papers*. 2019. No. 221. DOI: https://doi.org/10.1787/16ed2d78-en (дата звернення: 02.08.2023).

6. A taxonomy of digital intensive sectors / F. Calvino et al. *OECD Science, Technology and Industry Working Papers*. 2018. No. 2018/14. DOI: https://doi.org/10.1787/f404736a-en (дата звернення: 09.08.2023).

7. Risk Management of Digital Information: A File Format Investigation / G. W. Lawrence et al. Washington, D.C. : Council on Library and Information Resources, 2000.

8. World Corporate Top R&D Investors: Industrial Property Strategies in the Digital Economy : A JRC and OECD common report / T. Daiko et al. Luxembourg : Publications Office of the European Union, 2017. URL: https://www.oecd.org/sti/world-top-rd-investors.pdf (дата звернення: 17.08.2023).

9. Edvards J. Building a Smart Factory with AI and Robotics. *Robotics Business Review*. URL: https://www.roboticsbusinessreview.com/wp-content/uploads/2018/02/RBR_BuildingAI_WP3.pdf (дата звернення: 09.08.2023).

10. Harris E., Younggren J. N. Risk management in the digital world. *Professional Psychology: Research and Practice*. 2011. Vol. 42. No. 6. P. 412–418. URL: https://psycnet.apa.org/doi/10.1037/a0025139 (дата звернення: 11.08.2023).

11. Ciborra C. Imbrication of representations: Risk and digital technologies. *Journal of Management Studies*. 2006. Vol. 43. No. 6. P. 1339–1356.

12. Gartner, Inc. Gartner Says Solving 'Big Data' Challenge Involves More Than Just Managing Volumes of Data. *Business Wire*. 2011. URL: https://www.businesswire.com/news/home/20110627005655/en/Gartner-Says-Solving-Big-Data-Challenge-Involves-More-Than-Just-Managing-Volumes-of-Data (дата звернення: 10.08.2023).

13. Ferracane M., Lee-Makiyama H., van der Marel E. Digital Trade Restrictiveness Index. European Center for International Political Economy. 2018. 137 p. URL: https://ecipe.org/wp-content/uploads/2018/05/DTRI_FINAL.pdf (дата звернення: 09.08.2023).

14. OECD. OECD Guide to Measuring the Information Society. Paris : OECD Publishing, 2011. DOI: https://doi.org/10.1787/9789264113541-en (дата звернення: 09.08.2023).

15. OECD. Trade and cross-border data flows : Preliminary Draft. Paris : OECD Publishing, 2018.

16. OECD. Working Party on International Trade in Goods and Trade in Services Statistics : Result of the 2018 WPTGS Stocktaking Questionnaire. 2018.

17. OECD. Measuring Digital Transformation: A Roadmap for the Future. Paris : OECD Publishing, 2019.

18. OECD. Digital Innovation: Seizing Policy Opportunities. Paris : OECD Publishing, 2019.

19. Suntsova O. The definition of smart economy and digital transformation of business in the concepts Industry 4.0 and 5.0. *Technology audit and production reserves*. 2022. Vol. 4. No. 66. P. 18–23. DOI: https://doi.org/10.15587/2706-5448.2022.265105 (дата звернення: 09.08.2023).

20. Suntsova O. Econometric and digital business transformation in industry 4.0 and 5.0 concepts. *Financial and credit systems: prospects for development*. 2022. Vol. 2. No. 5. P. 36–47.

21. OECD. Understanding Enhanced Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies. Paris : OECD Publishing, 2019.

22. OECD. Data Driven Innovation: Big Data for Growth and Well-being. Paris : OECD Publishing, 2015.

23. Coyle D., Nguyen D. Cloud Computing and National Accounting : ESCoE Discussion Paper 2018-19. Economic Statistics Centre of Excellence, 2018.

24. Cisco public. Cisco Visual Networking Index: Forecast and Trends, 2017–2022 : White Paper. 2019. URL: https://twiki.cern.ch/twiki/pub/HEPIX/TechwatchNetwork/HtwNetworkDocuments/white-paper-c11-741490.pdf (дата звернення: 09.08.2023).

25. Сунцова О. О. Розвиток рекреаційно-туристичного потенціалу регіону за рахунок впровадження дорадницько-консалтингових проектів. *Вісник Київського національного університету технологій та дизайну. Серія Економічні науки*. 2016. № 6. С. 32–39.

26. Suntsova O. Digitalization and globalization in taxation in the context of modern practice of introduction of blockchain technologies. *Financial and credit systems: prospects for development*. 2021. Vol. 3. No. 3. P. 27–35.

27. McGrattan E. R. Intangible Capital and Measured Productivity : Working paper. 2017. URL: https://www.nber.org/system/files/working_papers/w23233/w23233.pdf (дата звернення: 10.08.2023).

28. Сунцова О. О. Вплив цифрових бізнес-активів та фінансових технологій на економічне зростання країни. *Інфраструктура ринку*. 2022. № 68. С. 254–260.

29. Сунцова О. О. Фінансові технології як складова цифрової економіки: тенденції в реаліях пандемії COVID-19. *Економічний вісник. Серія: фінанси, облік, оподаткування*. 2021. № 7. С. 161–175. DOI: https://doi.org/10.33244/2617-5932.7.2021.161-175 (дата звернення: 11.08.2023).

30. Brynjolfsson E., Rock D., Syverson C. Artificial Intelligence and the Modern Productivity Paradox: A Clash of Expectations and Statistics. University of Chicago Press, 2018. URL: https://www.nber.org/system/files/working_papers/w24001/w24001.pdf (дата звернення: 09.08.2023).

31. Saunders A., Brynjolfsson E. Valuing Information Technology Related Intangible Assets. *Mis Quarterly*. 2016. Vol. 40. No. 1. P. 83–110.