МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Навчально-науковий інститут бізнесу, економіки та менеджменту
Кафедра економічної кібернетики

«До захисту допущено»
Завідувач кафедри
_____ Віталія КОЙБІЧУК
(підпис) (Ім'я та ПРІЗВИЩЕ)
____ _____ 2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня бакалавр
зі спеціальності 051 «Економіка» ,
освітньо-професійної програми «Економічна кібернетика»
на тему: Економіко-математичне моделювання тенденцій розвитку страхування кібер-ризиків

Здобувача групи ЕК-91а Борщенка Костянтина Юрійовича

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Костянтин БОРЩЕНКО

Керівник д.е.н., професор,
доцент кафедри економічної кібернетики  Антон БОЙКО

Суми – 2023

Анотація

кваліфікаційної бакалаврської роботи на тему

«ЕКОНОМІКО-МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТЕНДЕНЦІЙ РОЗВИТКУ СТРАХУВАННЯ КІБЕР-РИЗИКІВ»

студента Борщенка Костянтина Юрійовича

Актуальність кваліфікаційної роботи обумовлена тим, що в умовах війни кібер загрози набули нового значення. Кібер-атакам піддаються як державні, так і комерційні установи, а збитки які вони наносять є непомірними для суб'єктів господарювання. Єдиним ринковим інструментом забезпечення фінансової стійкості економічних агентів та збереження їх репутації є кіберстрахування. Воно не тільки дозволяє відшкодувати понесені збитки, але й при підтримці фахівців страхової компанії створити надійну превентивну систему цифрової безпеки.

Мета кваліфікаційної роботи – розробка економіко-математичної моделі тенденцій розвитку страхування кібер-ризиків.

Об'єктом дослідження є соціально-економічні відносини, що виникають між суб'єктами страхування кібер-ризиків.

Предметом дослідження є економіко-математичні методи та моделі характеристики тенденцій розвитку страхування кібер-ризиків.

Задачами дослідження є: розкриття змісту кібер-ризиків; дослідження особливостей страхування кібер-ризиків; дослідження підходів до моделювання страхових ризиків; визначення постановки задачі моделювання; формування інформаційної бази дослідження, розробка моделі прогнозування тенденцій розвитку страхування кібер-ризиків; здійснення практичної реалізації моделі прогнозування тенденцій розвитку страхування кібер-ризиків; перевірити якості моделі.

Для досягнення мети роботи використані методи дослідження: аналіз, узагальнення, моделювання, аналогія.

Ключові слова: страхування, кіберстрахування, моделювання, прогнозування, експоненціальне згладжування, багатофакторна регресія.

Зміст кваліфікаційної роботи викладено на 31 сторінці. Список використаних джерел із 40 найменувань, розміщений на 5 сторінках. Робота містить 1 таблицю, 5 рисунків, а також 1 додаток, розміщений на 1 сторінці.

Рік виконання кваліфікаційної роботи – 2023 рік.

Рік захисту роботи – 2023 рік.

Міністерство освіти і науки україни

Сумський державний університет

Навчально-науковий інститут бізнесу, економіки та менеджменту

Кафедра економічної кібернетики

ЗАТВЕРДЖУЮ

Завідувач кафедри

к.е.н., доцент

_____ В. В. Кобійчук

«___» _____ 2023 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

(спеціальність 051 Економіка «Економічна кібернетика»)

студенту 4 курсу, групи ЕК-91а

Борщенку Костянтину Юрійовичу

1. Тема роботи Економіко-математичне моделювання тенденцій розвитку страхування кібер-ризиків.

затверджена наказом по університету від «23» травня 2023 року

2. Термін подання студентом закінченої роботи «16» червня 2023 року.

3. Мета кваліфікаційної роботи розробка економіко-математичної моделі тенденцій розвитку страхування кібер-ризиків.

4. Об’єкт дослідження соціально-економічні відносини, що виникають між суб’єктами страхування кібер-ризиків

5. Предмет дослідження економіко-математичні методи та моделі характеристики тенденцій розвитку страхування кібер-ризиків

6. Орієнтовний план кваліфікаційної роботи, терміни подання розділів керівникові та зміст завдань для виконання поставленої мети

Розділ 1. Теоретичні основи моделювання страхування кібер-ризиків — 23 травня 2023 року

У розділі 1. Розкрити зміст кібер-ризиків та проаналізувати особливості їх страхування. Дослідити підходи до моделювання страхових ризиків. Провести постановку задачі моделювання.

Розділ 2 Побудова економіко-математичної моделі прогнозування тенденцій розвитку страхування кібер-ризиків – 3 червня 2023 року

У розділі 2 Розробити модель прогнозування тенденцій розвитку страхування кібер-ризиків. Здійснити практичну реалізацію моделі прогнозування тенденцій розвитку страхування кібер-ризиків та перевірити її на адекватність.

8. Консультації з роботи:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1			
2			
3			

9. Дата видачі завдання: «3» квітня 2023 року.

Керівник кваліфікаційної роботи  А. О. Бойко
(ініціали, прізвище)

Завдання до виконання одержав  К. Ю. Борщенко
(ініціали, прізвище)

ЗМІСТ

ВСТУП 7
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ МОДЕЛЮВАННЯ СТРАХУВАННЯ КІБЕР-РИЗИКІВ 9
1.1. Зміст кібер-ризиків та особливості їх страхування 9
1.2. Дослідження підходів до моделювання страхових ризиків 15
1.3. Постановка задачі моделювання 21
РОЗДІЛ 2 ПОБУДОВА ЕКОНОМІКО-МАТЕМАТИЧНОЇ МОДЕЛІ ПРОГНОЗУВАННЯ ТЕНДЕНЦІЙ РОЗВИТКУ СТРАХУВАННЯ КІБЕР-РИЗИКІВ 23
2.1 Опис вхідного масиву даних дослідження 23
2.1 Розробка методичних засад прогнозування тенденцій розвитку страхування кібер-ризиків 27
2.3 Практична реалізація моделі прогнозування тенденцій розвитку страхування кібер-ризиків та перевірка її на адекватність 31
ВИСНОВКИ 37
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 38
ДОДАТОК А 43

ВСТУП

Цифровізація та глобалізація призвели до того, що за оцінками експертів до 2025 року колективні дані людства досягнуть 175 зеттабайт. Ці дані включають в себе все - від потокового відео і додатків для знайомств до баз даних охорони здоров'я. Захист усіх цих даних є життєво важливим.

Основною метою кіберзлочинців є отримання інформації - наприклад, імен, паролів і фінансових записів, які потім продаються в даркнеті. Атаки можуть статися в будь-який час, і жертвами можуть стати як приватні особи, так і організації.

Мета кваліфікаційної роботи – розробка економіко-математичної моделі тенденцій розвитку страхування кібер-ризиків.

Об’єктом дослідження є соціально-економічні відносини, що виникають між суб’єктами страхування кібер-ризиків.

Предмет дослідження – економіко-математичні методи та моделі характеристики тенденцій розвитку страхування кібер-ризиків.

Завдання, які необхідно виконати під час написання кваліфікаційної роботи:

– розкрити зміст кібер-ризиків;
– проаналізувати особливості страхування кібер-ризиків;
– дослідити підходи до моделювання страхових ризиків;
– провести постановку задачі моделювання;
– розробити модель прогнозування тенденцій розвитку страхування кібер-ризиків;
– здійснити практичну реалізацію моделі прогнозування тенденцій розвитку страхування кібер-ризиків;
– перевірити якості моделі.

Методи дослідження – порівняння, аналіз, синтез, наукове узагальнення, багатофакторне регресійне моделювання, метод експоненційного згладження.

Практична значущість роботи полягає у створенні розробці моделі прогнозування розвитку страхування кібер-ризикам, що дозволяє суб’єктам господарювання та державним установам сформувати тактичні та стратегічні програми цифрового захисту.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ МОДЕЛЮВАННЯ СТРАХУВАННЯ КІБЕР-РИЗИКІВ

1.1.Зміст кібер-ризиків та особливості їх страхування

Кібер-ризики, також відомі як кібербезпекові ризики, відносяться до небезпек, пов'язаних з використанням комп'ютерів, мереж і цифрових технологій. Вони включають у себе можливість несанкціонованого доступу до інформації, крадіжку даних, втрату або пошкодження цифрових активів, а також різного роду атаки на комп'ютерні системи та мережі [28].

Кібер-ризики можуть мати серйозні наслідки для організацій та індивідуальних користувачів. Вони можуть призвести до фінансових втрат, порушення конфіденційності даних, втрати репутації, порушення законодавства та інших негативних наслідків [7].

Деякі типи кібер-ризиків включають:

1. Фішинг: це метод шахрайства, при якому зловмисники намагаються отримати конфіденційну інформацію, таку як паролі, банківські реквізити або особисті дані, шляхом використання підроблених електронних повідомлень або веб-сайтів. Зловмисники надсилають електронні листи або повідомлення, позначені як легітимні, від імітованих компаній, банків або організацій. Ці повідомлення можуть містити прохання про оновлення паролю, надання особистих даних або виконання фінансових транзакцій. Якщо користувач упадає в пастку і розкриває свої конфіденційні дані, зловмисники отримують доступ до їх облікових записів або фінансової інформації [20].

2. Віруси та шкідливі програми: це програми, які призначені для завдання шкоди комп'ютерним системам або крадіжки інформації. Вони

можуть поширюватися через електронну пошту, незахищені веб-сайти, підроблені програми та інші канали. Зловмисники можуть створювати та розповсюджувати віруси, черв'яки, троянські програми та інші шкідливі програми через пошту, завантажувані файли, підроблені веб-сайти або вразливості в операційних системах. Ці програми можуть пошкоджувати дані, перехоплювати конфіденційну інформацію або навіть отримувати дистанційний доступ до комп'ютерної системи.

3. DDoS-атаки: атаки з відмовою в обслуговуванні (DDoS) спрямовані на перевантаження комп'ютерних систем або мереж шляхом відправки великої кількості запитів. Це призводить до відмови в обслуговуванні для законних користувачів. Це може призвести до значного зниження продуктивності, втрати ділової активності та втрати довіри користувачів.

4. Крадіжка даних: зловмисники можуть зламати системи та мережі. Зловмисники можуть зламати комп'ютерні системи або мережі, щоб незаконно отримати доступ до конфіденційної інформації, такої як особисті дані користувачів, фінансова інформація або банківська інформація.

Часто жертвами зловмисників стають ланцюги постачання різних компаній. Кіберінциденти, такі як злам у постачальника програмного забезпечення для управління SolarWinds та Log4j у світі з відкритим кодом, ставлять під загрозу організації по всьому світу. Аналітична компанія Gartner прогнозує, що до 2025 року 45% світових організацій так чи інакше постраждають від атак на ланцюги постачання [23].

Окремим видом кібер-ризиків є криптоджекінг. Це форма кібератаки, коли зловмисники незаконно використовують обчислювальні ресурси комп'ютера або мобільного пристрою користувача для видобутку криптовалюти. Це стало особливо поширеним явищем з появою популярних криптовалют, таких як Bitcoin і Monero [24].

Механізм криптоджекінгу зазвичай включає в себе використання шкідливого коду (наприклад, JavaScript-скрипту), який без відома користувача вбудовується в веб-сторінки або віруси, які інсталюються на комп'ютері або пристрої. При відвідуванні інфікованих веб-сайтів або запуску інфікованих файлів, шкідливий код починає використовувати обчислювальні ресурси пристрою для майнінгу криптовалюти [27, 3, 14].

Однією з причин популярності криптоджекінгу є його прихованість. Користувачі зазвичай не помічають, що їх обчислювальні ресурси використовуються для майнінгу, оскільки це відбувається в фоновому режимі. Однак це може призводити до сповільнення роботи пристрою, збільшеного енергоспоживання і скорочення терміну його служби.

Кіберзлочинність може впливати на бізнес роками після першої атаки. Витрати, пов'язані з кібератаками – судові позови, підвищення страхових тарифів, кримінальні розслідування та негативні відгуки у пресі можуть швидко вивести компанію з бізнесу:

Частиною підтримки високого рівня безпеки є забезпечення того, щоб працівники, не пов'язані з безпекою, знали, як безпека впливає на їхню повсякденну діяльність. Створення навчальної програми з підвищення обізнаності про безпеку є необхідною частиною стратегії безпеки будь-якої компанії. Співробітники, починаючи від співробітників і закінчуючи генеральними директорами, постійно отримують фішингові електронні листи. Якщо у вашому середовищі є мобільні пристрої та пристрої Інтернету речей, створення плану реагування на мобільні інциденти є обов'язковим. Згідно зі звітом "Стан стійкості кібербезпеки 2021" від Accenture, вартість витоку даних зросте з $3 трильйонів щороку до понад $5 трильйонів у 2024 році.

Одна атака - чи то витік даних, шкідливе програмне забезпечення, програми-вимагачі або DDoS-атака - коштуватиме компаніям у США в середньому 18 000 доларів у 2022 році порівняно з 10 000 доларів у 2021

році, а 47% всього американського бізнесу так чи інакше постраждають від кібератак, згідно зі звітом Hiscox "Звіт про кіберготовність 2022".

Згідно зі згаданим вище звітом IBM/Ponemon Institute, середня загальна вартість витоку даних у 2022 році становила 4,35 мільйона доларів. Найдорожчими були порушення в галузі охорони здоров'я - в середньому $10,10 млн. Найдорожче обійшлися порушення в США - $9,44 млн [36].

Хоча 43% атак спрямовані на малий та середній бізнес, за даними Accenture, лише 14% цих підприємств готові захищатися.

За винятком Міністерства оборони, уряд США заклав у бюджеті на 2023 рік 10,89 мільярда доларів на кібербезпеку. Міністерство внутрішньої безпеки отримає приблизно 2,6 мільярда доларів у 2023 році [26].

До 2023 року кіберзлочинці викрадуть понад 33 мільярди записів, що на 175% більше, ніж у 2018 році.

За даними Cybersecurity Ventures, до 2027 року глобальні витрати на навчання з кібербезпеки сягнуть 10 мільярдів доларів. Зі збільшенням кількості інтернет-користувачів внутрішні загрози стають такими ж важливими, як і загрози ззовні. Навчання співробітників розпізнавати загрози безпеці та повідомляти про них може посилити вашу стратегію кіберзахисту [13].

Враховуючи високий рівень ризику отримати значні втрати через кібер-загрози, виникає необхідність у страхуванні цих ризиків [29].

Страхування кібер-ризиків відрізняється від інших типів страхування, таких як страхування життя, страхування майна і страхування цивільної відповідальності, через свою специфіку і унікальні виклики, пов'язані з цифровим середовищем. Ось деякі ключові аспекти, які роблять страхування кібер-ризиків особливим:

1. Швидкозмінність технологій: Кібер-ризики постійно еволюціонують, оскільки зловмисники постійно шукають нові способи атак. Технологічні зміни, включаючи розвиток штучного інтелекту,

Інтернету речей і хмарних технологій, створюють нові кібер-загрози. Страхування кібер-ризиків повинно бути гнучким та адаптованим до цих змін.

2. Несподіваність та непередбачуваність: Кібератаки можуть статися в будь-який час і будь-якій компанії, незалежно від її розміру чи галузі. Вони можуть мати непередбачувані наслідки, такі як крадіжка конфіденційної інформації, зупинка бізнес-операцій чи пошкодження репутації. Страхування кібер-ризиків допомагає організаціям підготуватися до таких непередбачуваних подій і зменшити їхні наслідки [25].

3. Нестача стандартизованих даних: Визначення обсягу кібер-ризиків та оцінка збитків можуть бути складними завданнями через відсутність повних та стандартизованих даних. Кібер-атаки можуть мати далекосяжні наслідки, які можуть бути важко оцінити в грошовому виразі. Страхування кібер-ризиків повинно розвиватися разом з цією галуззю та надавати універсальні методи оцінки та врегулювання збитків [40, 39, 38].

4. Індивідуалізація та специфіка: Кожна компанія має унікальний стек технологій, архітектуру мережі та схему безпеки. Страхування кібер-ризиків повинно бути здатне адаптуватися до конкретних потреб кожної організації, забезпечуючи індивідуальні поліси та заходи безпеки.

5. Проактивний підхід: Особливість кібер-ризиків полягає в тому, що необхідно бути не лише реактивним, а й проактивним. Організації повинні приділяти увагу попередженню кібер-атак, вдосконаленню систем безпеки та навчанню персоналу. Страхування кібер-ризиків може сприяти впровадженню таких проактивних заходів [32].

Страхування кібер-ризиків є важливим інструментом для організацій, оскільки допомагає зменшити фінансові та репутаційні збитки від кібер-атак, а також забезпечує підтримку від експертів з кібербезпеки та відшкодування збитків. Проте, враховуючи постійну зміну кібер-загроз,

важливо регулярно переглядати та адаптувати поліси страхування, щоб вони відповідали найсучаснішим ризикам [34, 37].

Страховий захист від кібер-ризиків існує у двох формах: як кібер-обмовка до класичних полісів страхування майна/відповідальності та як окремий кібер-поліс.

Багато комерційних страхових компаній пропонують індосамент для покриття деяких видів кібер-відповідальності та ризиків витоку даних. Кібер-індосамент є привабливим для малого та середнього бізнесу, оскільки він є відносно економічно вигідним і може бути доданий до існуючого полісу без додаткового андеррайтингу. Зазвичай їх додають до таких полісів, як: комерційна загальна відповідальність (CGL), страхування від помилок та упущень (E&O), відповідальність директорів та посадових осіб (D&O), відповідальність за вірність та злочини, переривання діяльності (BI), страхування електронного обладнання (EEI), поліс власників бізнесу (BOP) тощо. Однак вважається, що кіберстрахування створює ілюзію захисту через низькі ліміти збитків та багато винятків [35].

Автономне кіберстрахування має різні розділи, які дозволяють адаптувати умови покриття до індивідуальних потреб страхувальників. Страхове покриття включає як збитки першої сторони, так і збитки третьої сторони, що призводять до юридичної відповідальності. Покриття від першої особи захищає від прямих збитків та кишенькових витрат, яких зазнав страхувальник. Зокрема, покриття включає: витрати на відновлення даних, прямі збитки від кіберзлочинів, переривання бізнесу, кібервимагання, судові витрати, витрати на зв'язки з громадськістю для управління репутаційними збитками, витрати на проведення судової експертизи для визначення причини та масштабу порушення або мережевої події. Покриття відповідальності перед третіми особами призначене для захисту від відповідальності за порушення конфіденційності, відповідальності за порушення мережевої безпеки, відповідальності за

шкоду, заподіяну ЗМІ або веб-контенту, а також витрат на захист у зв'язку з регуляторними вимогами щодо захисту приватності [17].

1.2.Дослідження підходів до моделювання страхових ризиків

При моделюванні страхових ризиків існує кілька підходів, які допомагають страховим компаніям оцінити й управляти ризиками. Основні підходи до моделювання страхових ризиків включають статистичний аналіз, стохастичне моделювання та використання математичних моделей ризик-моделювання. Ось їх сутність [31]:

1 Статистичний аналіз: Цей підхід базується на аналізі статистичних даних, що вказують на минулі страхові події. Страхові компанії використовують історичні дані щодо збитків, факторів ризику та інших важливих змінних для розуміння ймовірності страхових подій. Це допомагає визначити середній рівень ризику та розрахувати премії, враховуючи потенційні збитки.

1. Стохастичне моделювання: Цей підхід передбачає використання стохастичних (випадкових) процесів для моделювання страхових ризиків. Він враховує небезпечні події, які можуть мати різні рівні імовірності. Застосовуються методи, такі як марковські ланцюги, моделі Монте-Карло та інші для симуляції різних можливих сценаріїв ризику. Це дозволяє оцінити ризикованість та визначити фінансові наслідки для страхових компаній [30].

2. Математичні моделі ризик-моделювання: Цей підхід використовує математичні моделі для аналізу страхових ризиків. Він базується на теорії ймовірностей, статистиці та інших математичних підходах для оцінки ймовірності страхових подій, розрахунку страхових премій та управління ризиками. Моделі, такі як модель премії за великими збитками (extreme

value theory), модель страхових платежів (loss payment model) та інші, можуть використовуватись для розрахунку ризику й оцінки фінансових наслідків.

Використання цих підходів дозволяє страховим компаніям краще розуміти ризики, з якими вони стикаються, та встановлювати адекватні премії для покриття цих ризиків. Вони також допомагають управляти портфелем страхових ризиків, приймати рішення щодо резервування коштів та розробляти стратегії ризик-управління [33].

Прикладом імітаційного моделювання взаємозалежності рівня безпеки та ризику виникнення кібер-загрози є робота Rainer Bohme та Galina Schwartz, які запропонували комплексну формальну основу для класифікації ринкових моделей кіберстрахування. Автори врахували три аспекти: взаємозалежну безпеку, корельований ризик та інформаційну асиметрію. Автори розглянули кіберстрахування як інструмент вирівнювання стимулів для кращої мережевої безпеки [2].

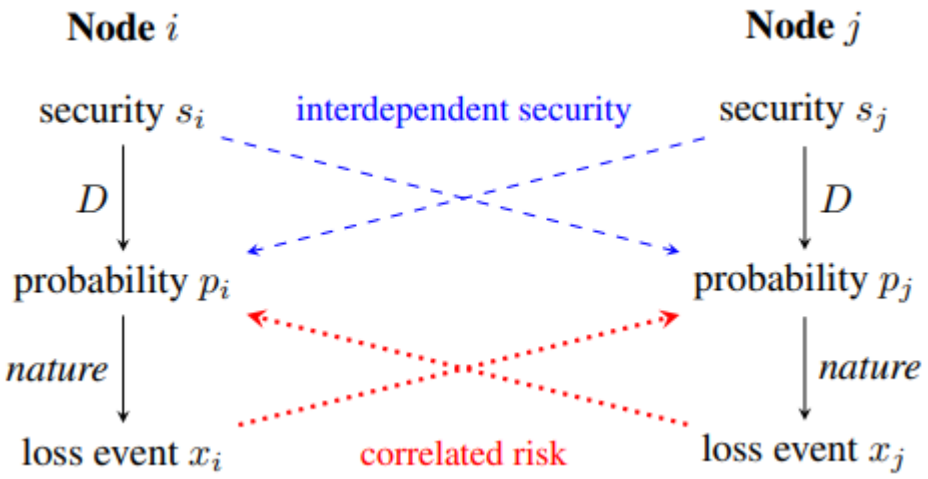

Рисунок 1.1 – Двонаправлена модель, що ілюструє взаємозалежність між безпекою та корельованим ризиком у надходження кібер-ризику

Інше дослдіження показує використання Бета-біноміальної моделі, яка належить до класу узагальнених адитивних моделей розташування,

масштабу і форми (GAMLSS) і може бути підігнана до даних з використанням максимальної штрафної правдоподібності. А також Однофакторної моделі з латентною змінною, де на ймовірність атаки для кожного вузла впливає латентна змінна з двома станами, яку можна інтерпретувати як стан активності джерела глобальної атаки [2].

Для моделювання ризиків у кібер-страхуванні використовується модель Гордона-Лоеба – для прийняття рішень щодо конкуруючих інвестицій у кібербезпеку та кіберстрахування. Оптимальне поєднання інвестицій та страхування відповідно до припущень моделі Гордона-Лоеба досліджується через розгляд витрат та вигод від інвестицій у безпеку разом із придбанням страховки за незалежною ставкою страхового внеску. За експоненціальної (постійна абсолютна несхильність до ризику) та логарифмічної (постійна відносна несхильність до ризику) функцій корисності виявлено, що коли страхова премія є нижчою за певне значення, корисність максимізується за умови страхування та інвестицій у безпеку [16].

Для встановлення цін за послуги кіберстрахування може бути використана актуарна модель на основі Копули для ціноутворення на поліси кіберстрахування [12].

Моделювання системних кіберризиків вимагає моделей ефектів зворотного зв'язку, локальної та глобальної взаємодії, а також стратегічної взаємодії. По-перше, виникнення кіберінцидентів можна врахувати за допомогою процесів Хокса [1] на агрегованому рівні, цьому відношенні процеси Хокса можна інтерпретувати як підхід "зверху вниз". По-друге, моделі епідемічних мереж відображають взаємозв'язок і каскадне поширення ризиків; цей висхідний підхід може зосереджуватися на локальних зв'язках, але також може відображати глобальну взаємодію через агреговані, середні величини поля. Обидва підходи можна розглядати як механічні моделі взаємодії, в яких раціональна або стратегічна поведінка

агентів, як правило, не відображається. На цьому фокусується третій підхід, а саме моделі теорії ігор [8].

Систематичну залежність кіберінцидентів можна моделювати за допомогою процесів Кокса; вони дозволяють врахувати емпіричні особливості, такі як автокореляція кібератак. Процеси Кокса зосереджені на загальних факторах, але вони не моделюють зараження у взаємопов'язаних системах. Альтернативою є процеси Хокса, процеси, що самозбуджуються, які відображають ефекти зворотного зв'язку, специфічну форму системного кіберризику; вони також фіксують стилізований факт автокореляції кількості подій [5, 9, 15].

Взаємопов'язаність є ключовою характеристикою кіберсистем. Системні кіберризики можуть поширюватися і посилюватися в мережах взаємопов'язаних компаній, економічних суб'єктів або фінансових установ. Моделі кібермереж для поширення інфекційних ризиків складаються з наступних трьох ключових компонентів:

1. Мережа (також звана графом), вузли якої представляють компоненти або агентів. Цими суб'єктами можуть бути окремі корпорації, підсистеми комп'ютерів або окремі пристрої. Ребра мережі відповідають можливим каналам переходу, наприклад, IT-з'єднанням або обміну даними/комп'ютерним кодом.

2. Процес поширення в мережі, який моделює розповсюдження заразного кіберризику, наприклад, поширення комп'ютерного вірусу, троянської програми або програми-вимагача.

3. Модель збитків, яка визначає серйозність кіберподій та їхній фінансовий вплив на різних агентів у мережі.

Моделі, що використовуються для прогнозування трендів і аналізу часових рядів, включають AR (авторегресійну модель), ARMA (авторегресійно-рухомий середній модель), ARIMA (авторегресійно-

рухомий середній-інтегрований модель), логістичну регресію та модель з розподіленим лагом:

1. Авторегресійна модель (AR): AR-модель базується на попередніх значеннях залежної змінної. Вона передбачає, що поточне значення залежить від попередніх значень з затримкою. Наприклад, AR(1)-модель передбачає, що поточне значення залежить від попереднього значення з одним періодом затримки [22].

2. Авторегресійно-рухомий середній модель (ARMA): ARMA-модель поєднує авторегресійну компоненту (AR) і рухомий середній (MA). Вона використовує попередні значення залежної змінної та попередні значення помилок моделі для прогнозування майбутніх значень [21].

3. Авторегресійно-рухомий середній-інтегрований модель (ARIMA): ARIMA-модель поєднує авторегресійну компоненту (AR), рухомий середній (MA) та інтегровану компоненту (I). Вона використовує додатковий шлях для управління трендом у часовому ряді, інтегруючи ряд до стаціонарного стану перед застосуванням AR та MA моделей [19].

4. Логістична регресія: Логістична регресія використовується для моделювання ймовірності виникнення події з двома можливими результатами. Вона широко використовується для прогнозування ймовірності бінарних подій, таких як класифікація, споживча поведінка, прогнозування ризиків тощо.

5. Модель з розподіленим лагом: Ця модель враховує затримки у впливі попередніх значень залежної змінної на поточне значення. Вона використовує різні затримки для врахування впливу минулих значень на майбутні.

Ці моделі є лише кількома прикладами методів прогнозування трендів і аналізу часових рядів. В залежності від конкретної задачі та типу даних, можуть бути використані інші моделі, такі як експоненційне згладжування,

GARCH (Generalized Autoregressive Conditional Heteroskedasticity), SVM (Support Vector Machines) та багато інших.

Багатофакторна регресія є потужним інструментом для моделювання страхування кібер-ризиків. Вона дозволяє враховувати вплив різних факторів на страхові збитки та побудувати прогнози на основі цих факторів. Перш ніж побудувати модель, необхідно визначити різні фактори, які можуть впливати на страхові збитки в кібер-сфері. Це можуть бути такі фактори, як розмір компанії, сфера діяльності, рівень кіберзахисту, історія інцидентів тощо [11].

Наступним кроком є збір відповідних даних, які включають інформацію про страхові збитки та значення обраних факторів. Ці дані можуть бути отримані з внутрішніх систем страхових компаній, статистичних даних, даних про інциденти тощо.

За допомогою багатофакторної регресії можна побудувати модель, яка враховує вплив обраних факторів на страхові збитки. У цьому випадку, залежна змінна буде страхові збитки, а фактори виступатимуть як незалежні змінні. Модель буде шукати статистичні залежності між факторами та збитками і визначати коефіцієнти регресії [6].

Після побудови моделі необхідно провести оцінку її якості. Це включає аналіз статистичної значущості коефіцієнтів регресії, визначення показників якості моделі (наприклад, R-квадрат) та проведення тестів на адекватність моделі.

Після валідації моделі можна використовувати її для прогнозування страхових збитків на майбутні періоди. Це можна зробити, використовуючи значення факторів для майбутніх періодів та розраховуючи очікувані страхові збитки за допомогою моделі регресії [18].

Метод експоненційного згладжування є ще одним популярним підходом до прогнозування трендів. Він використовується для прогнозування часових рядів без врахування факторів зовнішнього впливу.

Основна суть методу полягає в тому, що він враховує зважені значення попередніх спостережень, де ваги залежать від їх віддаленості у часі. Згладжування здійснюється шляхом розрахунку середнього значення з попередніх спостережень з використанням певного коефіцієнта згладжування.

Для побудови прогнозів методом експоненційного згладжування необхідно визначити оптимальне значення коефіцієнта згладжування, яке залежить від характеристик досліджуваного часового ряду. Потім застосовується формула для розрахунку прогнозних значень, яка базується на попередньому спостереженні та коефіцієнті згладжування [10].

Загалом, застосування багатофакторної регресії та методу експоненційного згладжування дозволяє моделювати та прогнозувати страхові ризики, забезпечуючи підставу для прийняття обґрунтованих рішень у сфері страхування кібер-ризиків.

1.3.Постановка задачі моделювання

Страхування кібер-ризиків є складною багатогранною задачею, оскільки залежить від великої кількості факторів, які не пов’язані між собою та мають як суб’єктивну так і об’єктивну сторону, а саме обсяг страхового ринку, готовність страхувальників витрачати кошти на покриття цього ризику, а також активністю й обсягом кібер-атак. Окрім того, справедливо зазначити, що моделювання тенденцій розвитку страхування кібер-ризиків стикається з такою проблемою, як незначний період дослідження, оскільки сам процес діджиталізації економіки нетривалий в часі, а страхування кібер-ризиків ще молодше.

Таким чином, основним завданням на наш погляд в розрізі моделювання тенденцій розвитку страхування кібер-ризиків є прогнозування. Саме процес прогнозування дозволяє визначити декілька трендів (варіантів) становлення будь-якого процесу та з'ясувати яким чином кожен зі стейкхолдерів повинен себе вести в тій чи іншій ситуації.

Отже, в рамках нашого дослідження необхідно обрати такий інструментарій прогнозування та такі вхідні дані, які б максимально описували перспективи кібер страхування. На наш погляд, прогнозувати необхідне не безпосередньо параметри характеристики процесу страхування кібер-ризиків, а фактори, які описують ймовірність настання або, навіть рівень очікуваності страхувальників, кібер шоку [4].

Задачами дослідження є, по-перше, визначення взаємозалежності базового показника характеристики страхування кібер-ризиків (світові премії з кіберстрахування) від релевантних показників характеристики очікувань потенційних страхувальників, по-друге, прогнозування за допомогою відповідних методів релевантних показників, а, по-третє, знаходження відповідно до встановленого рівняння багатофакторної регресії значення світових премій з кіберстрахування за кожний наступний період часу.

Проведення практичних розрахунків запропоновано здійснювати за допомогою таких програмних засобів, як Statistica 11 та Microsoft Excel.

Отже, задачею цього дослідження є побудова економіко-математичної моделі прогнозування розвитку страхування кібер-ризиків

РОЗДІЛ 2 ПОБУДОВА ЕКОНОМІКО-МАТЕМАТИЧНОЇ МОДЕЛІ ПРОГНОЗУВАННЯ ТЕНДЕНЦІЙ РОЗВИТКУ СТРАХУВАННЯ КІБЕР-РИЗИКІВ

2.1 Опис вхідного масиву даних дослідження

Зупиняючись на дослідженні вхідного масиву інформації для побудови прогнозу розвитку страхування кібер-ризиків, зауважимо, що інформаційна база включатиме три блоки показників: перший, результативний, характеризує динаміку становлення ринку кіберстрахування, другий, релевантні показники, описують очікування страхувальників щодо можливості настання кіберризику, а третій це вартість даних послуг страхування. Так, до першого блоку відносимо – світові премії з кіберстрахування, до другої – частка організацій, які зазнали принаймні однієї успішної кібератаки; частка респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «вірогідною»; індекс загрози, що відображає загальну стурбованість щодо кібератак; індекс занепокоєння безпекою, а до третього – темпи зростання тарифів з кіберстрахування.

Вибір показників другого блоку обумовлений тим, що за результатами дослідження компанії KPMG, більше ніж 60% опитаних топ-менеджерів світових компаній наполягають на тому фактів, що кібератаки обов’язкові для будь-якого економічного агента. Виходячи з цього, все більше компаній реального та фінансового секторів економіки почали розробляти системи індивідуального захисту конфіденційної інформації. Суб’єкти господарювання концентрують власні зусилля як на превентивних мірах протидії кібератакам, так і на засобах пост-реагування, основними з яких в

сучасних умовах є страхування. Саме кіберстрахування, у разі настання ризику, дозволяє здійснити покриття фінансових збитків, закамульованих в результаті порушення роботи інформаційній системі компанії, відшкодувати штрафні санкції та компенсувати репутаційні втрати.

Чотири релевантні показники визначені експертним шляхом на основі Cyberthreat Defense Report. Цей звіт щорічно готує CyberEdge Group, використовуючи результати опитування менеджерів різних компаній з 17 країн світу. Аналітичне згрупування розглянутих вище показників проведено за допомогою таблиці 2.1.

Так, на основі аналізу вхідного масиву даних дослідження, справедливо зауважити, що світові премії з кіберстрахування неодмінно зростали, досягнувши у 2022 р. значення в 11 млрд дол. США, це майже у чотири рази більше ніж значення 2016 р. Це свідчить про активне зростання попиту на страхування ризиків пов’язаних з наслідком реалізації кібератак протягом 2016-2022 рр.

Досліджуючи релевантні показники опису рівня стурбованість суб’єктів господарювання щодо кіберзагроз, зазначимо, що частка організацій, які зазнали принаймні однієї успішної кібератаки починаючи з 2016 року не зменшувалась нижче ніж рівень у 75%, в середньому щорічний темп приросту складав більше ніж 4%. Це свідчить про той факт, що кожного року збільшується не тільки чисельність підприємств та установ, які піддаються кібер атакам, але й частота даних атак на них.

Другий показник цієї групи частка респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «вірогідною», описує очікування суб’єктів господарювання відносно рівня успішності кібер атак на їх установу. Так, протягом 2015-2018 рр. цей показник складав більше ніж 50%, а вже наступні чотири роки (2019-2022 рр.) більше ніж 65% менеджерів вважали, що протягом року їх компанія майже 100% буде актована хакерами.

Таблиця 2.1 – Інформаційна база прогнозування розвитку страхування кібер-ризиків за 2014-2022 рр.

Показник	Рік								
	2014	2015	2016	2017	2018	2019	2020	2021	2022
Світові премії з кіберстрахування, млрд. дол. США	2,5	3	3,6	4,3	5,2	6,2	7,5	9,1	11,2
Частка організацій, які зазнали принаймні однієї успішної кібератаки, %	61,9	70,5	75,6	79,2	77,2	78,0	80,7	86,2	85,3
Частка респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «вірогідною», %	38,1	51,9	62,1	61,5	62,3	65,2	69,3	75,6	76,1
Індекс загрози, що відображає загальну стурбованість щодо кібератак, од	3,61	3,26	3,71	3,75	3,54	3,52	3,79	3,88	3,88
Індекс занепокоєння безпекою, од	2,94	2,99	3,37	3,41	3,18	3,19	3,53	3,65	3,64
Темп зростання страхових тарифів з кіберстрахування, %	70	55	50	67	88	76	110	106	136

Джерело: складено авторкою на основі [**Помилка! Джерело посилання не знайдено.**, 7]

Третій та четвертий показники досліджуваної вибірки описують рівень стурбованості менеджерів компаній щодо кіберзагроз. Як індекс загрози, так й індекс занепокоєння безпекою змінювались нерівномірно то зростаючи, то спадаючи.

Циклічна динаміка досліджуваних показників з незначним розмахом прослідковується починаючи з 2015 р., проте останні два роки дані індекси неодмінно зростали. Таким чином, справедливо зробити висновок, що менеджери міжнародних компаній в різних країнах світу беззаперечно стурбовані та розуміють загрозу реалізації кібератак, крім того, вони реально оцінюють і наростаючу руйнівну силу кібератак й низький рівень захищеності власної інформаційної системи, а тим більше розуміють рівень фінансових втрат, який може бути спричинений цими подіями.

Проте, зупиняючись на актуальності поставленої задачі, щодо прогнозування рівня розвитку кіберстрахування зауважимо, що не зважаючи на зростаючий тренд обсягу валових премій за цим видом страхування та розуміння суб'єктами страхування наростаючої загрози від кібератак, неодмінне збільшення цього сегменту страхового ринку є спірним питанням. Це пов'язано з тим, що цілком ймовірна ситуація, коли частота кібератак буде значна, обсяг збитків, які вони спричиняють буде великий, а рівень інформаційної безпеки компанії навпаки низький. Тому, вартість кіберстрахування для компаній, особливо невеликих, може бути непомірною.

Досліджуючи безпосередньо темпи зростання вартості кіберстрахування, зауважимо, що починаючи з 2020 р. щорічні темпи зростання тарифів з цього виду страхування перевищили 100%, а попередні періоди (20014-2019 рр.) цей показник становив не менше 50%.

Безумовно, рівень насиченості ринок кіберстрахування ще довго не настане, проте, й активне зростання може значно сповільнитись. Отримані результати важливі не тільки для страхових компаній з точки зору розвитку якості та різноманітності послуг з кіберстрахування, але й з точи зору вимог до

страхувальників з приводу захищеності їх внутрішньої бази даних та інформаційної системи.

Отже, необхідно розробити та формалізувати такий механізм визначення прогнозних значень розвитку кіберстрахування, який би враховував як поточні тенденції ринку, так і очікування клієнтів, а також темп приросту вартості даного виду страхування. Саме від цих складових наразі залежить розвиток ринку страхування кібер ризиків. Тільки за умови зацікавленості усіх стейкхолдерів ринок може розвиватись страховики будуть диференціювати послуги, а страхувальники підтримувати стабільний попит на даний вид послуг.

2.1 Розробка методичних засад прогнозування тенденцій розвитку страхування кібер-ризиків

Отже, переходячи безпосередньо до побудови економіко-математичної моделі до прогнозування розвитку страхування кібер-ризиків зауважимо, що цей процес запропоновано реалізувати в чотири кроки:

1. Побудова багатофакторної регресії залежності обсягів світових премій з кіберстрахування від 1) частки організацій, які зазнали принаймні однієї успішної кібератаки; 2) частки респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «вірогідною»; 3) індексу загрози, що відображає загальну стурбованість щодо кібератак; 4) індексу занепокоєння безпекою; 5) темпів зростання тарифів з кіберстрахування за 2014-2022 рр.

2. Прогнозування на 2023-2025 рр. за допомогою експоненціального згладжування частки організацій, які зазнали принаймні однієї успішної кібератаки; частки респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «вірогідною»; індексу загрози,

що відображає загальну стурбованість щодо кібератак; індексу занепокоєння безпекою; темпів зростання тарифів з кіберстрахування.

3. На основі прогнозованих за допомогою експоненційного згладжування релевантних показників провести прогнозування обсягів світових премій з кіберстрахування на 2023-2025 рр.

4. Провести дослідження якості моделі.

Отже, розглянемо кожен з етапів більш детально. На першому етапі необхідно визначити специфікацію моделі взаємозв'язку між обсягом світових премій з кіберстрахування та часткою організацій, які зазнали принаймні однієї успішної кібератаки, часткою респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «вірогідною», індексом загрози, що відображає загальну стурбованість щодо кібератак, індексом занепокоєння безпекою, темпами зростання тарифів з кіберстрахування у вигляді лінійної багатофакторної регресії (2.1):

$$WIP = a_0 + a_1 OK + a_2 SKA + a_3 IT + a_4 IS + a_5 TT \quad (2.1)$$

де WIP – обсяг світових премій з кіберстрахування,

OK – частка організацій, які зазнали принаймні однієї успішної кібератаки,

SKA – частка респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «вірогідною»,

IT – індекс загрози, що відображає загальну стурбованість щодо кібератак,

IS – індекс занепокоєння безпекою,

TT – темпів зростання тарифів з кіберстрахування,

a_0 – вільний член,

$a_1 \ldots a_5$ – параметри рівняння.

Формалізована взаємозалежність дозволяє встановити напрямок та сили впливу кожного з релевантних показників на результативний.

На другому етапі необхідно провести прогнозування статистичних показників схильності до кіберстрахування на основі експоненціального згладжування.

В загальному вигляді модель експоненціального згладжування набуває наступного виду:

$$S_t = \alpha \cdot X_t + (1 - \alpha) \cdot S_{t-1} \tag{2.2}$$

де X_t – значення часового ряду в конкретний проміжок t;

α – параметр згладжування. Він може приймати значення нуль за умови ігнорування усіх поточних спостережень, а також одиницю у випадку цілковитого ігнорування поточних спостережень;

S_t, S_{t-1} – експоненціально згладжений рівень показника в момент часу t або (t-1).

Кожен наступний прогноз на один період вперед визначається наступним чином:

– за умови адитивного моделювання:

$$\begin{aligned} F_t &= S_t + I_{t-p} \\ I_t &= I_{t-p} + \delta \cdot (1 - \alpha) \cdot e_t \end{aligned} \tag{2.3}$$

– за умови мультиплікативного моделювання:

$$\begin{aligned} F_t &= S_t \cdot I_{t-p} \\ I_t &= I_{t-p} + \delta \cdot (1 - \alpha) \cdot e_t / S_t \end{aligned} \tag{2.4}$$

де δ – сезонний компонент згладжування, визначається для сезонних моделей;

S_t – просте експоненціально згладжене значення в момент часу t;

I_{t-p} – згладжений сезонний фактор (t мінус тривалість сезону);

e_t – залишки у момент часу t.

Зважаючи на поведінку вхідних даних моделі та поставлені завдання дослідження запропоновано розглядати тільки адитивну складову експоненціального згладжування.

Отже, з метою прогнозування на базі експоненціального згладжування у випадку характеристики часових рядів, як таких, що містять як експоненційну компоненту тренду, так і адитивну сезонну компоненту, необхідно здійснити додаткове обчислення згладжених значень для 1-ого періоду на основі початкових значень сезонних компонент. З метою визначення цих параметрів застосовують метод класичної сезонної декомпозиції. Так, для прогнозу початкового сезонного компоненту (S_0), а також поточного тренду (T_0) застосовують наступні формули:

$$T_0 = exp\left(\frac{\left(log(M_k) - log(M_1)\right)}{p}\right)$$
$$S_0 = exp\left((log(M_1) - p \cdot log(T_0)/2)\right) \quad (2.5)$$

де k – кількість повних сезонних циклів;

M_k – середнє значення для останнього сезонного циклу;

M_1 – середнє значення для першого сезонного циклу;

p – тривалість сезонного циклу.

Цікавим є випадок побудови прогнозу з використанням експоненціального згладжування для часових рядів, для яких характерно затухання тренду та адитивна сезонна компонента. Актуальність використання зазначеного підходу до моделювання виникає тоді, коли значення рівня часового ряду буде зростати, у той же час, ця тенденція буде повільно зникати протягом певного часу по мірі насичення, паралельно з цим прослідковується присутність сезонних коливань у вигляді адитивної компоненти. Отже, з метою визначення згладжених значень першого періоду дослідження, необхідні

початкові значення для сезонних параметрів. Паралельно з цим, з метою розрахунку прогнозу для першого спостереження в серії, потрібні обидві оцінки S_0 та T_0, що визначаються наступним чином:

$$T_0 = \frac{1}{\phi} \cdot \frac{M_k - M_1}{(k-1) \cdot p} \tag{2.6}$$

$$S_0 = M_1 - p \cdot T_0/2$$

де ϕ – змінна згладжування тренду, характерний моделям із затухаючим трендом.

На третьому етапі формалізації науково-методичного підходу до визначення трендів розвитку кіберстрахування спрогнозовані значення части організацій, які зазнали принаймні однієї успішної кібератаки, частки респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «вірогідною», індексу загрози, що відображає загальну стурбованість щодо кібератак, індексу занепокоєння безпекою, темпаму зростання тарифів з кіберстрахування підставляють у формулу 2.1 отримуючи тим самим обсяг світових премій з кіберстрахування за період 2023-2025 рр.
На завершальному етапі проводиться оцінювання якості моделі за допомого розрахунку критерію Стьюдента, коефіцієнта детермінації, рівня недовіри до результатів моделювання, та критерію Вальда.

2.3 Практична реалізація моделі прогнозування тенденцій розвитку страхування кібер-ризиків та перевірка її на адекватність

Використовуючи інструментарій MS Excel на основі даних таблиці 2.1 проведемо практичні розрахунки параметрів рівняння 2.1. Отже:

$$WIP = 1{,}056 + 0{,}00035OK + 0{,}00014SKA + 0{,}00148IT + 0{,}00075IS - 0{,}000167TT \quad (2.7)$$

де WIP – обсяг світових премій з кіберстрахування,

OK – частка організацій, які зазнали принаймні однієї успішної кібератаки,

SKA – частка респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «вірогідною»,

IT – індекс загрози, що відображає загальну стурбованість щодо кібератак,

IS – індекс занепокоєння безпекою,

TT – темпів зростання тарифів з кіберстрахування.

Справедливість побудованої моделі підтверджуються наступними показниками якості моделі: t-критерій дорівнює 7,2; p-рівень дорівнює 0,0000; R=0,982; χ^2= 202,56. Тобто всі показники перевищують свої мінімальні значення.

Таким чином, справедливо зауважити, що збільшення на 1% частки організацій, які зазнали принаймні однієї успішної кібератаки призводить до збільшення обсягу світових премій зі страхування кбіер-ризиків на 350 тис дол. США. У той же час, не безпосередній факт, а тільки очікування менеджерів компаній щодо успішної кібератаки на організацію протягом наступних 12 місяців менше впливають на результативний показник, так 1% його зростання призведе до збільшення світових премій на 140 тис дол. США.

У той же час, різниця між впливом на результативний показник досліджуваних індексів відрізняється ще на більше значення. Так, зростання на одиницю індексу загрози, що відображає загальну стурбованість щодо кібератак призводить до збільшення валових страхових премій з кіберстрахування на 1,48 млн дол. США. Паралельно з цим, зростання індексу занепокоєння безпекою призводить до збільшення премій зі страхування кібер ризиків на 750 тис дол. США., що вдвічі менша ніж вплив попереднього індексу.

Отже, справедливо зробити висновок, що до активного зростання обсягів кіберстрахування призводять реальні факти кібератак на компанії, а також загальне відчуття менеджерів компаній щодо кібератак, як явища. Єдиним

показником, що впливає на зростання ринку кіберстрахування є тарифи з кіберстрахування, так збільшення темпу приросту за ними в межах року призводить до зменшення обсягу страхових премій на 160 тис дол. США.

Переходячи до прогнозу релевантних показників на 2023-2025 рр. зазначимо, що на основі даних таблиці 2.1, модель експоненціального згладжування для частки організацій, які зазнали принаймні однієї успішної кібератаки (2.8) та частки респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «вірогідною» (2.9) набувають вигляду:

$$OK1_t = \alpha \cdot X_t + (1-\alpha) \cdot S_{t-1} + I_{t-p},\ I_t = I_{t-p},\ \text{S0=17,6}$$

$$OK2_t = LT_t + \alpha \cdot X_t + (1-\alpha) \cdot S_{t-1} + I_{t-p},\ I_t = I_{t-p} + (1-\alpha) \cdot e_t,\ \text{S0=-8,2 T0=3,144} \quad (2.8)$$

$$OK3_t = DT_t + \alpha \cdot X_t + (1-\alpha) \cdot S_{t-1} + I_{t-p},\ I_t = I_{t-p} + (1-\alpha) \cdot e_t,\ \text{S0=-12,2 T0=3,72}$$

$$SKA1_t = \alpha \cdot X_t + (1-\alpha) \cdot S_{t-1} + I_{t-p},\ I_t = I_{t-p},\ \text{S0=1,6}$$

$$SKA2_t = LT_t + \alpha \cdot X_t + (1-\alpha) \cdot S_{t-1} + I_{t-p},\ I_t = I_{t-p} + (1-\alpha) \cdot e_t,\ \text{S0=-2,1 T0=2,14} \quad (2.9)$$

$$SKA3_t = DT_t + \alpha \cdot X_t + (1-\alpha) \cdot S_{t-1} + I_{t-p},\ I_t = I_{t-p} + (1-\alpha) \cdot e_t,\ \text{S0=-8,1 T0=1,74}$$

де $OK1_t, SKA1_t$ – адитивна модель сезонності;

$OK2_t, SKA2_t$ – тренд-сезонна адитивна модель;

$OK3_t\ SKA3_t$ – тренд-сезонна адитивна модель із затухаючою тенденцією.

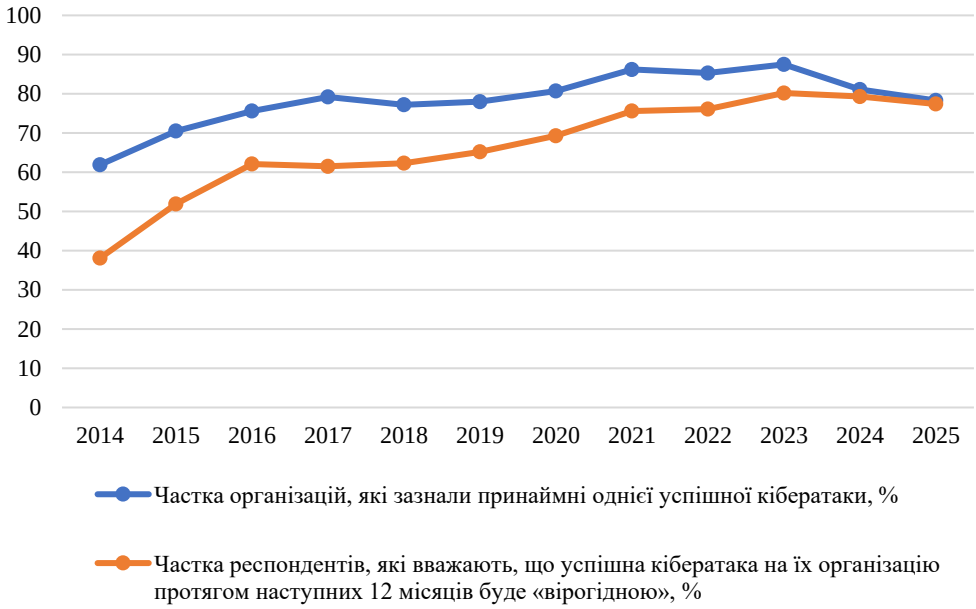

Рисунок 2.1 – Динаміка фактичних та прогнозних значень частки організацій, які зазнали принаймні однієї успішної кібератаки та частки респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «вірогідною» за 2014-2025 рр.

Отже справедливо зауважити, що прогнозні значення досліджуваних часток після 2023 р. починають поступово зменшуватись. Проте якщо частка організацій, яка зазнала принаймні однієї успішної кібератаки скоротилась за 2024-2025 рр. скоротилась на 9,2%, то частка респондентів, які вважають, що успішна кібератака на їх організацію протягом наступних 12 місяців буде «вірогідною» тільки на 2,8%.

Визначаючи за тією ж логікою та математичним інструментарієм досліджувані індекси (рисунок 2.2) зауважимо, що індекс занепокоєння безпекою неодмінно зменшується починаючи з 2022 р., тоді як індекс загрози, що відображає загальну стурбованість щодо кібератак, починає свій спадний тренд у 2023 р. зменшення даних індексів на нашу думку повинно бути пов’язано з завершенням війни та більш обнадійливою ситуацією в державі.

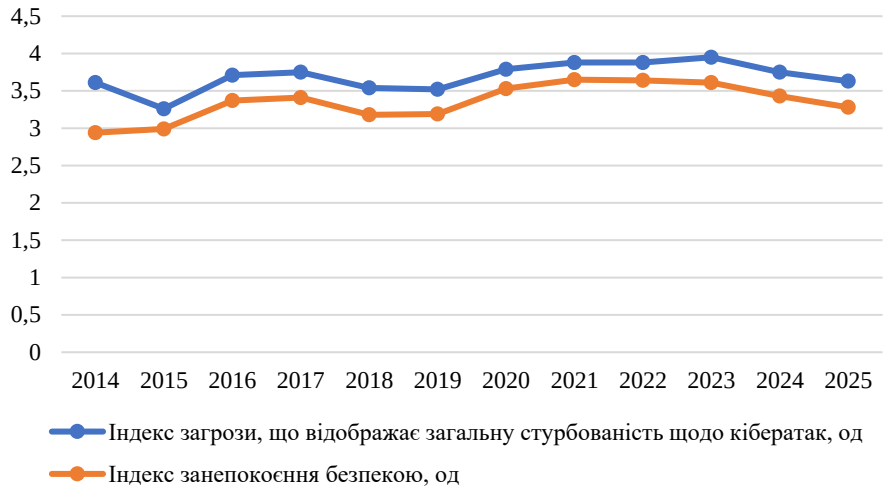

Рисунок 2.2 – Динаміка фактичних та прогнозних значень індексу загрози, що відображає загальну стурбованість щодо кібератак та індексу занепокоєння безпекою за 2014-2025 рр.

Зупиняючись на прогнозах динаміки тарифів з кіберстрахування (рисунок 2.3) зазначимо, що вони неодмінно зростають починаючи з 2022 р., цей тренд не змінився і в прогнозні 2023-2025 рр. прийому у 2025 р. прогнозний темп зростання рівня тарифів з цього виду страхування склав 153%. Це свідчить про те, що страхові послуги будуть розвиватись та охоплювати покриття все більших кібер-ризиків, а це безумовно призведе до зростання вартості.

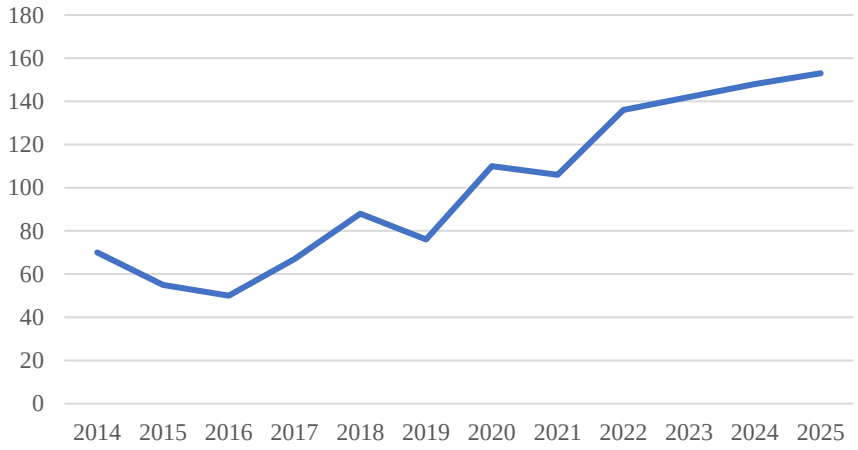

Рисунок 2.3 – Динаміка фактичних та прогнозних значень темпів зростання тарифів з кіберстрахування за 2014-2025 рр.

Спрогнозувавши п’ять релевантних показників впливу на тенденції розвитку кіберстрахування в світі підставимо їх у рівняння 2.7 та знайдемо обсяг світових премій зі страхування кібер-ризиків у 2023-2025 рр.

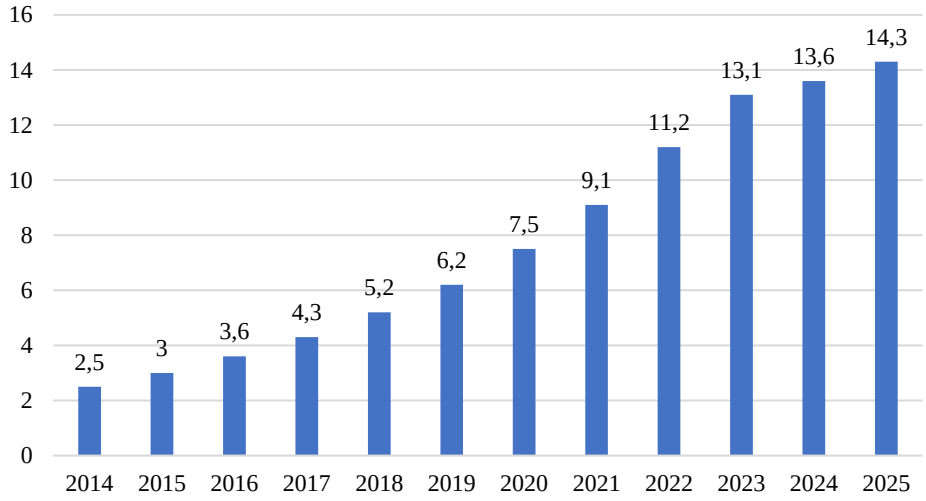

Рисунок 2.4 – Динаміка фактичних та прогнозних значень обсяг світових премій з кіберстрахування за 2014-2025 рр.

Таким чином, справедливо зробити висновок, що починаючи з 2024 р. темпи зростання обсягів світових премій зі страхування кібер-ризиків значно сповільняться і складуть в середньому щорічно 4,5%, проте загальний поступальний тренд збережеться. Це на нашу думку буде зумовлено по-перше, зростанням тарифів на цей вид страхування, а відповідно неспроможністю малих та середніх компаній включати у свій бюджет такі витрати, а по-друге, все ж таки вкладанням великих корпорацій власних ресурсів у системи цифрової безпеки, що зважаючи на молодий ринок кіберстрахування не дозволяє змінити тренд їх безпекового менеджменту. Проте з кожним роком актуальність страхування кібер ризиків буде зростати і можливо загальний тренд розвитку не носитиме стрімкого зростання, проте абсолютні значення валових премій будуть зростати.

ВИСНОВКИ

В ході виконання кваліфікаційної роботи було:

– розкрито зміст кібер-ризиків;

– проаналізовано особливості страхування кібер-ризиків;

– досліджено підходи до моделювання страхових ризиків;

– проведена постановка задачі моделювання;

– сформовано інформаційну базу дослідження;

– розроблена модель прогнозування тенденцій розвитку страхування кібер-ризиків;

– проведена практична реалізацію моделі прогнозування тенденцій розвитку страхування кібер-ризиків;

– перевірена якість моделі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Awiszus, K., Knispel, T., Penner, I. et al. Modeling and pricing cyber insurance. Eur. Actuar. J., 2023. № 13. P. 1-53. URL: https://doi.org/10.1007/s13385-023-00341-9

2. Böhme, R., & Kataria, G. Models and Measures for Correlation in Cyber-Insurance. *Workshop on the Economics of Information Security*, 2006. URL: https://core.ac.uk/download/pdf/162458449.pdf

3. Brychko, M., Bilan, Y., Lyeonov, S., & Mentel, G. (2021). Trust crisis in the financial sector and macroeconomic stability: A structural equation modelling approach. Economic Research-Ekonomska Istrazivanja, 34(1), 828-855. DOI: https://doi.org/10.1080/1331677X.2020.1804970.

4. Cyber insurance – statistics & facts. STATISTA. URL: https://www.statista.com/topics/2445/cyber-insurance/#topicOverview

5. Cyber Insurance. Beinsure. URL: https://beinsure.com/cyber/

6. Cyber Security Insurance Market – Growth, Trends, Forecast (2020 - 2025) Published: Jan 2020. Pages : 100. Publisher : Mordor Intelligence. Report code : ASDR-507856. URL: https://www.asdreports.com/market-research-report-507856/cyber-security-insurance-market-growth-trends-forecast

7. Cyberthreat Defense Report. URL: https://cyber-edge.com/cyberthreat-defense-report-2022/

8. Didenko, I., Sidelnyk, N. Insurance Innovations as a Part of the Financial Inclusion. Business Ethics and Leadership. 2021. 5(1), 127-135. DOI: https://doi.org/10.21272/bel.5(1).127-135.2021 (0,81 друк. арк.).

9. Didenko, I., Sidelnyk, N. Society's Readiness for Modern Challenges of the Insurance Market: Bibliometric Analysis. Financial Markets, Institutions and Risks. 2021. 5(1), 116-125. DOI: https://doi.org/10.21272/fmir.5(1).116-125.2021

10. Eckert C., Gatzert N., Schubert M.Analyzing spillover effects from data breaches to the US (cyber) insurance industry, *The European Journal of Finance*, 2023. №29(6). P. 669-692. DOI: 10.1080/1351847X.2022.2090267

11. Farkas S., Lopez O., Thomas M. Cyber claim analysis through Generalized Pareto Regression Trees with applications to insurance, 2020. P. 1-41. URL: https://hal.science/hal-02118080v2#

12. Hemantha S.B. Herath and Tejaswini C. Herath. Copula-based actuarial model for pricing cyber-insurance policies. *Insurance Markets and Companies*, 2011. №2(1). P. 7-20. URL: https://www.businessperspectives.org/images/pdf/applications/publishing/templates/article/assets/3934/IMC_2011_1_Herath.pdf

13. Kerner, S.M. 34 cybersecurity statistics to lose sleep over in 2023. *TechTarget*, 2023. URL: https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020

14. Polinkevych, O., Glonti, V., Baranova, V., Levchenko, V., & Yermoshenko, A. (2021). Change of business models of Ukrainian insurance companies in the conditions of COVID-19. Insurance Markets and Companies, 12(1), 83-98. DOI: http://dx.doi.org/10.21511/ins.12(1).2021.08.

15. Seliverstova, L. and Tkachenko, N. (2020). Trends in the development of the ukrainian insurance market, Investytsiyi: praktyka ta dosvid, vol. 3, pp. 10–14. DOI: 10.32702/2306-6814.2020.3.10 .

16. Skeoch, R.K. Henry. Expanding the Gordon-Loeb model to cyber-insurance. Computers & Security, 2022. № 112(102533). URL: https://www.sciencedirect.com/science/article/abs/pii/S0167404821003576

17. Strupczewski, G. 2018. Current state of the cyber insurance market. *Proceedings of Economics and Finance Conferences 6910062, International Institute of Social and Economic Sciences*. URL: https://ideas.repec.org/p/sek/iefpro/6910062.html

18. Tiutiunyk, I., Drabek, J., Antoniuk, N., Navickas, V., & Rubanov, P. (2021). The impact of digital transformation on macroeconomic stability: Evidence from EU countries. Journal of International Studies, 14(3), 220-234. DOI: https://doi.org/10.14254/2071-8330.2021/14-3/14.

19. Tsymbaliuk, I., Pavlikha, N., Zelinska, O., Ventsuryk, A., & Radko, A. (2021). Assessing the level of competitiveness of the insurance sector during economic crises: The example of Ukraine. Insurance Markets and Companies, 12(1), 72-82. DOI: http://dx.doi.org/10.21511/ins.12(1).2021.07.

20. Valinkevych, N., Polchanov, A., & Kovalenko, Y. (2020). A strategy of insurance market development in conditions of latent military conflict in ukraine. Economic Annals-XXI, 182(3-4), 15-24. doi:10.21003/EA.V182-02.

21. Vieriezubova, T., & Levchenko, V. (2017). Openness of the insurance market for foreign entities: methodology and experience of Ukraine. Financial Markets, Institutions and Risks, 1(2), 87-95. DOI: http://doi.org/10.21272/fmir.1(2).87-95.2017.

22. Yanyshyn, Y., Bryk, H. & Kashuba, Y. (2019). Problems and Perspectives of Internet-Insurance in Ukraine. Marketing and Management of Innovations, 4, 31-38. DOI: http://doi.org/10.21272/mmi.2019.4-03.

23. Yarovenko, H., Bilan, Y., Lyeonov, S., & Mentel, G. (2021). Methodology for assessing the risk associated with information and knowledge loss management. Journal of Business Economics and Management, 22(2), 369-387. DOI: https://doi.org/10.3846/jbem.2021.13925.

24. Yelnikova, Y., & Golochalova, I. (2020). Social Bonds as an Instrument of Responsible Investment. Financial Markets, Institutions and Risks, 4(4), 119-128. DOI: https://doi.org/10.21272/fmir.4(4).119-128.2020.

25. Братюк, В. П. (2015). Сутність кібер-злочинів та страховий захист від кіберризиків в Україні. Актуальні проблеми економіки, 9, 421-427. URL: http://nbuv.gov.ua/UJRN/ape_2015_9_54

26. Васильєва Т.А., Діденко І.В., Сідельник Н.Ю., Єфіменко А.Ю. (2022). Аналіз тенденцій розвитку страхових інновацій. Вісник СумДУ. Серія Економіка, 4, 267-273. DOI: 10.21272/1817-9215.2022.4-28.

27. Журавка Ф. О., Журавка О. С., Небаба Н. О. (2019). Проблемні аспекти сталого розвитку вітчизняного ринку страхування життя в умовах глобалізації. Інвестиції: практика та досвід, 5, С. 5-8. DOI: 10.32702/2306-6814.2019.5.

28. Журавка, Ф., Діденко , І., Маргасова, В., & Басанець, С. (2022). Моделювання динаміки розвитку страхового ринку в країнах OECD. Modeling the development of the economic systems, (4), 144–152. https://doi.org/10.31891/mdes/2022-6-19.

29. Ільчук, В. П., Парубець, О. М., Сугоняко, Д. О. (2018). Інноваційні підходи до розвитку ринку кіберстрахування в Україні. Ефективна економіка, 5. URL: http://www.economy.nayka.com.ua/?op=1&z=6295.

30. Інфографіка дослідницької компанії «Venture Scanner». URL: https://www.venturescanner.com/insurance-technology/.

31. Кіберзлочинність в Україні за 5 років зросла у понад два рази. URL: https://suspilne.media/65849-kiberzlocinnist-v-ukraini-za-5-rokiv-zrosla-u-ponad-dva-razi-avakov/.

32. Коваль, Н. В. (2016) Соціально-економічна нерівність в Україні та світі: проблеми оцінювання та шляхи їх вирішення. Економіка та держава, 2, 46-50. URL: http://nbuv.gov.ua/UJRN/ecde_2016_2_12

33. Кострач Л. М., Рудь Л. О. (2015). Тенденції розвитку страхових компаній в Україні. Збірник наукових праць Національного університету державної податкової служби України, №2, С. 135–153.

34. Маргасова В. Г., Коваленко Д. П. (2019). Проблемні питання функціонування страхового ринку України та особливостей його пруденційного регулювання. Науковий вісник Полісся, № 3 (19), С. 17–21. DOI:10.25140/2410-9576-2019-3(19)-17-21.

35. Нагайчук, Н. Г., Третяк, Н. М., Ткаленко, О. (2019). Страхування в системі управління кібер-ризиками підприємства в умовах цифрової економіки. Фінансовий простір, 1 (33), 97-111. URL: http://nbuv.gov.ua/UJRN/Fin_pr_2019_1_8

36. Пахненко О.М., Журавка О.С., Подгорна В.О., Сухомлин А.А. (2019). Аналіз конкурентних позицій страхових компаній на ринку «нон-лайф» страхування в Україні. Вісник Сумського державного університету. Серія Економіка, № 2, С. 88-94 DOI: 10.21272/ 1817-9215.2019.2-11.

37. Петрук О.М., Полчанов А.Ю., Ніколаєнко С.М., Дячек С.М. (2023) Антикризове фінансове управління страховими компаніями, Ефективна економіка, №4. DOI: https://doi.org/10.32702/2307-2105.2023.4.5.

38. Премії з кіберстрахування у 2020 році. URL: https://forinsurer.com/news/21/04/26/39654.

39. Приказюк, Н. В., Гуменюк, Л. С. (2020). Кібер-страхування як важливий інструмент захисту підприємств в умовах цифровізації економіки. Електронне наукове фахове видання «Ефективна економіка». 4. URL: http://www.economy.nayka.com.ua/pdf/4_2020/8.pdf

40. Сідельник Н. Ю. (2021). Кіберстрахування як дієвий спосіб зниження ризиків від кібершахрайств. Всеукраїнська науково-практична конференція «Регіональні особливості злочинності: сучасні тенденції та стратегії протидії». Кривий Ріг, С. 354 – 357. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/14423/1/%D0%97%D0%91%D0%86%D0%A0%D0%9A%D0%90_1%282%29.pdf.

ДОДАТОК А

SUMMARY

Borschenko K. Yu. Economic and mathematical modeling of trends in the development of cyber risk insurance. Qualification work of a bachelor. Sumy State University, Sumy, 2023.

The work reveals the content of cyber risks; investigates the features of cyber risk insurance; investigates approaches to modeling insurance risks; defines the modeling problem; forms the information base of the study, develops a model for forecasting trends in the development of cyber risk insurance; implements the practical implementation of the model for forecasting trends in the development of cyber risk insurance; checks the quality of the model.

Keywords: cyber insurance, cyber risks, forecasting, economic and mathematical modeling, exponential smoothing.

АНОТАЦІЯ

Борщенко К. Ю. Економіко-математичне моделювання тенденцій розвитку страхування кібер-ризиків. Кваліфікаційна робота бакалавра. Сумський державний університет, Суми, 2023 р.

В роботі розкрито зміст кібер-ризиків; досліджено особливості страхування кібер-ризиків; досліджено підходи до моделювання страхових ризиків; визначено постановку задачі моделювання; сформовано інформаційну базу дослідження, розроблено модель прогнозування тенденцій розвитку страхування кібер-ризиків; здійснено практичну реалізацію моделі прогнозування тенденцій розвитку страхування кібер-ризиків; перевірено якість моделі.

Ключові слова: кібер-страхування, кібер-ризики, прогнозування, економіко-математичне моделювання, експоненційне згладження.