In conclusion, I can say that at the end of March 2018 in Buenos Aires, Argentina, the G20 summit was held, a group of 20 major economies of the world. Regulation of the cryptocurrency has become one of the main topics discussed among the representatives of states. Participants of the G20 recognized that, given the current economic situation, citizens have the right to use cryptocurrencies. In addition, regulators are aware that the adoption of digital money will help governments improve the welfare of the population. Ministers also agreed that the traditional economy is going through a transition process and it is already impossible to separate digital technologies from it. The future has already come.

References

1. Nathaniel Popper, Digital gold. 2015.

2. Alan T. Norman, Cryptocurrency Investing Bible: The Ultimate Guide About Blockchain, Mining, Trading, ICO, Ethereum Platform, Exchanges, Top Cryptocurrencies for Investing and Perfect Strategies to Make Money. 2018.

3. Chris Burniske,. Cryptoassets : The Innovative Investor's Guide to Bitcoin and Beyond by Chris Burniske and Jack Tatar. 2017.

Валентина Лук'янова
д.е.н., професор
завідувач кафедри економіки підприємства і підприємництва
Хмельницький національний університет

РИЗИКИ ТА ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВ

Економічна система все більше стає відкритою і відповідно уразливою до зовнішніх ризиків і загроз. Будь-яке підприємство стає все більш залежним від змін умов зовнішнього середовища не лише країни відповідної локації, але й світової економіки.

Метою розгляду у нашій статті є детальний аналіз із виявленням груп факторів ризику бізнес-середовища функціонування і загроз економічній безпеці підприємств з акцентом на інформаційну складову.

В основу нашого дослідження покладено аналітичні спостереження німецької фінансової транснаціональної корпорації Allianz SE (щорічно опубліковані у Allianz Global Corporate & Specialty (AGCS). Основним напрямком діяльності компанії є страхування. Станом на 2013 рік, це найбільша у світі страхова компанія, 11 за величиною фінансова група та 25 найбільша компанія за оцінкою журналу Forbes. Також це найбільша фінансова компанія за обсягом доходу, станом на 2012 рік. Група Allianz присутня у більш ніж 70 країнах на 5 континентах (в т.ч. і в Україні). Майже 140 тис. співробітників обслуговують близько 88 мільйони клієнтів [1].

Спостереження базуються на ґрунтовному аналізі близько 2000 експертами із 80 країн ризиків і загроз, що виділяють ризик-менеджери для успішного функціонування бізнесу у різних країнах світу. Найперше експерти оцінюють ризики і загрози безпеці підприємств з точки зору їх імовірності та величині збитків (прямих і непрямих втрат) [2].

За даними експертів [2] збої у виробництві ось уже шостий рік займають верхній рядок серед найважливіших ризиків в Європі, Азіатсько-Тихоокеанському регіоні, на Близькому і Середньому Сході (таблиця 1). Цей ризик, на жаль, властивий будь-якому підприємству незалежно від обсягів бізнесу. За даними опитування експертів, кібер-інциденти вперше названі в числі найбільш шокуючих факторів, що сприяють збоям у виробництві, в той час як самі збої у виробництві стали, на їхню думку, найбільш вагомою причиною втрат після кібер-інцидентів. Згідно з даними Cyence Risk Analytics, в разі недоступності хмарного сервісу у постачальника хмарних послуг, що триває більше 12 годин, збитки можуть скласти 850 млн. дол. в Північній Америці і 700 млн. дол. в Європі, виходячи з того, що від

недоступності до інформації постраждає 50 тис. компаній трьох різних сфер (фінанси, охорона здоров'я і роздрібна торгівля) в кожному регіоні [2].

Таблиця 1

Найбільші ризики і загрози бізнесу

Вид ризику (загроза)	Рейтинг, %				
	2014 р.	2015 р.	2016 р.	2017 р.	2018 р.
Збої у виробництві	43	46	38	37	42
Кіберзагрози	12	17	28	30	40
Техногенні аварії	24	27	16	16	20
Репутаційні ризики	15	16	18	13	13
Технологічні зміни	10			12	15

Кіберзагрози продовжують підніматись в рейтингу і у 2018 р. є другим за важливістю ризиком для підприємств (таблиця 1). П'ять років тому, за оцінками експертів [2], вони знаходилися лише на 15-му місці. Такі загрози, як порушення даних, хакерські атаки або ж збої у виробництві внаслідок кібер-інциденту підтверджують, що це головний ризик для бізнесу в 11 досліджуваних країнах, а також на Американському континенті, і другий за значимістю ризик в Європі та Азіатсько-Тихоокеанському регіоні. Він також є самим недооціненим ризиком в довгостроковій перспективі.

Нещодавні інциденти, пов'язані з появою програм-вимагачів WannaCry і Petya, призвели до значних збитків великого числа компаній. Інша програма-вимагач Mirai і масштабна розподілена атака типу «відмова в обслуговуванні» (DDoS) на ключові інтернет-платформи і сервіси в Європі і Північній Америці наприкінці 2016 року вписуються у зростаючу тенденцію – появу "кібер-ураганів". Хакери можуть вплинути на функціонування великої кількості підприємств, вибравши в якості мети, наприклад, загальні елементи інтернет-інфраструктури, від яких вони залежать. Ця тенденція, швидше за все, збережеться і в подальшому. Заходи щодо захисту даних знову повернулися в центр уваги після масштабних порушень в США. Вступ в силу Загального регламенту щодо захисту даних (GDPR) по всій Європі в травні 2018 року зробить перевірки ще більш ретельними.

Дані Барометра ризиків Allianz показують, що стурбованість кібер-загрозами серед компаній сегмента малого та середнього бізнесу зростає. Зокрема, для невеликих компаній цей ризик перемістився з шостого на друге місце, а для середніх компаній – з третього на перше місце рейтингу [2]. Найбільш високі місця в рейтингу загроз кібер-інциденти займають серед компаній сегмента Розваги і Медіа, компаній, що надають фінансові послуги, а також компаній, що відносяться до сегменту технологій і телекомунікації.

Нові технології як фактор ризику теж зростають за рейтингом. Вони є другим найбільшим довгостроковим ризиком, поступаючись лише кібер-інцидентам, з якими тісно взаємопов'язані. Уразливість автоматизованих, автономних і самонавчальних машин до відмови або до дій кібер-зловмисників буде в майбутньому зростати, що може призвести до значних порушень критичної інфраструктури. Незважаючи на те, що в майбутньому число незначних збитків, пов'язаних з автоматизацією і послабленням моніторингу, може скоротитися, на зміну їм можуть прийти більш значні втрати. Підприємствам потрібно бути готовим до нових сценаріїв несення відповідальності, поява яких викликано описаним вище переходом відповідальності від людини до машини або до виробника програмного забезпечення. Це зробить покладання відповідальності і надання страхового покриття для такої відповідальності більш складною справою.

Інший недооцінений різновид технологічних ризиків для таких країн як Україна – це зростання технологічного розриву у економічному розвитку, технологічне відставання і відповідні наслідки не лише в економічній сфері, але й технічній грамотності населення, соціальному розвитку, екологічним загрозам тощо.

Репутаційні втрати (13% у 2018 р.) – основна причина економічних втрат для підприємств які поряд з кіберризиками є загрозами інформаційної безпеки бізнесу. На жаль, ці два види ризиків тісно переплелись і часто їх вадко відокремити.

Отже, можна зробити висновок, що з одного боку важко виділити дію окремих чистих видів ризиків і загроз на підприємницьку діяльність, а з іншого – значну потребу до збільшення інформаційної безпеки діяльності підприємства, що відображена не лише в кіберзагрозах, але й ризиках збоїв у виробництві, репутаційних та технологічних ризиках та ін.

Список використаних джерел

1. [Електронний ресурс]. – Режим доступу: https://www.allianz.com/en/about_us/who_we_are/at-a-glance/

2. «Барометр рисков». Allianz назвал глобальные риски компаний в 2018 году. [Електронний ресурс]. – Режим доступу: http://sb-malakut.com.ua/barometr-riskov-allianz-nazval-globalnye-riski-kompanij-v-2018-godu

Володимир Муравський
к.е.н., доцент
Тернопільський національний економічний університет,
Василь Муравський
викладач
Тернопільський національний економічний університет

МЕРЕЖЕВА СТРУКТУРА АВТОМАТИЗОВАНОЇ БУХГАЛТЕРІЇ ПІДПРИЄМСТВА

Розвиток новітніх комп’ютерно-комунікаційних технологій та глобалізація економічних процесів призвела до виникнення нових типів облікових структур. Значної популярності в умовах розвитку комунікаційних технологій набула мережева організаційна структура. Мережеву організацію діяльності пов’язують із синергетичною інтеграцією групи підприємств, які паралельно здійснюють реалізацію продукції (робіт. послуг) через традиційні ринкові канали і механізми електронної комерції, можуть розташовуватися в різних територіальновіддалених місцях, але обов’язково об’єднані для досягнення спільної мети. Мережеві компанії охоплюють функціонування декількох фірм або їх структурних підрозділів з формуванням ефективних комунікацій на основі договірних відносин. Значна кількість структурних елементів в організації діяльності мережевих компаній визначає певну специфіку обліку, що пов’язана з активним інформаційним обміном між етапами автоматизованої обробки даних. Іншими словами, первинна або частково оброблена інформація може тривалий час мігрувати між обліковими фахівцями різних фірм, які входять в мережу. Завершальним етапом мережевих комунікацій є консолідація звітності з відправкою її зацікавленим особам та інституціям.

Оскільки мережева структура організації діяльності передбачає об’єднання декількох підприємств, її екстраполяція на малі суб’єкти господарювання видається недоцільною. Тобто, складні моделі управління неефективно застосовувати в діяльності невеликих підприємств з незначною кількістю працівників. Проте завдяки перевазі комп’ютерно-комунікаційної форми щодо вільної масштабованості й адаптованості до умов діяльності, мережева структура організації актуальна і для малих підприємств, які паралельно випускають декілька видів продукції, реалізовують товари через мережу Інтернет, відкривають філії, задіюють різні маркетингові канали просування товарів тощо. Багатоаспектність діяльності є визначальним чинником вибору організаційної структури мережевого типу, що потребує врахування динамічних змін умов внутрішнього та зовнішнього середовища. Як доводить М. М. Шигун, мережеві структури поділяються на