УДК 330.131.7

КІБЕР-РИЗИКИ ЯК ОДИН ІЗ ВИДІВ СУЧАСНИХ РИЗИКІВ У ДІЯЛЬНОСТІ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ ТА УПРАВЛІННЯ НИМИ

CYBER RISKS AS ONE OF THE MODERN RISKS OF SMALL AND MEDIUM BUSINESS AND THEIR MANAGEMENT

Віннікова І.І.
кандидат економічних наук,
доцент кафедри менеджменту,
Київський національний економічний університет
імені Вадима Гетьмана

Марчук С.В.
асистент кафедри менеджменту,
Київський національний економічний університет
імені Вадима Гетьмана

Статтю присвячено дослідженню сутності кібер-ризиків та їх ролі для організацій малого та середнього бізнесу. Вивчено вітчизняний та зарубіжний досвід кібер-ризиків. Виділено основні ознаки, за якими було згруповано кібер-ризики. Узагальнено класифікацію кібер-ризиків. Розглянуто наслідки для організацій малого та середнього бізнесу від настання кібер-ризиків. Доведено, що найбільшою проблемою для малого та середнього бізнесу, з огляду на стрімкий розвиток інформації, інформаційних та комп'ютерних технологій, є кібер-ризики, в результаті чого організації несуть грошові втрати.

Ключові слова: *ризик, кібер-ризики, кібер-атаки, кібер-інциденти, управління кібер-ризиками.*

Статья посвящена исследованию сущности кибер-рисков и их роли для организаций малого и среднего бизнеса. Изучен отечественный и зарубежный опыт кибер-рисков. Выделены основные признаки, по которым были сгруппированы кибер-риски. Обобщена классификация кибер-рисков. Рассмотрены последствия для организаций малого и среднего бизнеса от наступления кибер-рисков. Доказано, что самой большой проблемой для малого и среднего бизнеса, учитывая стремительное развитие информации, информационных и компьютерных технологий, являются кибер-риски, в результате чего организации несут денежные потери.

Ключевые слова: *риск, кибер-риски, кибер-атаки, кибер-инциденты, управление кибер-рисками.*

The article is devoted to the study of the essence of cyber-risk and its role for organizations of small and medium-sized businesses. We studied the domestic and foreign experience of cyber-risk. Identified the main features for which cyber- risks were aggregated. A review of the classification of cyber-risks. The consequences for small and medium-sized businesses from cyber-risk were considered. It has been proved that the biggest problem for small and medium-sized businesses, considering the rapid development of information, information and computer technologies, are cyber-risks, as a result of this organizations lose money.

Key words: *risk, cyber risk, cyber-attack, cyber incidents, cyber-risk management.*

Постановка проблеми. Розвиток сучасної економіки потребує реалізації всього потенціалу інформаційних технологій, за допомогою яких у найкоротші терміни можливо задовольнити потреби внутрішнього і зовнішніх ринків.

Щодня людство виробляє 2,5 ексабайта інформації, при цьому обсяг бізнес-даних подвоюється кожні 14 місяців. «Розумні» пристрої та нові послуги можуть бути причиною непередбачених наслідків та загроз.

Організації малого та середнього бізнесу стають усе більш залежними від інформаційних систем, що робить їх уразливими для кібер-ризиків: витоку даних внаслідок кібератак і комп'ютерних вірусів, втрати даних через людський фактор або збої у роботі носіїв інформації.

Кібер-ризики пов'язані з використанням комп'ютерного обладнання та програмного забезпечення як у місцевих (локальних) мережах, так і в глобальній інтернет-мережі; в розрахунково-платіжних системах, системах інтер-

нет-торгівлі, промислових системах управління; а також ризик пов'язаний із накопиченням, зберіганням і використання особистих даних.

Кібер-ризики можуть призводити до прямих та непрямих грошових втрат в організаціях малого та середнього бізнесу. В першому випадку можна легко виміряти збитки в грошовому еквіваленті. В другому випадку необхідно залучати експерта або фахівця для якісної оцінки величини збитків в організації.

На міжнародному економічному форумі в 2015 році кібер-ризики названі одними з ключових комерційних ризиків, оскільки наслідки втрати даних можуть бути катастрофічними для бізнесу.

Можна вважати, що найбільшою проблемою для малого та середнього бізнесу, з огляду на стрімкий розвиток інформації, інформаційних та комп'ютерних технологій, є кібер-ризики.

Тому питання класифікації та управління кібер-ризиками набуває особливої актуальності.

Аналіз останніх досліджень і публікацій. Дослідженню питань кібер-ризиків присвячено праці таких учених, як В.П. Братюк [1], Е.Д. Семенова [2], С. Волосович [3], Ю. Кожедуб [4].

Виділення не вирішених раніше частин загальної проблеми. Глобальне бізнес-середовище та інтернет разом із величезними діловими можливостями та вигодами посилюють ймовірність кібер-загроз та кібер-ризиків для організацій. За даними Європейської Комісії [1, с. 26], сьогодні на планеті понад 9 млрд. електронних пристроїв, які підключені до глобальної мережі, а до 2020 р. експерти прогнозують зростання їх кількості до 24 млрд. одиниць. Отже ймовірність кібер-ризиків щоденно зростає. Дослідженням питань кібер-ризиків присвячено праці вітчизняних та закордонних учених. Однак, незважаючи на кількість опублікованих праць та їхню наукову цінність, відсутнє чітке розуміння сутності кібер-ризиків, не визначено вплив кібер-ризиків на діяльність малих та середніх підприємств, відсутній комплексний аналіз кібер-ризиків.

Формулювання цілей статті (постановка завдання). Метою статті є узагальнення теоретичних положень, обґрунтованих закордонними та вітчизняними науковцями для зменшення грошових втрат організацій малого і середнього бізнесу.

Виклад основного матеріалу дослідження. В останні кілька років суттєво збільшилася кількість кібер-атак на світові та українські організації. Метою хакерів стають не тільки державні інститути і підприємства, а й приватний сектор (малий та середній бізнес), адже комп'ютерні системи, які використовують у своїй діяльності організації малого та середнього бізнесу, є уразливими та мають багато прогалин. Щодня тисячі малих підприємств в усьому світі піддаються кібер-атакам. Крадії намагаються вкрасти інформацію та гроші, або втрутитися в бізнес. Наприклад, лише у Великій Британії в 2014 році 60% організації малого бізнесу відчули вплив кібер–ризиків (пережили кібер-атаки, в результаті яких втратили приблизно від 65000 фунтів стерлінгів до 115 000 фунтів стерлінгів) [5].

Згідно із звітом про ризики кібербезпеки Cybersecurity Venturesreport, до 2019 року бізнес у світі буде стикатися з атаками кожні 14 секунд. До 2021 року збитки від загроз кібербезпеки будуть оцінюватися в 6 трлн дол. Крім збільшення кількості кібератак, буде зростати й рівень складності кіберзлочинів [6].

Кібер-інциденти продовжують рух угору в рейтингу і зараз є другим за важливістю ризиком для компаній усього світу (40%) в цьому рейтингу [7]. З огляду на мінливу природу кібер-ризику, а також зростання числа кібер-інцидентів, ризик займає один із верхніх рядків серед найважливіших ризиків у світі. Такими є ключові висновки Барометра ризиків Allianz, щорічно публікується Allianz Global Corporate & Specialty (AGCS). Звіт ґрунтується на думці 1911 експертів із ризик-менеджменту з 80 країн світу [7].

А лише п'ять років тому кібер-ризики знаходилися лише на 15 місці. Такі загрози, як порушення даних, хакерські атаки або ж перерви у виробництві внаслідок кібер-інциденту підтверджують, що це є головним ризиком для бізнесу на Американському континенті і другим за значущістю ризиком у Європі та Азіатсько-Тихоокеанському регіоні.

Кібер-ризики є найбільш недооціненими ризиками в довгостроковій перспективі в Україні.

Яскравим прикладом цього є те, що у 2017 році під час кібератаки вірусу Petya постраждали понад 1500 компаній, а 13 тис комп'ютерів були заражені. За рік український бізнес втратив від кібератак мільярди гривень.

Нами проведено аналіз даних щодо кибер-ризиків, вплив яких відчували організації малого та середнього бізнесу в 2017 році як в Україні, так і в світі (таблиця 1) [8].

За результатами опублікованих наукових та практичних робіт фахівців, а також даних таблиці 1 ми згрупували кібер-ризики за такими ознаками, як: 1) втрата або крадіжка носіїв інформації та мобільних пристроїв; 2) доступ сторонніх осіб до конфіденційної інформації за допомогою вразливих хмарних сховищ; 3) ненавмисне розголошення співробітниками конфіденційної інформації; 4) навмисні дії співробітників (інсайдерів); 5) неконтрольоване копіювання даних співробітниками. На основі перелічених ознак нами було складено узагальнену класифікацію кібер-ризиків, яку зображено на рис. 1.

Отже, кібер-шантаж, фішингові атаки, зломи особистих пристроїв і крадіжка даних – це сучасні ризики для діяльності малих та середніх підприємств. Часто малий та середній бізнес вважають більш легкою мішенню порівняно з великими компаніями. За даними компанії Symantec, 75% організацій малого та середнього бізнесу стали жертвами фішингових атак. Серед великих компаній постраждало тільки 35%.

Таблиця 1

Топ-10 кібер-ризиків у 2017 році

№ з\п	Назва	
1.	Petya	програма-вимагач, яка шифрує дані
2.	Blueborne	вразливість – у протоколі Bluetooth
3.	NotPetya	програма, яка знищує дані на ПК
4.	Wannacry	програма-шифрувальник, що вимагає викуп за дешифрування
5.	KRACK	критична уразливість мереж Wi-Fi
6.	EternalBlue	програма для одержання віддаленого доступу до системи
7.	Bad rabbit	вірус-шифрувальник, розроблений для ОС сімейства Windows
8.	Loki / Locky	Android-шкідливий / шифрувальник Windows
9.	Reaper	вірус, спрямований на IoT-пристрої
10.	Критична вразливість у доступі під root користувачем в MacOS	

Джерело: розроблено авторами на основі [8]

У світлі зростання кількості і серйозності цього питання організації малого та середнього бізнесу змушені внести до свого списку ще одну небезпеку для бізнесу, на яку раніше закривали очі, – це кібер-ризики.

Якщо великі організації зазнають величезних збитків від кібер-ризиків, але виживають, то організації малого та середнього бізнесу можуть поплатитися своїм існуванням: приблизно 60% з них закриються протягом півроку після втрати даних.

Організації малого та середнього бізнесу можуть мати корисну для хакера інформацію; комп'ютер може бути зламаний та використаний для атаки когось іншого; або бізнес може забезпечити доступ до цілей більш високого профілю через свої товари, послуги або ролі в ланцюжку постачання. Загальний негативний ефект від кібер-ризиків також може включати втрату прибутку, неможливість отримати банківський кредит, пошкодження інформаційної системи, зниження продуктивності, втрату репутації проміж клієнтів. На жаль, у цьому відношенні організації малого та середнього бізнесу часто мають більше втрачати, ніж великі підприємства, тому що кібер-атака буває надзвичайно коштовною.

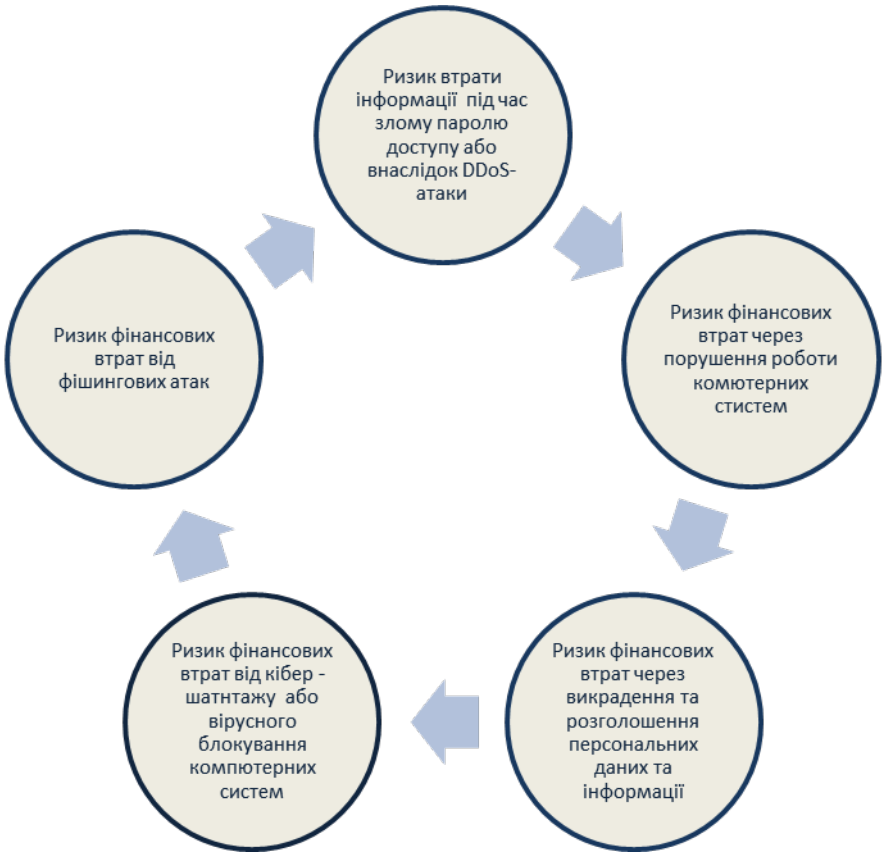

Рис. 1. Узагальнена класифікація кібер-ризиків

Джерело: узагальнено авторами на основі [7-9]

Настання кібер-ризиків для організацій малого та середнього бізнесу приводить до наслідків, які наведені в таблиці 2.

На жаль, більшість як закордонних, так і вітчизняних власників малого та середнього бізнесу вважають, що кібер-злочинці націлюються тільки на великі підприємства з великим товарообігом і великою клієнтською базою даних. Але, незважаючи на те, що великі глобальні організації – це перше, що спадає на думку, коли йдеться про кіберзлочинність, ніхто сьогодні не захищений від хакерських атак.

Проведене британськими дослідниками анкетування стосовно репутації малого бізнесу і кібер-ризику довело, що 58% клієнтів у разі виникнення інциденту з меншою

Таблиця 2

Наслідки для організацій малого та середнього бізнесу від настання кібер-ризиків

Вплив на малий та середній бізнес	Збиток
Припинення або уповільнення бізнес-процесів	Втрата клієнтів та прибутку
Втрата конкурентної переваги	
Збиток для бренду та втрата репутації	Зниження вартості бізнесу
Судові розгляди та позови	Витрати на усунення наслідків, штрафи і санкції регулюючих органів

Джерело: розроблено авторами на основі [9]

ймовірністю використовували би послуги компанії, а 89% постраждалих організацій малого та середнього бізнесу повідомили про 30-відсоткові втрати клієнтів.

Такі наслідки змусили бізнес і державу звернути пильну увагу на питання кібербезпеки, але, на жаль, інвестувати в захист на постійній основі поки готові одиниці. З огляду на все вищенаведене з 25 травня 2018 року набрав чинності Загальноєвропейський регламент про захист персональних даних (англ. GDPR – General Data Protection Regulation). GDPR погоджує стандарти захисту даних в межах ЄС, а діяльність тих, хто не прислухається до попередження, може бути підірвана штрафами Ради зі стандартів безпеки даних індустрії платіжних карт (англ. PCI SSC – Payment Card Industry Security Standards Council).

Регламент є загальнообов'язковим документом без необхідності імплементації його норм у національне законодавство кожної країни-учасниці. Норми Регламенту є нормами прямого дії. Найбільше потрібно зосередитися на тих компаніях, які організовують свою діяльність у сфері інформаційних технологій та здійснюють її через всесвітню мережу Інтернет, оскільки їхня діяльність більшою мірою пов'язана з персональними даними, ніж діяльність будь-яких інших компаній. Порушення норм регламенту передбачає штраф у розмірі до 20 млн євро або до 4% від річного обороту компанії [10].

При цьому більшість представників бізнесу як у Європі, так і в Україні почали усвідомлювати, що з розвитком технологій ризики від кібер-загроз будуть тільки підвищуватися.

Для зменшення кібер-ризиків і оптимізації нових можливостей організації малого та середнього бізнесу мають бути захищеними, пильними і гнучкими.

Як свідчить світова практика, для ефективного захисту даних організації малого та середнього бізнесу повинні дотримуватися розподіленої інфраструктури та резервного копіювання. Відомо, що будь-які дані, що зберігаються в одному місці, можуть бути втрачені – це лише питання часу. Резервне копіювання значно скорочує простоювання системи в разі втрати даних, кібератак або технічних неполадок, а розподілена інфраструктура ефективно усуває ризик недоступності.

Також для організацій малого та середнього бізнесу є важливим розуміння того, яку саме інформацію необхідно захищати. Фахівці компанії «Ернст енд Янг» (YE) виділяють такі види інформації, яка потребує захисту від кібер-загроз: 1) економічна (інформація щодо видів продукції чи послуг; статистика обсягів продажів; фінансові транзакції; звітність до її офіційної публікації; прогнози виробництва; інформація щодо заробітної платні); 2) персональна інформація (номери кредитних карток; паспортні дані; ідентифікаційні номери; інформація для доступу в системи – логіни, паролі, ключі, налаштування); 3) інформація про споживачів і клієнтів (реєстри клієнтів; реквізити партнерів; реєстри потенційних клієнтів); 4) ділова інформація (постанови, які видані регулюючими органами щодо роботи бізнесу; інтелектуальна власність; проектна документація) [11].

Малий та середній бізнес має постійно підтримувати свою основну безпеку можливості захисту від загроз та дотримуватися галузевих комп'ютерних стандартів і правил. Потрібно встановити можливості для виявлення кібер-порушень і передбачення нових загроз. Треба розвинути здатність реагувати на неминучі кібератаки і повернення до звичайних операцій якомога швидше. Головним складником у цьому питанні, на наш погляд, може стати управління кібер-ризиком організацій малого та середнього бізнесу, яке повинно включати комплекс таких дій: 1) навчання і підготовка користувачів з метою підвищення їх інформованості;

2) розроблення процедур управління IT-інцидентами, в тому числі процедур реагування та ліквідації наслідків їх виникнення; 3) розроблення керівництва з кібербезпеки (воно повинно містити найкращі практики кібербезпеки, які організації малого та середнього бізнесу очікують від співробітників. Доцільно включити процедури забезпечення безпеки працівників, постачальників та клієнтів. Політика в галузі кібербезпеки повинна містити також протоколи, яких працівники повинні дотримуватися у разі порушення); 4) використання процедур захисту від шкідливих програм; контроль використання змінних носіїв інформації; 5) до цього комплексу з управління кібер-ризиком можливо додати страхування кібер-ризиків.

Висновки. Отже, кібер-ризики сьогодні виходять далеко за межі крадіжки і шахрайства, що включає втрату конкурентної переваги внаслідок вкраденого інтелектуального

майна, втрату клієнта чи бізнесу, довіри партнера та загальний збиток для репутації та бренду організацій малого і середнього бізнесу. Складність кібер-ризиків в Україні та світі, на жаль, у подальшому буде тільки зростати. Більше підключених пристроїв, більше джерел даних, більше автоматизації процесів, сторонні стосунки створюють нові можливості для кібер-атак та інцидентів.

Як кібер-інциденти, так і пов'язані з ними витрати продовжують зростати, зростає й усвідомлення того, що 100% безпека від них є неможливою в сучасних умовах.

Організацій малого та середнього бізнесу сьогодні повинні вкладати кошти в обґрунтовані заходи контролю безпеки для захисту своїх найважливіших активів від кібер-ризиків.

Певні комплексні дії можуть допомогти організаціям малого та середнього бізнесу знизити ці ризики та втрати від них.

Всі ці дії можна об'єднати в одне комплексне поняття «управління кібер-ризиком» яке не є одноразовим рішенням. Це поточний шлях (комплекс дій) для керівників малих та середніх підприємств.

Управління кібер-ризиком стає стратегічним імперативом, який має глибокий характер та наслідки для загальної продуктивності організацій малого та середнього бізнесу.

Управління кібер-ризиком зосереджується на оцінці загроз, потенційному впливі та вразливості малих і середніх підприємств.

Управління кібер-ризиками нерозривно пов'язане зі здатністю організацій малого та середнього бізнесу вести свій бізнес ефективно.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Братюк В.П. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні / В.П. Братюк // Актуальні проблеми економіки. 2015. № 9. С. 421–427. URL: http://nbuv.gov.ua/UJRN/ape_2015_9_54.

2. Семенова Е.Д. Становление нового цифрового мира и проблемы менеджмента кибер-рисков [Текст] / Е.Д. Семенова, К.И. Тарасова // Маркетинг і менеджмент інновацій. 2017. № 3. С. 236–244. URL: http://10.21272/mmi.2017.3-22.

3. Волосович С. Детермінанти виникнення та реалізації кібер-ризиків / С. Волосович, Л. Клапків // Зовнішня торгівля: економіка, фінанси, право. – 2018. № 3. С. 101–115.

4. Кожедуб Ю. Аналіз документів з керування ризиком кібербезпеки. Information Technology and Security. 2017. Vol. 5. No 1. С. 82–95.

5. Small businesses: What you need to know about cyber security. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/412017/BIS-15-147-small-businesses-cyber-guide-March-2015.pdf.

6. Global Cyber Security Industry 2018-2022. URL: https://www.reportlinker.com/market-report/Cybersecurity/517851/Cyber-Security?utm_source=adwords1&utm_medium=cpc&utm_campaign=Transportation&utm_adgroup=Cybersecurity_Reports&gclid=EAIaIQobChMIrqvcm5nq3AIVx44YCh39Ww5eEAAYASAAEgKx6vD_BwE.

7. Барометра ризиків Allianz. URL: https://www.agcs.allianz.com.

8. В. Якушев. Кібербезпека-2018: чого чекати бізнесу? URL: https://mind.ua/openmind/20180414-kiberbezpeka-2018-chogo-chekati-biznesu. Global Economic Forum, The Global Risks Report 2017. 12thEdition. URL: http://wef.ch/risks2017.

9. 5 ways to make global e-commerce easier for everyone. December, 2017. URL: https://www.weforum.org/agenda/2017/12/ecommerce-trade-wto-growth-opportunity.

10. GDPR. URL: https://www.olans.com.ua/novij-reglament-yes-pro-personalni.

11. Посилення цифрового середовища проти кібер-загроз. URL: https://www.pwc.com/ua/uk/survey/2018/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks-ukr.pdf.