МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

КАФЕДРА СТАТИСТИКИ

«СТАТИСТИКА – ІНСТРУМЕНТ СОЦІАЛЬНО-ЕКОНОМІЧНИХ ДОСЛІДЖЕНЬ»

ЗБІРНИК НАУКОВИХ СТУДЕНТСЬКИХ ПРАЦЬ

ВИПУСК 6

Частина І

Одеса
2020

УДК 311
ББК 60.6

Статистика – інструмент соціально-економічних досліджень: збірник наукових студентських праць. Випуск 6. Частина І. – Одеса, ОНЕУ. – 2020. – 202 с.

Автори:

Вітковська К. В. – к.е.н., доцент кафедри статистики Одеського національного економічного університету,

Милашко О. Г. – к.е.н., доцент кафедри статистики Одеського національного економічного університету,

Ольвінська Ю. О. – к.е.н., доцент кафедри статистики Одеського національного економічного університету,

Підгорний А.З. – к.е.н., професор, завідувач кафедри статистики Одеського національного економічного університету,

Погорєлова Т. В. – к.е.н., доцент кафедри статистики Одеського національного економічного університету,

Самотоєнкова О. В. – к.е.н., доцент кафедри статистики Одеського національного економічного університету,

Тарасова К. І. – к.е.н., доцент кафедри статистики Одеського національного економічного університету,

Абалмасова М. П. – студентка факультету менеджменту, обліку та інформаційних технологій Одеського національного економічного університету,

Агапченко К. А. – студентка факультету менеджменту, обліку та інформаційних технологій Одеського національного економічного університету,

Березорудський А. М. – студент факультету менеджменту, обліку та інформаційних технологій Одеського національного економічного університету,

Білоус О. Ю. – студент факультету економіки та управління підприємництвом Одеського національного економічного університету,

Бойко В. С. – студентка факультету менеджменту, обліку та інформаційних технологій Одеського національного економічного університету,

Бойчева О. П. – студентка факультету менеджменту, обліку та інформаційних технологій Одеського національного економічного університету,

Бурлаєва В. С. – студентка факультету менеджменту, обліку та інформаційних технологій Одеського національного економічного університету,

Гаращенко О. В. – студентка факультету менеджменту, обліку та інформаційних технологій Одеського національного економічного університету,

Капустян Г. В. – студентка факультету економіки та управління підприємництвом Одеського національного економічного університету,

Лабенко О. В. – студентка факультету економіки та управління підприємництвом Одеського національного економічного університету,

Любович А. А. – студентка факультету менеджменту, обліку та інформаційних технологій Одеського національного економічного університету,

Манєва К. П. – студентка факультету менеджменту, обліку та інформаційних технологій Одеського національного економічного університету,

Мівшук Ю. І. – студентка факультету економіки та управління підприємництвом Одеського національного економічного університету,

Мотишена В. В. – студентка факультету менеджменту, обліку та інформаційних технологій Одеського національного економічного університету,

Осадчук Я. В. – студентка факультету економіки та управління підприємництвом Одеського національного економічного університету,

Стародубцева Т. В. – студентка факультету менеджменту, обліку та інформаційних технологій Одеського національного економічного університету,

Унтілов В. В. – студент факультету менеджменту, обліку та інформаційних технологій Одеського національного економічного університету,

Чайковська О. О. – студентка факультету економіки та управління підприємництвом Одеського національного економічного університету,

Чумаченко Н. В. – студентка факультету менеджменту, обліку та інформаційних технологій Одеського національного економічного університету,

Штельмашук М. С. – студентка факультету економіки та управління підприємництвом Одеського національного економічного університету.

У збірнику наводяться результати дослідження студентів та викладачів кафедри статистики щодо застосування сучасних статистичних методів для оцінки соціально-економічних процесів у деяких країнах світу, в Україні та окремих регіонах. Висновки та рекомендації авторів можуть бути корисними для викладачів, аспірантів і студентів, які займаються аналізом процесів, що відбуваються в суспільстві та економіці країни.

ЗМІСТ

КІБЕР-РИЗИКИ ЯК ПОХІДНА РОЗВИТКУ ТЕХНОЛОГІЙ

Мотишена В. В.[1], **Тарасова К. І.**[2]

1 – студент, кафедра статистики,
2 – канд. екон. наук, доцент, кафедра статистики
Одеський національний економічний університет, м. Одеса

АНОТАЦІЇ

Мотишена В. В., Тарасова К. І. Кібер-ризики як похідна розвитку технологій. *Розглянуто поняття термінів «кібер-атака», «кібер-безпека» та «кібер-ризики». Встановлено основні види та джерела походження кібер-ризиків. Проаналізовано динаміку показників в Україні та світі. Виявлено кібер-загрози для світової торгівлі. Обґрунтовано методи боротьби із кібер-ризиками.*
Ключові слова: *кібер-атака, кібер-безпека, кібер-ризики, кібер-загрози.*

Motyshena V. V., Tarasova K. I. Cyber risk as a derivative of technology development. *The terms "cyber-attack", "cyber security" and "cyber risk" are considered. The main types and sources of origin of cyber-risks are established. The dynamics of the indicators in Ukraine and in the world is established. Cyber threats to the world trade are identified. Methods for combating cyber risk are substantiated.*
Keywords: *cyber-attack, cyber security, cyber risks, cyber threats.*

ПОСИЛАННЯ НА РЕСУРС

Мотишена, В. В. *Кібер-ризики як похідна розвитку технологій* [Текст] / В. В. Мотишена, К. І. Тарасова // Статистика – інструмент соціально-економічних досліджень : збірник наукових студентських праць. Випуск 6. Частина І – Одеса, ОНЕУ. – 2020. – С. 116 – 123.

Постановка проблеми у загальному вигляді. Кожна сучасна людина звикла турбуватися про свою безпеку, включаючи в неї не лише фізичку та моральну сторони, а й безпеку своїх фінансових заощаджень, власних інформаційних та медіа даних, приватних володінь тощо. Розвиток мережевої сітки створив надзвичайно зручні умови передачі будь-якої інформації, не залежно від того, кому належить ця інформація: індивідууму чи підприємству. Разом із цим, з'явилися й проблеми ймовірності витоку даних, їх модифікація в негативних цілях та отримання фінансових та моральних наслідків. Починаючи з 2012 р. проблема кібер-ризиків є однією із найголовніших загроз людству.

Розвиток світової павутини на сьогоднішній день залишається некерованим та неконтрольованим механізмом, і цей особливий механізм здійснює неабиякий вплив економічного, політичного та гуманітарного характеру.

Аналіз досліджень і публікацій останніх років. Актуальність досліджень кібер-ризиків полягає у постійному розвитку та розширенні поняття, появі нових витоків, видів, класифікацій та активізації процесів кібер-загроз загалом. Такі проблеми не могли залишитись без уваги вчених. Особливої уваги заслуговують загальнотеоретичні праці таких дослідників як: В. Братюка, М. Елінга, К. Семенової, Ю. Кожедуба та інших.

Істотну роль у дослідженні сутності кібер-ризиків відіграють приватні інституції: консалтингові, страхові компанії та компанії з інформаційного та програмного забезпечення, зокрема AON, PricewaterhauseCoopers, Deloitte, Ernstand Young, Society of Actuaries, International Association, Allianz, Geneva Association [1].

Виділення невирішених раніше частин загальної проблеми. З огляду на новизну проблеми кібер-ризиків, частина питань щодо їх типів, видів, основних загроз і методів управління залишається й досі невирішеними.

Мета роботи. Основною метою дослідження є аналіз розвитку кібер-ризиків в Україні та світі, а також виявлення наслідків даного явища для національної та світової економіки.

Виклад основного матеріалу. Кібер-атака, кібер-безпека та кібер-ризики – це три взаємопов'язані терміни. Перший процес проявляє себе як спроба реалізації загрози, другий – як захист від здійснення даної загрози, а третій – це ризики, що можуть виникнути при здійсненні першого та відсутності другого процесів. Загалом, кібер-ризик – 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, системах Інтернет-торгівлі, промислових системах управління, а також це ризик, пов'язаний з накопиченням, зберіганням і використанням особистих персональних даних [2].

Формування кібер-ризиків можна розглянути за трьома різними підходами: причинно-наслідковий, секторальний та інструментальний. Причинно-наслідковий підхід включає в себе наслідки реалізації та походження кібер-ризиків. Секторальний розрізняє сфери реалізації кібер-ризиків. Інструментальний акцентує увагу на інструментах, за допомогою яких реалізуються кібер-ризики [3]. Одним із інструментів реалізації кібер-ризику є кібератака; другою формою реалізації кібер-ризиків є кібер-інцидент; третьою – кібер-тероризм; четвертою – кібер-війна. Ключовий критерій поділу на зазначені форми – це мотивація кібер-втручання та механізм його впливу на інформаційні системи [4].

Існує чимало класифікацій кібер-ризиків, вони постійно змінюються або доповнюються, тому слід розглянути декілька з них. Й. Кебула та Л. Янг систематизували та виділили чотири основні класи джерел виникнення операційних кібер-ризиків (рис. 1):

Рис. 1. Класифікація джерел та форм кібер-ризиків Й. Кебула та Л. Янга

Для того, аби класифікація не втрачала своєї актуальності, її постіно змінюють та покращують, вносять нові складові. В сучасному розумінні вона має наступний вигляд (рис. 2):

Рис. 2. Класифікація джерел кібер-ризиків

Більш спростованою версією попередньої класифікації є наступна, яка має назву узагальненої класифікації, та включає в себе 5 складових елементів (рис. 3):

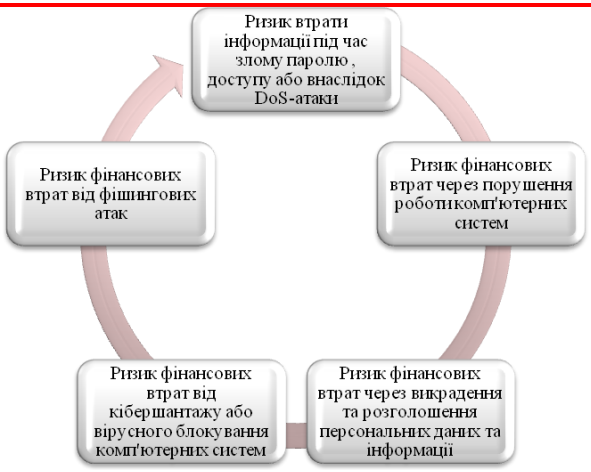


Рис. 3. Узагальнена класифікація кібер-ризиків

Реалізація кібер-ризиків може наставати внаслідок наступних подій:

1. Нецільові атаки – фішинг, кардінг, sms-шахрайство.
2. Цільові атаки – фінансове шахрайство, викрадення баз даних, промислове шпигунство, DoS-атаки, вимагання.
3. Внутрішні атаки – викрадення, знищення інформації, сприяння цільовим атакам.

Найчастіше кібер-атаки здійснюються на підприємствах, фірмах та організаціях, погіршуючи їх репутацію, приносячи збитки та створюючи ситуації, за які доводиться відповідати перед законом, або стає неможливо отримати позики в банку, пошкоджується інформаційна база та погіршується репутація. У будь-якому випадку, встояти перед атаками дуже важко, особливо якщо йдеться про дрібний та середній бізнес, підприємства якого, на відміну від великого, у 60% випадків змушені припиняти свою діяльність після реалізації кібер-ризиків. Атака на дрібні та середні підприємства здійснюється частіше через можливість доступу через них до більш крупних фірм, яким вони, наприклад, надають певні послуги [5, 6]. Наслідки від настання кібер-ризиків для організацій малого та середнього бізнесів можна розбити на наступні групи:

I. Припинення та уповільнення бізнес-процесів, втрата конкурентної переваги.

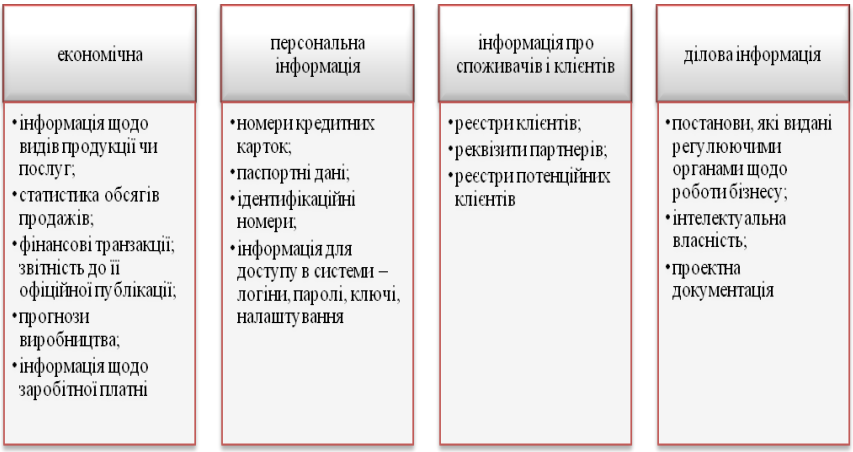
II. Збитки для бренду та втрата репутації.

III. Судові розгляди та позови.

Перша група наслідків характеризується збитками у вигляді втрати клієнтів та прибутку, друга – зниженням вартості бізнесу, третя – витратами на усунення наслідків, сплату штрафів та санкцій регулюючих органів. Істиною залишається те, що будь-яка організація вважає себе

добре захищеною, через що не бачить сенсу інвестицій у покращення системи кібер-безпеки, тому ця галузь розвивається занадто повільними темпами. Лише у 2018 р. набув чинності Загальноєвропейський регламент про захист персональних даних, який передбачає спеціальну систему нормативів, відповідно до яких повинна організовуватись діяльність будь-якої організації, компанії та інших фірм у межах ЄС, а у разі порушення даних норм та недотримання стандартів передбачається штраф у розмірі 20 млн. євро або до 4% від річного обороту компанії.

Кожна організація, зазвичай, надає інформацію для своїх користувачів, яка знаходиться у вільному доступі. Така інформація має цінність, але не потребує настільки високого рівня захисту. Але є інформація, яку потрібно захищати в першу чергу і яка потребує спеціального захисту. Виділяють декілька видів інформації, яка потребує



кібер-захисту (рис. 4):

Рис. 4. Класифікація інформації, яка потребує захисту від кібер-загроз

Кожна компанія задається питанням, які дії для запобігання кібер-атак вона може здійснювати зі своєї сторони. Перш за все, це інформованість користувачів та надання корисних інструкцій з користування (наприклад, порада встановлення безпечного паролю, підбор паролю програмою). Другою ознакою виступає розробка спеціальних протоколів з користування працівниками та дії у разі виникнення загрози, спроби загрози, які в свою чергу повинні також виявлятись спеціальними програмами. І третьою, не менш важливою ознакою, виступає страхування кібер-ризиків.

В. Братюк зазначає, що страхування кібер-ризиків спрямоване на подолання наслідків втручання кібер-злочинців (відновлення функцій, інформації, комунікацій) та пов'язане з покриттям всіх необхідних для

цього витрат, а також на відшкодування збитків, які є результатом простою комп'ютерних систем [7].

Кібер-страхування – це страховий продукт, що захищає компанію від ризиків, пов'язаних з використанням мережі Інтернет, а також із ризиками, що відносяться до інформаційних технологій, IT-інфраструктури та діяльності підприємства в кіберпросторі [8].

Страхування в такій сфері передбачає відшкодування та забезпечення компенсацією організації за прийнятну ціну у разі кібер-атаки, яка може в свою чергу спричинити перерви у виробництві, втрати та відновлення даних, розслідування інцидентів тощо. Також у страхові послуги можуть входити й антикризовий піар з метою відновлення репутації та витрати на захист у суді та відновлення роботи IT-систем.

Розглянувши теоретичні значення сфери кібер-ризиків, можна проаналізувати їх розвиток за останній період в Україні та світі. На рис. 5 зображено динаміку масштабних кібер-інцидентів.

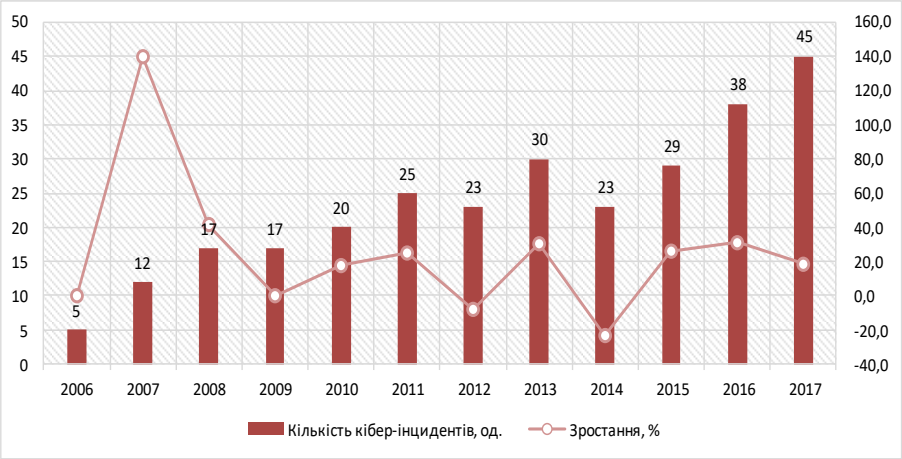


Рис. 5. Кількість кібер-інциденті у світі , 2006-2017 рр.

Проведені дослідження стверджують, що щороку внаслідок кібер-злочинності втрачається 445-600 млрд. дол. США, що в свою чергу становить 1% світового рівня валового внутрішнього продукту. Найбільшу частку у структурі кібер-атак займає кібер-злочинність – 81,7%, кібер-шпигуство займає 12,2%, кібер-війни – 4,3%, хактівізм – 1,7%.

Щодо України, то і вона стала полігоном для кібер-злочинності, втрачаючи дані та гроші. Кількість вірусних заражень і хакерських атак в Україні за останній рік зросла в десять разів – це 100 мільйонів випадків. За словами експертів, хакери вийшли на безпрецедентний рівень технічної складності. Зловмисники використовують шифрування, легальні

Інтернет-сервіси, а також мережеві віруси-вимагачі. За останні п'ять років в Україні кількість інформаційних злочинів зросла мінімум у 2,5 рази.

Згідно з аналітичними звітами за останні 2-3 роки, близько 3% від загальних витрат на IT в світі припадає на кібер-безпеку.

У відповідності до звіту компанії Sophos, сформованого за підсумками опитування 3100 IT-фахівців із 12 країн, 68% компаній постраждали від кібератак в 2018 р., незважаючи на всі спроби запобігти їм. При цьому 91% IT-фахівців зізналися, що атаки були успішними, незважаючи на використання сучасних методів захисту. У числі найбільш популярних векторів атак респонденти назвали електронну пошту (33%), уразливості в програмному забезпеченні (23%), а також використання несанкціонованих USB-накопичувачів або інших зовнішніх пристроїв (14%). За даними експертів, якщо у світі не буде створено реальної дієвої системи кібер-захисту, то вже у 2021 р. бізнес може зазнати збитків від кібератак на суму $6 трлн [9, 10].

Висновки. Кібер-ризики проявляються сьогодні у будь-якій сфері діяльності, незалежно від розмірів та фінансового стану організацій; кожна з них знаходиться у небезпеці навіть із наявністю сучасних технологій та захисних програм, кваліфікованого персоналу та спеціальних системам захисту. Наслідки кібер-ризиків призводять до фінансових втрат організацій або повної ліквідації їх зі світового ринку, і як наслідок, цей процес спричинив появу кібер-страхування, яке має змогу частково або повністю відшкодовувати втрати після чергових кібератак. Вислів «хто володіє інформацією, той володіє світом» є досить доречним у даному випадку, адже інформація, яка опиняється в руках зловмисників може нанести незворотної шкоди для людства. Одна справа, коли йдеться про персональну інформацію користувачів соціальних мереж, яка зазвичай призводить до особистих незручностей та моральних переживань, і зовсім інша справа, коли викрадена інформаціє носить політичний характер на державному рівні і під загрозою опиняється ціле людство.

ЛІТЕРАТУРА

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. – [Електронний ресурс] – Режим доступу: http://nbuv.gov.ua/UJRN/ape_2015_9_54.

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

3. Семенова Е. Д., Тарасова К. И. Становление нового цифрового мира и проблемы менеджмента кибер-рисков. Маркетинг і менеджмент інновацій. 2017. № 3. С. 236–244.

4. 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.

5. Тарасова К. І. Менеджмент інформаційної безпеки малих та середніх підприємств / К. І. Тарасова // Стратегії та інновації: актуальні управлінські практики (13 квітня 2017). – Кривий Ріг: ДонНУЕТ імені Туган-Барановського, 2017. – С. 416-418.

6. Ольвінська Ю. О. Роль розвитку малого бізнесу у реструктуризації регіонального ринку праці / Ю. О. Ольвінська // Социально-экономические аспекты промышленной политики. Управление трудовыми ресурсами: государство, регион, предприятие. – Донецк: ІЕП, 2006. – Т.2. – С. 345-350.

7. За п`ять років кількість кібератак в Україні зросла в 2,5 рази: Колективне ділове медіа. – [Електронний ресурс] – Режим доступу: https://business.ua/news/6976-za-p-yat-rokiv-kilkist-kiberatak-v-ukrajini-zrosla-v-2-5-razi.

8. Покатіс В. IT та телеком. – [Електронний ресурс] – Режим доступу: https://delo.ua/business/ugroza-kiberatak-esche-vysokaja-no-poteri-budut-351923/.

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

10. Віннікова І.І., Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними // І.І. Віннікова, С.В. Марчук // Східна Європа: економіка, бізнес та управління. – Випуск 5 (16) 2018.

ЗБІРНИК НАУКОВИХ СТУДЕНТСЬКИХ ПРАЦЬ

«СТАТИСТИКА – ІНСТРУМЕНТ СОЦІАЛЬНО-ЕКОНОМІЧНИХ ДОСЛІДЖЕНЬ»

ВИПУСК 6

Частина І

Одеса
2020