3. Digital transformation: The CFO’s role [Електронний ресурс] // McKinsey & Co. – 2019. – Режим доступу до ресурсу: https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/digital-transformation-the-cfos-role.
4. Кравченко О. О. Поведінкові аспекти управління корпоративними фінансами / О. О. Кравченко, В. В. Приймук. // Ефективна економіка. – 2019. – №10. – С. 147–153.
5. Geetanjali P. Sectoral Analysis of Factors Influencing Dividend Policy: Case of an Emerging Financial Market [Електронний ресурс] / P. Geetanjali, R. Shailesh // Journal of Risk and Financial Management. – 2019. – C.1-18 –
6. Режим доступу до ресурсу: https://www.mdpi.com/1911-8074/12/3/110/pdf.

УДК 330.131

***Яценко І.В.***
*аспірант*
*Університет державної фіскальної служби України*

**Кіберризик як сучасне явище на фінансових ринках**

З активним розвитком цифрових послуг відповідальність бізнесу за зберігання, використання, обробку, контроль за конфіденційністю персональних даних суттєво зросла. Дійсно, новітні ризики та недопрацювання в роботі з великими масивами персональних даних обертаються величезними штрафами, витратами на відновлення і захист ділової репутації. Трансформаційні зрушення в економіці щодо всезагальної цифровізації характеризуються як позитивними, так і негативними аспектами, які, насамперед, пов'язані з інформаційною безпекою. Звичайно Україна не є виключенням у списку країн, для яких властивими є кібер-інциденти.

Дійсно, кіберзлочинність в останні роки стає практично буденним явищем. В інформаційних релізах часто посідає інформація про зникнення великих сум з рахунків найбільших світових банків або про затримання чергового хакера. А

такі словосполучення як «кібератаки», «кібервійська», «кіберпростір» увійшли в повсякденний вжиток будь-якого економічного агента. Говорячи про кіберризик зазначимо, що – це «ризик, пов'язаний з використанням комп'ютерного обладнання та програмного забезпечення як в місцевих (локальних) мережах, так і в глобальній інтернет-мережі; в розрахунково-платіжних системах, в системах інтернет-торгівлі і в промислових системах управління. Також це ризик, пов'язаний з накопиченням, зберіганням і використанням особистих персональних даних» [1, с. 422].

Зауважимо, що особлива схильність фінансових установ до кібер-ризику пояснюється їх залежністю від критичних інфраструктур та взаємозв'язаних мереж. До критичних інфраструктур фінансового ринку відносимо платіжні та розрахункові системи, торгові платформи, центральні депозитарії цінних паперів та центральні контрагенти. Їх ідентифікація як «критична інфраструктура» пояснюється тим, що вони представляють собою системний вузол, а тому будь-яка реалізована атака одномоментно провокує негативні наслідки для широкого кола учасників фінансових ринків.

Порушення функціонування інфраструктури фінансового ринку або набору великих фінансових установ може зумовлювати суттєвий вплив на рівень концентрації ризику. Так, якщо порушується безперервність функціонування платіжних та розрахункових систем, учасники ринку не зможуть обробляти операції, а отже, піддаватимуться ризику ліквідності та платоспроможності. Аналогічно, центральні контрагенти повинні регулярно оцінювати вплив подій, які можуть бути результатом кібератаки та здатні зумовлювати збої у рамках клірингової діяльності.

До речі, з урахуванням певного набору інцидентів, пов'язаних з порушенням даних, а також вступу в силу нового закону про захист персональних даних на території ЄС та інших країн кіберризики стали ключовою небезпекою для бізнесу у 2019 році та наступні роки [2]. Кібер-інциденти сьогодні обходяться компаніям в суму близько 600 млрд євро в рік, в той час як в 2014 році ця цифра становила 445 млрд євро [2]. Це в три рази

вище, ніж сума збитків від природних катаклізмів за останні 10 років, склала 208 млрд євро. Кібер-злочинці використовують все більш інноваційні підходи для крадіжки даних, вчинення шкідливих дій або фінансового вимагання. Зростає і число кіберзагроз на державному рівні, а також з боку хакерських організацій, об'єктом уваги яких стають провайдери критичної інфраструктури або ж комерційна інформація компаній.

Загалом, переконані у тому, що наразі кожен сектор економіки повинен володіти механізмом попередження негативних викликів, які надходять із віртуального середовища. У цьому аспекті нам видається доречним до вирішення цієї проблеми залучити інститут аудиту, що полягатиме у розширені функціоналу аудиторів публічних компаній та перевірці ними, окрім фінансової звітності, також і достовірності оприлюдненої ними інформації про кібербезпеку. Відмітимо, що подібні зміни повністю відповідають стандартам аудиту, згідно з якими аудитори фінансової звітності повинні дослідити і перевірити якість того, як компанії використовують інформаційні технології та вплив останніх на фінансову звітність. На нашу думку, сюди також повинно входити розуміння ступеня автоматизації управління компанією, оскільки це пов'язано з підготовкою фінансової звітності, загальні механізми контролю за використанням IT, що важливі для ефективного функціонування автоматизованих засобів управління, а також усвідомлення аудиторами надійності даних і звітів компанії, які використовуються під час підготовки фінансової звітності.

При цьому, аудитори можуть надавати компаніям консультаційні послуги чи послуги з підтвердження інформації про кібербезпеку, оскільки публічні компанії часто добровільно розкривають інформацію про свої механізми управління кіберризиками. До таких послуг можуть бути віднесені:

1) проведення оцінки, у рамках якої аудитори можуть допомогти компаніям визначити основні кіберризики, виявити прогалини у процесах та механізмах контролю та розробити ефективну систему контролю;

2) підтвердження. Аудитори можуть провести перевірку відповідно до стандартів Американського інституту дипломованих публічних бухгалтерів (AICPA) та надати незалежний звіт про те, чи відповідає опис програми управління ризиками кібербезпеки специфікаціям системи звітності компанії. Критерії AICPA для систем контролю в межах кібербезпеки можуть використовуватися аудиторами в разі виконання поставленого завдання.

**Список використаних джерел:**

1. Братюк В. П. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні. *Актуальні проблеми економіки*. 2015. № 9. С. 421-427.

2. Електронний ресурс: Режим доступу: https://insuranceukraine.online/