НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)

«_____»_____2025 р.

Магістерська дисертація

на здобуття ступеня магістра

за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»
спеціальності 125 «Кібербезпека та захист інформації»

на тему: Оцінювання ефективності заходів кіберзахисту у фінансовому секторі за допомогою моделі Cyber Value-at-Risk

Виконав: здобувач вищої освіти II курсу, групи ФБ - 41мп
(шифр групи)

Заріцький Олександр Васильович
(прізвище, ім'я, по батькові) (підпис)

Керівник: к.т.н, доцент, Гальчинський Леонід Юрійович
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент:
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2025

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – другий (магістерський)
Спеціальність – 125 «Кібербезпека та захист інформації»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Дмитро ЛАНДЕ
(підпис)

«___»_____2025 р.

ЗАВДАННЯ
на магістерську дисертацію здобувачу вищої освіти

Заріцький Олександр Васильович
(прізвище, ім'я, по батькові)

1. Тема роботи: Оцінювання ефективності заходів кіберзахисту у фінансовому секторі за допомогою моделі Cyber Value-at-Risk,
керівник роботи: Гальчинський Леонід Юрійович, к.т.н, доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від « 4 » листопада 2025 р. № 4797-с

2. Термін подання здобувачем вищої освіти роботи « 12 » грудня 2025 р.

3. Вихідні дані до роботи: результати моделювання фінансових втрат із використанням стохастичних методів;

4. Зміст роботи: аналіз підходів до оцінювання кіберризиків у фінансовому секторі, дослідження економічних наслідків кібератак та концепції Cyber Value-at-Risk, розробка алгоритмічної основи моделювання фінансових втрат із використанням імовірнісних методів, оцінювання показників VaR та CyVaR, а також аналіз впливу заходів кіберзахисту на рівень сукупного ризику з метою кількісної оцінки ефективності прийнятих рішень зхахисту.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): презентація.

6. Дата видачі завдання : « 22 » вересня 2025 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Формулювання тематики та визначення напряму дослідження магістерської роботи	01.09.2025 – 21.09.2025	Виконано
2	Опрацювання наукових публікацій, міжнародних стандартів та методичних матеріалів з оцінювання кіберризиків і CyVaR	08.09.2025 – 29.09.2025	Виконано
3	Погодження теми та завдання на магістерську дисертацію	22.09.2025	Виконано
4	Аналіз кіберзагроз фінансового сектору та формування сценаріїв кіберінцидентів для моделювання фінансових втрат	23.09.2025 – 06.10.2025	Виконано
5	Дослідження методів кількісної оцінки фінансових втрат від кіберінцидентів та вибір моделі Cyber Value-at-Risk	29.09.2025 – 06.10.2025	Виконано
6	Розробка алгоритмічної основи моделювання фінансових втрат із використанням імовірнісних методів	06.10.2025 – 20.10.2025	Виконано
7	Моделювання розподілів фінансових втрат та розрахунок показника CyVaR	20.10.2025 – 30.11.2025	Виконано
8	Аналіз хвостових ризиків та дослідження впливу екстремальних збитків на сукупний ризик	20.11.2025 – 24.11.2025	Виконано
9	Оцінювання впливу заходів кіберзахисту на рівень фінансових втрат та порівняльний аналіз ризику до і після впровадження контролів	24.11.2025 – 08.12.2025	Виконано
10	Передзахист магістерської дисертації	16.12.2025	
11	Захист магістерської дисертації	23.12.2025	

Здобувач вищої освіти _____ Заріцький Олександр
(підпис) (**Власне ім'я, ПРІЗВИЩЕ**)

Керівник роботи _____ Леонід Гальчинський
(підпис) (**Власне ім'я, ПРІЗВИЩЕ**)

РЕФЕРАТ

Обсяг дипломної роботи **«89»** сторінок, **«14»** ілюстрацій, **«1»** додаток та **«41»** джерело літератури. У роботі проаналізовано сучасні підходи до оцінювання кіберризиків у банківському секторі України та досліджено можливості кількісної оцінки ризику за допомогою моделі Cyber Value-at-Risk (CyVaR). Розглянуто теоретичні засади моделювання кіберризиків, побудову розподілів частоти та тяжкості інцидентів, а також застосування симуляцій Монте-Карло для прогнозування можливих фінансових втрат.

Об’єкт дослідження: управління кіберризиками банківських установ.

Предмет дослідження: методика CyVaR для оцінювання кіберризику.

Мета дослідження: застосування CyVaR для визначення потенційних збитків та ефективності заходів кіберзахисту.

Методи дослідження: аналіз джерел, математичне моделювання, симуляційні обчислення.

Результати роботи можуть бути використані для оцінки кіберризиків та планування заходів кіберзахисту в організаціях банківського секору України.

Ключові слова: кіберризик, CyVaR, банківський сектор, моделювання Монте-Карло.

ABSTRACT

The master's thesis consists of “89” pages, includes “14” illustrations, “1” appendice and “41” references. The study analyzes modern approaches to assessing cyber risks in the banking sector of Ukraine and examines the applicability of the Cyber Value-at-Risk (CyVaR) model as a quantitative method for estimating potential financial losses from cyber incidents. The thesis explores the theoretical foundations of cyber risk modelling, the construction of frequency and severity distributions, and the use of Monte Carlo simulations for forecasting annual loss distributions.

Object of research: cyber risk management in banking institutions.

Subject of research: the CyVaR methodology for cyber risk assessment.

Purpose of the study: to apply the CyVaR model to estimate potential cyber losses and evaluate the effectiveness of cybersecurity measures.

Research methods: analysis of literature, mathematical modelling, simulation-based computation.

The results can be used for cyber risk assessment and cybersecurity planning within organizations of the Ukrainian banking sector.

Keywords: cyber risk, CyVaR, banking sector, Monte Carlo simulation.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

VaR – Value at Risk, показник фінансового ризику, що визначає потенційні збитки за певний період;

CyVaR – Cyber Value at Risk, показник кіберризику, що характеризує максимальний можливий збиток при заданому рівні довіри;

Кіберризик – імовірність фінансових та операційних втрат, спричинених кіберінцидентами;

Кіберінцидент – порушення конфіденційності, цілісності або доступності інформаційних систем;

MCMC – Markov Chain Monte Carlo, метод марковських ланцюгів Монте-Карло для оцінювання параметрів моделей;

APT – Advanced Persistent Threat, високорівнева цілеспрямована кібератака;

CERT-UA – команда реагування на комп’ютерні надзвичайні події України;

DDoS – Distributed Denial of Service, розподілена атака на відмову в обслуговуванні;

Фішинг – метод соціальної інженерії для отримання конфіденційної інформації;

ВСТУП

Стрімка цифровізація фінансових послуг та глибока інтеграція інформаційних технологій в операційну діяльність банківських установ призвели до суттєвого зростання залежності банківського сектору України від стійкості та надійності інформаційних систем. Водночас кількість та складність кіберінцидентів невпинно збільшуються, що створює загрозу не лише для окремих фінансових організацій, а й для стабільності національної фінансової системи загалом. За умов воєнного стану та підвищеної активності ворожих кіберугруповань проблема оцінювання та управління кіберризиками набуває особливої актуальності, оскільки атаки на банківські сервіси, платіжну інфраструктуру чи фінансові дані можуть мати критичні наслідки для економічної безпеки держави [1][2].

Класичні методики управління ризиками, що застосовуються у фінансовій сфері, виявляються недостатньо ефективними для оцінювання кіберризиків через їх непередбачуваний, стохастичний та важкохвостий характер. Тому актуальною стає потреба у використанні кількісних моделей, здатних відображати реальний вплив кіберінцидентів і прогнозувати можливі фінансові втрати. Однією з найбільш перспективних методик є модель Cyber Value-at-Risk (CyVaR), яка дозволяє оцінити потенційні збитки з певним рівнем довіри та використовується у провідних міжнародних фінансових інститутах для аналізу ризикового профілю організацій [3],[4],[5].

Метою даної магістерської роботи є застосування методу CyVaR для оцінки кіберризиків банківського сектору України, зокрема моделювання потенційних втрат на наступний рік за допомогою симуляцій Монте-Карло. Для досягнення мети досліджено теоретичні засади кількісного оцінювання ризику, проаналізовано сучасні стандарти та методики управління кіберризиками, а також розроблено експериментальну модель прогнозування на основі статистичних розподілів частоти і тяжкості кіберінцидентів.

Результати роботи можуть бути використані банківськими установами для формування системи управління кіберризиками, планування бюджету

кіберзахисту, визначення пріоритетів впровадження контролів та підвищення стійкості фінансової інфраструктури України.

1 ТЕОРЕТИЧНІ ЗАСАДИ КІБЕРРИЗИКІВ У ФІНАНСОВОМУ СЕКТОРІ

1.1 Еволюція економічного розуміння ризику та формування поняття кіберризику

У класичній економічній думці ризик розглядається як природна характеристика будь-якої діяльності людини, а особливо — діяльності, пов’язаної з грошовими потоками та комерційними відносинами. Ще у працях Френка Найта [6] було запропоновано фундаментальне розмежування між ризиком та невизначеністю. Під ризиком він розумів події, імовірність настання яких може бути визначена на основі статистичних даних, тоді як невизначеність він трактував як події, імовірність яких принципово не може бути оцінена, оскільки вони або не мають історичної бази, або є унікальними за своєю природою. Це розмежування стало одним із підґрунтів сучасного кількісного аналізу ризиків.

У фінансовому секторі ризик почали формально описувати значно раніше, ніж у багатьох інших галузях, що пояснюється потребою вимірювати волатильність фінансових активів, аналізувати кредитні дефолти, прогнозувати ліквідність та оцінювати надійність фінансових інструментів. У результаті склалася розвинена система класифікації фінансових ризиків: ринкові, кредитні, ліквідності, операційні. З часом саме операційний ризик став тією категорією, яка поглинула у себе велику кількість некласичних загроз, пов’язаних із внутрішніми процесами, технологічними збоями та людськими помилками [7].

У міру розвитку цифрових технологій почала з’являтися нова сфера загроз, які не могли бути адекватно описані традиційними інструментами операційного ризику. На початку 2000-х років регулятори, зокрема Базельський комітет, почали використовувати термін «кіберризик» для опису тих ситуацій, коли негативні події виникали внаслідок атак на інформаційні системи, витоків даних чи несанкціонованих змін у технологічних процесах. Потім стало зрозуміло, що кіберризик не є простою підмножиною операційного ризику, а

має настільки специфічні властивості, що потребує окремих моделей, методів вимірювання та регуляторного підходу.

У відмінності від інших ризиків кіберризик має спрямовану природу: він породжується не випадковим збоєм або помилкою, а часто цілеспрямованими діями зловмисника, який адаптується, змінює тактику, підбирає оптимальний момент атаки і здатний використовувати творчий підхід. Тобто кіберризик є не просто стохастичним процесом, а результатом взаємодії з активним противником. З цієї причини методологічний апарат класичного аналізу ризиків часто стає недостатнім.

Також унікальною особливістю кіберризику є його нелінійний характер. Більшість інцидентів мають малий або середній масштаб, але дуже обмежена частка — катастрофічний рівень втрат. Це створює важкохвостий розподіл збитків, який не підпорядковується нормальному розподілу та принципово ускладнює прогнозування. Водночас кіберризики надзвичайно динамічні: нові уразливості з’являються постійно, так само як і нові техніки атак, тоді як традиційні фінансові ризики розвиваються більш прогнозовано.

Саме внаслідок накопичення цих специфічних характеристик кіберризик був виділений у самостійну категорію. Сьогодні він розглядається як окремий клас економічного ризику, тісно пов’язаний із інформаційною безпекою, поведінковими аспектами персоналу, технічними характеристиками IT-систем і регуляторними вимогами.

1.2 Сучасний зміст поняття кіберризику та його властивості

На сьогодні кіберризик визначають як імовірність фінансових, операційних або репутаційних втрат, що виникають у результаті порушення конфіденційності, цілісності або доступності інформаційних систем і даних. Це визначення охоплює декілька ключових елементів: наявність загрози, яка може бути як зовнішньою (APT-групи, кіберзлочинні синдикати, шахраї), так і внутрішньою (недоброчесні співробітники); наявність вразливості, яка робить

актив доступним для атаки; сам актив, що має певну цінність; потенційні наслідки інциденту.

Кіберризик — це стохастична величина, параметри якої постійно змінюються. Це означає, що математичні моделі, застосовувані для його оцінки, повинні враховувати обмеженість історичної інформації, потенційну неповноту даних, швидкість еволюції загроз та складність залежностей між різними чинниками. Класичні методи оцінки ризику, які припускають стаціонарність процесів, нормальність розподілів та стабільність параметрів, не підходять для кіберризиків.

З цієї причини в аналітичних системах кіберризику активно використовують розподіли із важкими хвостами (heavy-tailed distributions), такі як логнормальний, гамма-розподіл, розподіл Парето та загальний розподіл Парето [8]. Саме вони дають змогу описати рідкісні, але руйнівні події, що формують основну частку фінансових збитків [9][10].

У статті «Оцінювання ймовірності фінансових втрат фінансової установи внаслідок кіберінцидентів на основі кількісних методів аналізу ризику» [11] також підкреслено важкохвостий характер розподілу збитків та продемонстровано, що навіть обмежена кількість серйозних кіберінцидентів формує значну частку сумарних втрат, що має бути враховано при побудові моделей CyVaR.

Більш того, кіберризик відрізняється від традиційних ризиків тим, що кількість інцидентів та їх тяжкість залежать від дій противника. Тобто ці процеси не є незалежними або випадковими — вони є адаптивними. Це створює додаткову складність у вимірюванні, адже на відміну від коливань ринку або кредитних дефолтів, кіберзагрози не підпорядковуються природним економічним законам, а є результатом інтелектуальної діяльності людей.

Таким чином, сучасне поняття кіберризику охоплює складну взаємодію між технологічними, людськими, процесними та зовнішніми факторами, що формує надзвичайно складний і динамічний клас ризиків.

1.3 Кіберризик у контексті діяльності фінансових установ

Фінансовий сектор України та світу є однією з найбільш привабливих цілей для кіберзлочинців [12]. Це пояснюється декількома фундаментальними факторами, такими як концентрація фінансових ресурсів, наявність великих масивів конфіденційних даних, висока цифровізація процесів та критична роль фінансових установ для економічної стабільності країни. У банках відбувається постійна взаємодія з платіжними системами, міжбанківськими мережами, мобільними додатками, API та хмарними провайдерами, що значно збільшує площину атаки.

У разі атаки на банк збитки можуть мати багатоаспектний характер. Вони включають прямі фінансові втрати, пов'язані з шахрайськими транзакціями, крадіжкою коштів або вимаганням. Додатково виникають операційні втрати через простій критичних сервісів, непрямі втрати через необхідність відновлення систем та проведення цифрової форензики, а також значні репутаційні збитки. Особливо небезпечною є ситуація, коли атаки мають системний характер, тобто спрямовані не на одну установу, а на цілу фінансову екосистему [13].

У згаданій статті автора окреслено ключові закономірності формування втрат у банківському секторі та показано, що навіть одиничні інциденти великого масштабу мають відповідальний вплив на розподіл втрат. Це значною мірою обґрунтовує необхідність використання моделі Cyber Value-at-Risk, яка дозволяє вимірювати не лише середній рівень збитків, але і поведінку розподілу у його верхній частині (95-й чи 99-й квантилі).

У сучасних умовах, особливо у період повномасштабної агресії проти України, кіберризик для фінансового сектора набуває ще більшого значення. CSIRT-NBU [14] та інші аналітичні установи зафіксували істотне зростання кількості атак на фінансові установи, зокрема шкідливих програм руйнівного типу, цілеспрямованих фішингових кампаній та складних багатоступеневих атак APT-груп. Це створило принципово новий рівень ризиковості, що вимагає переосмислення традиційних підходів до оцінки ризику.

1.4 Фактори, які формують кіберризик: технологічні, людські, процесні та зовнішні

Кіберризик у фінансовому секторі формується під впливом взаємопов'язаних компонентів, що відображають вразливості інформаційних систем, цінність захищуваних активів та характеристики потенційного противника. Такий підхід відповідає сучасним кількісним моделям оцінювання ризику, зокрема підходам, описаним у роботах А. Орландо [8], де кіберризик розглядається не як статичний показник, а як результат динамічної взаємодії між активами, загрозами та рівнем захищеності організації.

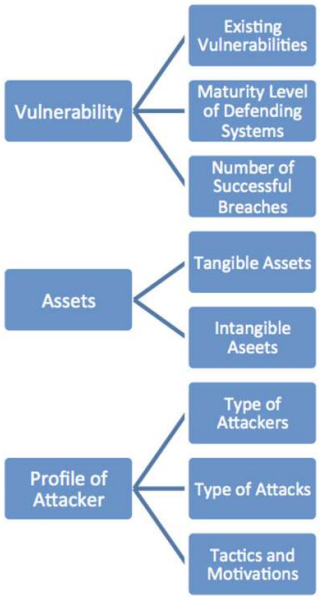

Рисунок 1.1 - Сектори та відсоток атак, що на них припадають [8]

Ключовим елементом цієї взаємодії є вразливість, яка визначається наявністю технічних, організаційних і процесних слабких місць. До таких факторів належать існуючі вразливості програмного забезпечення, рівень зрілості систем кіберзахисту, ефективність процесів управління вразливостями та історія успішних компрометацій. Використання застарілих технологічних рішень, складні інтеграції з третіми сторонами та недостатній рівень контролю доступу суттєво підвищують імовірність успішної реалізації кібератаки. У кількісних моделях ризику ці характеристики безпосередньо впливають на частоту інцидентів, визначаючи параметри стохастичних моделей [15].

Другим фундаментальним компонентом є активи фінансової установи, які можуть мати як матеріальний, так і нематеріальний характер. До них належать фінансові ресурси, платіжна інфраструктура, інформаційні системи, персональні дані клієнтів, а також репутаційний капітал організації. Саме вартість та критичність активів визначають потенційну тяжкість фінансових втрат у разі кіберінциденту. У моделі CyVaR активи формують основу розподілу збитків, оскільки масштаби втрат прямо залежать від того, які саме ресурси були скомпрометовані та якими є наслідки їх порушення для операційної діяльності установи.

Третім елементом структури кіберризику є профіль зловмисника, який охоплює тип атакуючої сторони, використовувані вектори атак, тактики та мотивацію. На відміну від багатьох традиційних фінансових ризиків, кіберризик має спрямований характер, оскільки зловмисник здатний адаптувати свою поведінку до рівня захисту організації та цінності її активів. У фінансовому секторі це особливо проявляється у діяльності організованих кіберзлочинних угруповань і APT-груп, які застосовують складні багатоступеневі атаки, комбінуючи технічні методи з соціальною інженерією.

Таким чином, кіберризик у фінансовому секторі слід розглядати як результат одночасного впливу вразливостей, активів та профілю противника. Саме ця взаємодія визначає як імовірність виникнення кіберінцидентів, так і масштаби потенційних фінансових втрат. Такий структурований підхід створює методологічну основу для подальшого кількісного моделювання кіберризику та застосування моделі Cyber Value-at-Risk, у межах якої зазначені компоненти трансформуються у параметри стохастичних моделей частоти та тяжкості збитків.

1.5 Економічна природа втрат від кіберінцидентів

Втрати, які виникають у результаті кіберінцидентів, мають багатовимірну економічну природу та не обмежуються лише прямими фінансовими збитками. У загальному випадку вони включають одноразові прямі втрати, пов’язані з крадіжкою коштів, несанкціонованими фінансовими операціями або вимаганням, а також витрати на технічне відновлення інформаційних систем, оплату послуг кіберфорензики, реагування на інциденти та відновлення бізнес-процесів. Додатково фінансові установи несуть юридичні витрати, пов’язані з розслідуванням інцидентів, судовими позовами та виконанням регуляторних вимог, а також штрафи та санкції з боку наглядових органів.

Окрему категорію становлять непрямі економічні втрати, які часто мають довгостроковий характер. До них належать втрати від простою критичних сервісів, зниження продуктивності персоналу, порушення операційної діяльності, а також репутаційні збитки, що можуть призводити до відтоку клієнтів, зниження довіри до фінансової установи та зменшення її ринкової вартості. У багатьох випадках саме непрямі та репутаційні втрати формують найбільшу частку сумарного економічного ефекту від кіберінциденту, хоча їх кількісна оцінка є складнішою.

Ключовою особливістю кіберзбитків є їх стохастичний характер. Неможливо точно передбачити момент настання інциденту, тип активу, який буде скомпрометовано, або масштаб фінансових наслідків. Крім того, розподіл втрат має виражений важкохвостий характер: більшість інцидентів призводить до відносно незначних збитків, однак невелика кількість подій може спричинити катастрофічні фінансові наслідки. Саме ця властивість принципово ускладнює використання класичних детермінованих підходів до оцінювання ризику та обґрунтовує необхідність застосування кількісних методів, що базуються на моделюванні можливих сценаріїв втрат.

1.6 Роль систем кіберзахисту у формуванні розподілу кіберризику

З позиції кількісного аналізу заходи кіберзахисту відіграють ключову роль у формуванні розподілу кіберризику та безпосередньо впливають на його основні параметри. Насамперед вони впливають на частоту успішних кіберінцидентів, зменшуючи ймовірність їх реалізації. У стохастичних моделях це відображається у зниженні параметра λ, який характеризує середню кількість інцидентів за певний період часу. Ефективні системи виявлення загроз, управління вразливостями, моніторингу подій безпеки та реагування на інциденти здатні істотно скоротити кількість успішних атак.

Другим важливим механізмом впливу заходів кіберзахисту є зменшення тяжкості фінансових втрат. Навіть у випадку успішної атаки наявність резервних копій, сегментації мережі, швидких процедур реагування та планів безперервності бізнесу дозволяє обмежити масштаб збитків та скоротити час простою систем. У кількісних моделях це проявляється у зміні параметрів розподілу тяжкості збитків та зменшенні ймовірності виникнення екстремальних значень.

У роботах, присвячених кількісному аналізу кіберризиків, зокрема у дослідженнях А. Орландо [8] та Л.Гальчинського і О. Урсола [16] , показано, що впровадження ефективних заходів кіберзахисту має найбільший вплив саме на верхній хвіст розподілу збитків. Це означає, що системи захисту не лише знижують середній рівень втрат, а й суттєво зменшують значення показника Cyber Value-at-Risk. Таким чином, оцінювання ефективності контролів повинно здійснюватися не лише з точки зору зниження ймовірності інцидентів, а й з позиції їх впливу на форму розподілу кіберризику в цілому.

1.7 Кіберризик як об’єкт математичного моделювання

Кіберризик за своєю природою є випадковою величиною, яка формується внаслідок складної взаємодії множини стохастичних процесів. Його адекватний опис неможливий у межах простих детермінованих або середніх оцінок, оскільки такі підходи не враховують ані мінливість параметрів, ані ймовірність екстремальних подій. Саме тому моделювання кіберризику

потребує застосування сучасного математичного апарату, що включає байєсовий підхід, методи Монте-Карло та методи марковських ланцюгів Монте-Карло (MCMC) [17].

У кількісних моделях кіберризику загальні фінансові втрати розглядаються як результат поєднання двох випадкових компонентів: частоти кіберінцидентів та тяжкості збитків від кожного інциденту. Такий підхід дозволяє формалізувати ризик у вигляді стохастичного процесу та побудувати емпіричний розподіл можливих втрат. Методи Монте-Карло використовуються для генерації великої кількості сценаріїв розвитку подій, що дає змогу відтворити поведінку розподілу навіть у його верхніх квантилях.

Водночас обмеженість та неповнота історичних даних про кіберінциденти зумовлює необхідність застосування методів MCMC для оцінювання параметрів моделей. Байєсовий підхід дозволяє врахувати невизначеність параметрів, сформувати апостеріорні розподіли та отримати більш стійкі оцінки ризику. Саме поєднання методів Монте-Карло та MCMC створює надійну математичну основу для побудови моделі Cyber Value-at-Risk, яка здатна забезпечити точне та обґрунтоване оцінювання фінансових втрат навіть за умов високої невизначеності та динамічного характеру кіберзагроз.

Висновки до розділу 1

У розділі сформовано теоретичну основу дослідження кіберризиків у фінансовому секторі та показано еволюцію підходів до розуміння ризику — від класичних економічних концепцій до виокремлення кіберризику як самостійної категорії. Обґрунтовано, що кіберризик має спрямований, динамічний і нелінійний характер, а розподіл втрат є важкохвостим, що унеможливлює застосування традиційних статистичних методів оцінювання.

Показано специфіку прояву кіберризиків у діяльності фінансових установ, зокрема їх системний вплив, багатовимірну економічну природу втрат та підвищену актуальність в умовах зростання кіберзагроз для України. Систематизовано ключові фактори формування кіберризику та доведено роль систем кіберзахисту у зміні частоти інцидентів і масштабу фінансових втрат.

Отримані теоретичні положення обґрунтовують доцільність застосування кількісного моделювання та використання моделі Cyber Value-at-Risk як інструменту оцінювання екстремальних кіберзбитків у фінансовому секторі.

2 ТЕОРЕТИЧНІ ПІДХОДИ ДО ОЦІНЮВАННЯ КІБЕРРИЗИКІВ У ФІНАНСОВОМУ СЕКТОРІ

2.1 Економічна логіка та історичний розвиток моделей оцінювання ризиків

У науковій та практичній площині питання оцінювання ризику завжди займало особливе місце. Протягом XX століття фінансова індустрія розробила широкий спектр інструментів для кількісного вимірювання ризиків, що дозволило формалізувати такі явища, як волатильність активів, ймовірність дефолту, коливання відсоткових ставок та інші процеси, притаманні фінансовим ринкам. Саме фінансова математика та економетрика стали першими дисциплінами, у яких ризик почали розглядати не як суто якісну характеристику, а як чітко визначену кількісну величину.

Поступово виникла потреба не лише в класифікації ризику, а й у створенні моделей, які могли б описати економічні параметри випадкових процесів. Базельські угоди, починаючи з Basel I, а потім Basel II та Basel III, стали ключовими етапами у розвитку кількісних методів оцінювання ризику, оскільки вони встановили загальнообов'язкові вимоги щодо капіталу, що має покривати можливі ризики. На ранніх етапах оцінювання операційного ризику вважалося другорядною задачею порівняно з оцінюванням ринкового та кредитного ризиків. Однак із часом стало зрозуміло, що збитки від операційних подій — збоїв, шахрайства, помилок у процесах — можуть мати не менш руйнівні наслідки, ніж ринкові коливання [18][19].

Зі зростанням рівня цифровізації фінансових процесів, появою електронного банкінгу, мобільних додатків, API-екосистем та високою залежністю фінансової інфраструктури від цифрових технологій виникла принципово нова категорія загроз — кіберзагрози, що, відповідно, вимагали нових підходів до оцінювання ризику. Уже на початку 2010-х років наукова спільнота почала визнавати, що кіберризик не описується у межах класичних моделей операційного ризику, а має власну структуру закономірностей, властивостей та характеристик.

Таким чином, розвиток теорії кіберризику можна розглядати як логічне продовження еволюції фінансових моделей ризику, але з урахуванням нових параметрів, які раніше не існували в економічній науці: активного противника, навмисної деструктивної поведінки, високої швидкості зміни загроз та порушення класичних статистичних припущень щодо розподілів.

2.2 Якісні моделі оцінювання кіберризиків у традиційній практиці

Першим етапом у розвитку підходів до оцінювання кіберризику стали якісні моделі, що базуються на експертних судженнях. У межах таких моделей ризик класифікується за категоріями (низький, середній, високий) на основі суб'єктивної оцінки ймовірності та впливу інцидентів. Подібні підходи широко застосовуються в організаціях на початкових етапах формування системи управління інформаційною безпекою [20].

Основною перевагою якісних моделей є їх простота та швидкість впровадження. Вони не потребують наявності великих масивів історичних даних і дозволяють швидко отримати загальне уявлення про рівень ризику. Проте з економічної точки зору такі моделі мають суттєві обмеження. Вони не дозволяють виміряти ризик у грошовому еквіваленті, не забезпечують можливості порівняння альтернативних заходів захисту за економічною ефективністю та не підтримують прийняття інвестиційних рішень.

Крім того, якісні моделі не враховують стохастичний характер кіберінцидентів і не відображають можливість виникнення рідкісних, але катастрофічних подій. В умовах швидкої еволюції кіберзагроз та високої динаміки атак рішення, що ґрунтуються виключно на експертних оцінках, стають дедалі менш надійними.

2.3 Напівкількісні моделі: перехідний етап між експертною оцінкою та економічним моделюванням

Напівкількісні моделі стали проміжним етапом між якісними підходами та повноцінним кількісним моделюванням. У таких моделях експертні оцінки

трансформуються у числові шкали, наприклад від 1 до 5, а ризик визначається за допомогою матриць ризиків або карт ризику.

Ці моделі дозволили частково формалізувати процес оцінювання та зробили його більш структурованим. Вперше у практиці управління кіберризиками почали використовуватися поняття частоти подій та їх потенційного впливу, хоча й у спрощеному вигляді. Напівкількісні моделі стали важливим методологічним кроком, оскільки підготували ґрунт для переходу до економічно обґрунтованих кількісних підходів.

Разом з тим, напівкількісні моделі залишаються значною мірою суб'єктивними та не дозволяють прогнозувати реальні фінансові втрати. Вони не відображають розподіл збитків і не дають можливості аналізувати поведінку ризику у верхніх квантилях, що є критично важливим для фінансових установ [21].

2.4 Кількісні моделі ризику та їх застосування у сфері кібербезпеки

Справжній прорив у сфері оцінювання кіберризику став можливим лише після початку впровадження кількісних методів, які дозволяють оцінити фінансовий вплив інцидентів у грошовому вимірі. На відміну від якісних і напівкількісних моделей, кількісні моделі базуються на статистичній оцінці розподілів частоти та тяжкості інцидентів, що дозволяє формувати математичні моделі збитків.

Основною ідеєю кількісної оцінки кіберризику є представлення загальних збитків як результату добутку частоти інцидентів та тяжкості кожного інциденту. Частота інцидентів зазвичай моделюється як випадковий процес (часто пуассонівський), тоді як тяжкість може моделюватися через логнормальний, гамма-розподіл або важкохвості розподіли, такі як розподіл Парето.

Ці моделі дозволяють отримати апроксимацію реального розподілу кіберзбитків і, відповідно, використовувати підхід Value-at-Risk (VaR) для оцінювання найгірших сценаріїв. Саме ця логіка стала основою для створення

моделі Cyber Value-at-Risk, що дозволяє фінансовим установам оцінити потенційно найбільший можливий збиток з імовірністю 95% або 99%.

2.5 Модель FAIR як перша повноцінна формалізація кіберризику

Однією з перших моделей, яка намагалася кількісно описати структуру кіберризику, стала модель FAIR (Factor Analysis of Information Risk) [22]. Вона запропонувала розглядати ризик як функцію очікуваної кількості загрозових подій та очікуваної величини збитку, створивши структуру для подання ризику у числовій формі. Модель FAIR стала революційною у сфері інформаційної безпеки, оскільки вона запропонувала формальний підхід до вимірювання ризику, що раніше вважалося складним або навіть неможливим.

Проте FAIR мала певні обмеження: вона значною мірою покладалася на експертні оцінки, не враховувала важкохвості розподілу збитків, не містила механізмів оцінювання невизначеності параметрів та не дозволяла повноцінно моделювати поведінку противника. Водночас вона створила концептуальну основу для розвитку складніших моделей, таких як CyVaR.

2.6 Необхідність переходу до складніших математичних моделей

У міру накопичення статистичних даних про кіберінциденти науковці почали усвідомлювати, що класичні методи оцінювання ризику є недостатніми для опису кіберзагроз. Це пояснюється декількома чинниками: частота інцидентів змінюється у часі та залежить від поведінки зловмисників, тяжкість збитків має важкохвостий характер, а самі інциденти можуть бути залежними один від одного. Крім того, кількість даних про серйозні інциденти зазвичай є дуже малою, а отже, класичні статистичні методи оцінювання параметрів розподілів працюють погано.

У таких умовах дослідники почали використовувати методи Монте-Карло та методи марковських ланцюгів Монте-Карло (MCMC) для моделювання стахастичних процесів та оцінювання параметрів розподілів. Передусім це стосується моделі CyVaR, яка потребує точного моделювання розподілу збитків і визначення верхніх квантилів цього розподілу [23].

Висновки до розділу 2

У другому розділі систематизовано теоретичні підходи до оцінювання кіберризиків у фінансовому секторі та простежено еволюцію моделей ризику — від класичних фінансово-економічних концепцій до сучасних кількісних підходів у сфері кібербезпеки. Показано, що розвиток методів оцінювання ризиків у фінансовій індустрії створив методологічне підґрунтя для формалізації кіберризику, однак традиційні моделі операційного ризику виявилися недостатніми для опису специфіки кіберзагроз.

Проаналізовано якісні та кількісні моделі оцінювання кіберризиків, визначено їх роль у практиці управління ризиками та окреслено ключові обмеження. Зокрема, такі підходи не дозволяють здійснювати економічно обґрунтовану оцінку втрат, порівнювати ефективність заходів захисту та враховувати імовірність екстремальних подій, що є критично важливим для фінансових установ.

Окрему увагу приділено кількісним моделям ризику, які ґрунтуються на стохастичному моделюванні частоти та тяжкості інцидентів. Показано, що саме ці моделі забезпечують можливість оцінювання кіберризику у грошовому вимірі та створюють основу для застосування підходу Value-at-Risk у сфері кібербезпеки. Розглянуто модель FAIR як першу спробу формалізації кіберризику та визначено її значення для подальшого розвитку більш складних моделей. Обґрунтовано необхідність переходу до розширених математичних методів, зокрема Монте-Карло та MCMC, з огляду на динамічний, адаптивний і важкохвостий характер кіберзбитків. Зроблено висновок, що саме такі підходи є методологічною основою для побудови моделі Cyber Value-at-Risk, математичні аспекти якої розглядаються у наступних розділах роботи.

3 ТЕОРЕТИЧНІ ОСНОВИ МОДЕЛІ CYBER VALUE-AT-RISK (CyVaR)

3.1 Історичні передумови виникнення моделі VaR та її роль у фінансовій математиці

Формування сучасних підходів до кількісної оцінки ризиків нерозривно пов’язане з розвитком фінансової інженерії кінця XX століття. У 1990-х роках банківський сектор переживав масштабні трансформації, пов’язані з глобалізацією фінансових ринків, зростанням обсягів міжнародних операцій, розвитком похідних інструментів та збільшенням волатильності активів. У цих умовах постала потреба у створенні універсального інструменту, який дозволяв би оцінювати можливі втрати фінансового портфеля в умовах невизначеності.

Саме на цьому ґрунті у 1994 році компанія J.P. Morgan розробила концепцію Value-at-Risk (VaR) [24], яка згодом стала стандартом для вимірювання ризиків у фінансових установах по всьому світу. Основною ідеєю VaR було визначити величину можливих збитків, які з певною імовірністю не будуть перевищені протягом заданого періоду. Це дозволяло перейти від абстрактних міркувань про ризик до конкретної числової величини, що могла бути використана в управлінні капіталом та оцінюванні нормативів достатності капіталу відповідно до вимог Базельського комітету.

Модель VaR базувалася на припущенні про наявність історичних даних, які можуть бути використані для оцінювання майбутньої волатильності, та на припущенні про стаціонарність процесів, які визначають коливання ринкових активів. Вона довела свою ефективність у багатьох випадках, і протягом десятиліть VaR залишався базовим інструментом для аналізу ринкового ризику, кредитного ризику та навіть деяких елементів операційного ризику.

Однак з поширенням цифрових технологій і появою нових типів загроз стало зрозуміло, що модель VaR не може бути безпосередньо застосована для оцінки кіберризиків. Передусім це пов’язано з тим, що природа кіберзбитків радикально відрізняється від природи ринкових втрат. Якщо ринкові втрати формуються внаслідок змін у цінах активів, то кіберзбитки виникають у

результаті подій, які можуть бути рідкісними, але катастрофічними. Це означає, що розподіл кіберзбитків не є подібним до нормального або близького до нормального розподілу, який широко застосовується у фінансових моделях[25][26][27].

Таким чином, модель VaR стала лише відправною точкою для формування спеціалізованої моделі Cyber Value-at-Risk, яка враховує специфічні властивості кіберінцидентів: непередбачуваність, важкохвостий характер збитків, активність противника та відсутність стабільних історичних даних.

3.2 Логіка переходу від традиційного VaR до CyVaR

Хоча концепція VaR має високу аналітичну цінність, її пряма адаптація до кіберсфери є неможливою через фундаментальні відмінності між природою фінансових та кіберзбитків. У класичному підході VaR аналізує безперервні коливання вартості активів, тоді як у кіберризику збитки є дискретними та стохастичними, формуються окремими подіями та можуть мати значний розкид значень.

Додатковою проблемою є обмеженість даних. Якщо у фінансових ринків є десятиліття високочастотних даних, то у сфері кібербезпеки реальні історичні вибірки часто складаються з невеликої кількості інцидентів за рік, причому значна частина інцидентів не відображає всю можливу шкоду через обмеження розкриття інформації. Це означає, що параметри розподілу збитків у кіберризику не можуть бути надійно оцінені класичними методами.

Кіберінциденти мають також властивість кластеризації. Наприклад, у періоди підвищеної геополітичної напруги кількість атак на фінансовий сектор може різко зростати. Це порушує припущення про незалежність і рівномірність розподілу інцидентів у часі.

Усі ці властивості привели до усвідомлення необхідності розробити модель, яка б відображала реальну структуру кіберризику. Cyber Value-at-Risk, на відміну від класичного VaR, не ґрунтується на безперервному часовому ряді цін, а на стохастичному моделюванні частоти інцидентів та величини збитку

від кожного інциденту. Це означає, що CyVaR був спеціально створений як інструмент, здатний відтворити стохастичну природу кіберзбитків та оцінити найбільш негативні сценарії розвитку подій.

Таким чином, CyVaR є не просто адаптацією VaR, а фактично новою моделлю, що інтегрує підходи з теорії ризиків, статистичного моделювання, економіки кібербезпеки та теорії ймовірностей. Він дозволяє визначити очікувані фінансові втрати за умов підвищеної невизначеності та складності кіберзагроз.

3.3 Математичні основи моделі Cyber Value-at-Risk

У моделі Cyber Value-at-Risk (CyVaR) фінансові втрати організації розглядаються як результат реалізації випадкового процесу, що поєднує дві фундаментальні складові кіберризику: частоту виникнення кіберінцидентів та тяжкість фінансових наслідків кожного інциденту. Такий підхід безпосередньо походить з актуарної теорії операційного ризику та відомий як Loss Distribution Approach (LDA), який широко використовується у фінансовому секторі для оцінювання регуляторного капіталу [28].

З математичної точки зору загальний збиток фінансової установи за фіксований часовий період (наприклад, рік) моделюється як випадкова сума випадкової кількості випадкових величин. Це дозволяє адекватно врахувати як невизначеність кількості інцидентів, так і невизначеність масштабу кожного окремого збитку. Таким чином, загальний збиток можна подати як суму випадкових величин:

$$L = \sum_{j=0}^{N} X_j, \;\; N = 0,1,2, \ldots \qquad (3.1)$$

, де N — випадкова кількість інцидентів за період; X_i — випадкова величина, що описує фінансовий збиток від i-го інциденту; L — сукупний фінансовий збиток організації.

Цей вираз формалізує ідею, що загальні втрати виникають не від одного “середнього” інциденту, а як результат сукупності подій, кожна з яких може мати принципово різний фінансовий ефект. Саме така структура дозволяє

моделювати рідкісні, але катастрофічні події, які визначають верхній хвіст розподілу ризику.

3.3.1 Моделювання частоти кіберінцидентів

Кіберінциденти належать до класу рідкісних подій, які відбуваються випадково у часі. У більшості досліджень, зокрема в роботах А. Орландо [8], частота інцидентів моделюється як пуассонівський процес, що добре описує кількість незалежних подій за фіксований період часу. У випадках, коли спостерігається надмірна дисперсія або кластеризація атак, може застосовуватися негативний біноміальний розподіл.

$$N \sim Poisson(\lambda) \tag{3.2}$$

, де λ — середня кількість кіберінцидентів за період.

Параметр λ має чітку інтерпретацію з точки зору кіберзахисту: він безпосередньо відображає ефективність контролів, рівень зрілості SOC, моніторингу та реагування. Саме на цей параметр перш за все впливають превентивні заходи безпеки.

3.3.2 Моделювання тяжкості фінансових втрат

На відміну від частоти, тяжкість збитків характеризується асиметричним розподілом із важким правим хвостом. Емпіричні дослідження кіберінцидентів свідчать, що більшість подій мають низьку вартість (операційний шум), тоді як невелика кількість інцидентів призводить до надзвичайно великих втрат [29]. Це повністю узгоджується з результатами статті «Оцінювання ймовірності фінансових втрат фінансової установи внаслідок кіберзагроз методом Монте-Карло» [11] та підходом А. Орландо [8].

$$S_i \sim Lognormal(\mu,\sigma) \tag{3.3}$$

Параметр σ безпосередньо визначає ширину хвоста розподілу та відповідає за появу екстремальних втрат, які формують основний внесок у значення CyVaR на високих рівнях довіри.

3.3.3 Агрегований розподіл втрат

Поєднання випадкової частоти та випадкової тяжкості формує складений розподіл втрат. Аналітичний вигляд такого розподілу, як правило, не має замкненої форми, що зумовлює необхідність використання симуляційних методів.

$$F_L(x) = \sum_{n=0}^{\infty} p_n F_X^{*n}(x) \quad (3.4)$$

, де $F_X^{*n}(x)$ — n-кратна згортка функції розподілу тяжкості.

Агрегований розподіл фінансових втрат формується як результат поєднання випадкової кількості кіберінцидентів та випадкової величини збитків від кожного інциденту. З математичної точки зору такий розподіл є результатом n-кратної згортки кумулятивної функції розподілу тяжкості втрат, зваженої на ймовірність настання відповідної кількості інцидентів. Загальний вигляд цього розподілу визначається сукупністю імовірностей Xj і pn = Pr(N = n) є FX(x).

Аналітичний вираз для агрегованого розподілу втрат, як правило, не має замкненої форми. Це пов’язано з тим, що згортка випадкової кількості випадкових величин призводить до складного стохастичного об’єкта, параметри якого неможливо точно оцінити класичними аналітичними методами. Саме тому в задачах оцінювання кіберризику застосовуються методи машинного та імітаційного моделювання, які дозволяють отримати емпіричну апроксимацію агрегованого розподілу та оцінити його характеристики.

У наукових публікаціях, присвячених оцінюванню кіберризиків у різних галузях, сформувався стійкий консенсус щодо того, що розподіл фінансових втрат від кіберінцидентів суттєво відрізняється від нормального. Йому притаманна асиметрія та наявність важкого правого хвоста, що зумовлює домінуючий вплив рідкісних, але масштабних інцидентів на загальний рівень ризику. Водночас у науковій спільноті

відсутній єдиний підхід до вибору конкретного аналітичного закону розподілу для агрегованих втрат.

Найчастіше в якості робочих гіпотез для опису агрегованого розподілу розглядаються складені пуассонівські, негативні біноміальні або логнормальні моделі. Проте такі припущення мають оціночний характер і використовуються передусім як наближення, що дозволяє побудувати чисельну модель ризику. Практичне застосування цих моделей передбачає емпіричну перевірку припущень та оцінювання параметрів на основі наявних даних або експертної інформації.

3.3.4 Визначення показника Cyber Value-at-Risk

На основі емпіричного або змодельованого розподілу агрегованих фінансових втрат вводиться ключова кількісна метрика оцінювання кіберризику — Cyber Value-at-Risk (CyVaR). Вона визначається як квантиль розподілу сумарних втрат на заданому рівні довіри та відображає граничний рівень фінансового збитку, який може бути понесений фінансовою установою внаслідок кіберінцидентів протягом певного періоду.

$$\mathrm{CyVaR}_{\alpha}=F_L^{-1}(\alpha) \tag{3.5}$$

де $\alpha \in \{0.95,0.99\}$ — рівень довіри, а $F_L^{-1}(\alpha)$ — відповідний квантиль розподілу агрегованих фінансових втрат.

CyVaR показує максимальний рівень збитків, який з імовірністю α не буде перевищено протягом заданого часово́го горизонту. На відміну від середніх або очікуваних значень втрат, цей показник фокусується на верхній частині розподілу, де зосереджені рідкісні, але потенційно катастрофічні події. Саме такі події визначають реальний рівень фінансової стійкості установи та створюють основний ризик для її безперервної діяльності.

Використання CyVaR є особливо важливим для фінансових установ, оскільки дозволяє пов’язати результати стохастичного моделювання кіберінцидентів із практичними управлінськими рішеннями. Зокрема, значення CyVaR може використовуватися для обґрунтування обсягів резервного

капіталу, оцінювання допустимого рівня ризику, а також для аналізу економічної доцільності інвестицій у заходи кіберзахисту.

Таким чином, модель Cyber Value-at-Risk поєднує актуарний підхід до моделювання втрат із сучасними стохастичними методами, що дозволяє кількісно описати поведінку кіберризику в умовах високої невизначеності. Застосування CyVaR забезпечує можливість оцінювання фінансової стійкості установи, планування капіталу та кількісного аналізу впливу заходів кіберзахисту на рівень сукупного ризику навіть за умов обмежених та неповних даних.

3.4 Необхідність застосування методів Монте-Карло в моделюванні CyVaR

Оскільки агрегований розподіл фінансових втрат від кіберінцидентів не має аналітичного виразу у замкненій формі, його безпосереднє використання для обчислення показників ризику є неможливим. У таких умовах природним підходом до оцінювання Cyber Value-at-Risk є застосування методів імітаційного моделювання, зокрема методу Монте-Карло, який дозволяє чисельно відтворити розподіл сукупних втрат на основі заданих імовірнісних моделей [30].

Метод Монте-Карло ґрунтується на багаторазовому випадковому відтворенні можливих сценаріїв розвитку подій відповідно до заданих розподілів частоти та тяжкості кіберінцидентів. Кожна ітерація такого моделювання відповідає одному умовному періоду спостереження (наприклад, року діяльності фінансової установи) і формує одну реалізацію сукупного фінансового збитку [31].

Алгоритмічно процедура моделювання CyVaR методом Монте-Карло може бути подана у вигляді послідовності таких кроків.

Крок 1. Задання моделей частоти та тяжкості.

На першому етапі обираються імовірнісні розподіли, що описують частоту виникнення кіберінцидентів та величину збитків від кожного

інциденту. Частота моделюється як випадкова величина, що описує кількість інцидентів за фіксований період, тоді як тяжкість відображає фінансові наслідки окремої події. Параметри цих розподілів визначаються на основі історичних даних або попереднього статистичного аналізу.

Крок 2. Генерація кількості інцидентів.

Для кожної ітерації моделювання випадковим чином генерується значення кількості кіберінцидентів відповідно до обраного розподілу частоти. Це значення визначає, скільки окремих подій буде враховано у поточному сценарії.

Крок 3. Генерація тяжкості втрат.

Для кожного згенерованого інциденту випадковим чином формується величина фінансового збитку згідно з моделлю тяжкості. Таким чином отримується набір випадкових величин, що відповідають окремим інцидентам у межах одного сценарію.

Крок 4. Агрегація втрат.

Сумарний фінансовий збиток за одну ітерацію визначається як сума згенерованих індивідуальних втрат. Отримане значення є однією реалізацією випадкової величини сукупних збитків.

Крок 5. Багаторазове повторення симуляцій.

Описана процедура повторюється велику кількість разів, що дозволяє сформувати вибірку реалізацій сукупних фінансових втрат. На основі цієї вибірки будується емпіричний розподіл агрегованих збитків.

Крок 6. Оцінювання показника CyVaR.

Показник Cyber Value-at-Risk визначається як відповідний квантиль емпіричного розподілу сукупних втрат на заданому рівні довіри. Таким чином CyVaR оцінюється безпосередньо з результатів симуляцій, без необхідності аналітичного задання функції розподілу.

Застосування методу Монте-Карло є особливо доцільним у контексті кіберризиків, оскільки він дозволяє моделювати широкий спектр сценаріїв, включно з рідкісними, але потенційно катастрофічними подіями, які можуть бути відсутніми або слабо представленими в історичних даних. Саме ця властивість робить метод Монте-Карло ключовим інструментом для дослідження поведінки верхнього хвоста розподілу збитків і забезпечує можливість коректного оцінювання CyVaR для фінансових установ.

3.5 Використання методів MCMC для оцінювання параметрів моделей CyVaR

Однією з ключових проблем кількісного моделювання кіберризиків є обмеженість та неповнота історичних даних про кіберінциденти. На відміну від традиційних фінансових ризиків, для яких доступні великі часові ряди спостережень, дані про кіберінциденти часто є фрагментарними, нерівномірними у часі та схильними до впливу поодиноких екстремальних подій. За таких умов класичні підходи до оцінювання параметрів розподілів, зокрема метод максимальної правдоподібності, можуть призводити до нестабільних або зміщених оцінок, що суттєво знижує надійність подальших розрахунків ризику.

У цьому контексті доцільним є застосування байєсівського підходу до оцінювання параметрів моделей кіберризику, який дозволяє безпосередньо врахувати невизначеність, пов’язану з обмеженістю даних. На відміну від класичних методів, байєсівський підхід розглядає параметри моделей як випадкові величини та описує їх за допомогою апостеріорних розподілів. Це дає змогу перейти від точкових оцінок параметрів до їх повного імовірнісного опису.

Оскільки аналітичний вигляд апостеріорних розподілів для більшості моделей CyVaR є недоступним, їх оцінювання здійснюється із застосуванням методів марковських ланцюгів Монте-Карло (Markov Chain Monte Carlo, MCMC). Основна ідея MCMC полягає у побудові марковського ланцюга, стаціонарний розподіл якого збігається з шуканим апостеріорним розподілом

параметрів. Генеруючи достатньо довгу послідовність станів такого ланцюга, можна отримати вибірку з апостеріорного розподілу та використати її для подальшого аналізу.

У рамках моделей CyVaR методи MCMC застосовуються для оцінювання параметрів як розподілу частоти кіберінцидентів, так і розподілу тяжкості фінансових втрат. Це дозволяє врахувати невизначеність у значеннях параметрів, що безпосередньо впливає на форму агрегованого розподілу збитків та, відповідно, на значення показника Cyber Value-at-Risk.

Одним із найбільш поширених алгоритмів MCMC є алгоритм Метрополіса–Гастінгса, який використовується для генерації марковського ланцюга на основі механізму прийняття або відхилення запропонованих значень параметрів. Алгоритм починається з початкового вектора параметрів, після чого на кожному кроці генерується нова кандидатна точка з певного пропозиційного розподілу. Прийняття або відхилення цієї точки визначається співвідношенням апостеріорних імовірностей, що забезпечує збіжність марковського ланцюга до цільового розподілу [32] [33].

Застосування алгоритму Метрополіса–Гастінгса у моделі CyVaR дозволяє отримати вибірку з апостеріорного розподілу параметрів, на основі якої можна оцінити їх математичне сподівання, дисперсію, довірчі інтервали та інші статистичні характеристики. Важливою перевагою такого підходу є можливість безпосереднього поширення параметричної невизначеності на результати моделювання сукупних втрат і, відповідно, на оцінку CyVaR.

Отже, поєднання методів Монте-Карло для моделювання агрегованих фінансових втрат та методів MCMC для оцінювання параметрів моделей створює цілісну стохастичну рамку аналізу кіберризиків. Такий підхід дозволяє врахувати обмеженість даних, важкохвосту природу розподілів збитків і високий рівень невизначеності, що є характерними особливостями кіберризиків у фінансовому секторі. У наступному підрозділі буде розглянуто практичну реалізацію зазначених методів у межах моделі Cyber Value-at-Risk.

Висновки до розділу 3

У розділі сформовано теоретичні основи моделі Cyber Value-at-Risk як спеціалізованого інструменту кількісного оцінювання кіберризиків у фінансовому секторі. Показано, що модель VaR, яка стала стандартом фінансової математики наприкінці XX століття, створила концептуальне підґрунтя для вимірювання ризиків через граничні втрати, однак її класичні припущення є непридатними для опису природи кіберзбитків. Відмінності між ринковими та кіберризиками, зокрема дискретність інцидентів, важкохвостий характер втрат, обмеженість даних і наявність активного противника, зумовили необхідність формування окремої моделі.

Обґрунтовано логіку переходу від традиційного VaR до CyVaR як самостійної стохастичної моделі, що базується на актуарному підході до аналізу втрат. У межах CyVaR загальні фінансові збитки розглядаються як результат поєднання випадкової частоти кіберінцидентів та випадкової тяжкості фінансових наслідків кожної події, що дозволяє адекватно описати як типові, так і екстремальні сценарії розвитку ризику.

Розкрито математичні засади моделі CyVaR, включно з моделюванням частоти інцидентів, тяжкості фінансових втрат та формуванням агрегованого розподілу збитків. Показано, що відсутність аналітичного виразу для такого розподілу зумовлює необхідність використання імітаційних методів. Визначено показник Cyber Value-at-Risk як ключову кількісну метрику, що фокусується на верхніх квантилях розподілу та відображає потенційні катастрофічні втрати, критичні для фінансової стійкості установ.

Доведено доцільність застосування методу Монте-Карло для чисельного відтворення розподілу сукупних втрат та коректного оцінювання CyVaR за умов високої невизначеності. Окремо обґрунтовано використання байєсівського підходу та методів MCMC для оцінювання параметрів моделей CyVaR, що дозволяє врахувати обмеженість і неповноту даних та поширити параметричну невизначеність на результати розрахунків.

Таким чином, у розділі сформовано цілісну теоретико-математичну основу моделі Cyber Value-at-Risk, яка поєднує актуарні підходи, стохастичне моделювання та байєсівські методи. Отримані положення створюють підґрунтя для практичної реалізації CyVaR та її застосування для оцінювання кіберстійкості фінансових установ у наступних розділах роботи.

4 РЕАЛІЗАЦІЯ МОДЕЛІ ОБЧИСЛЕННЯ CYBER VALUE-AT-RISK

4.1 Загальна архітектура обчислювальної моделі Cyber Value-at-Risk

Реалізація моделі обчислення Cyber Value-at-Risk у межах даного дослідження побудована як багаторівнева стохастична система, що поєднує байєсівське оцінювання параметрів, імітаційне моделювання збитків та обчислення ризикових метрик. Такий підхід дозволяє відокремити процес оцінювання невизначених параметрів від процесу моделювання фінансових втрат і забезпечити їх узгоджену інтеграцію в єдину обчислювальну схему [11].

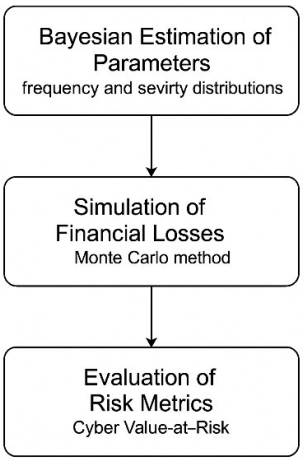

Рисунок 4.1 - Загальна схема алгоритму обчислення Cyber Value-at-Risk на основі методів Monte Carlo та MCMC

Загальна архітектура моделі складається з трьох взаємопов'язаних обчислювальних блоків. Перший блок відповідає за оцінювання параметрів розподілів частоти та тяжкості кіберінцидентів із використанням байєсівського підходу та методів марковських ланцюгів Монте-Карло. На цьому етапі історичні або експертні дані використовуються для формування апостеріорних розподілів параметрів, які відображають невизначеність, притаманну реальним даним про кіберінциденти.

Другий блок реалізує імітаційне моделювання фінансових втрат методом Монте-Карло. Для кожної реалізації параметрів, отриманих на попередньому етапі, генерується велика кількість сценаріїв кіберінцидентів

протягом заданого часового горизонту. У межах кожного сценарію формується випадкова кількість інцидентів і відповідні величини збитків, після чого обчислюється сукупний фінансовий збиток. Таким чином враховується як стохастичність самих інцидентів, так і невизначеність параметрів їх розподілів.

Третій блок призначений для оцінювання ризикових метрик на основі змодельованого розподілу сукупних втрат. На цьому етапі обчислюються значення Cyber Value-at-Risk для заданих рівнів довіри, а також можуть формуватися додаткові показники, що характеризують поведінку верхнього хвоста розподілу. Саме результати цього блоку є кінцевим виходом моделі та використовуються для аналізу фінансової стійкості установи й обґрунтування управлінських рішень.

Ключовою особливістю запропонованої архітектури є чітке розділення ролей між обчислювальними компонентами. Методи МСМС використовуються виключно для оцінювання параметрів і врахування їх невизначеності, тоді як метод Монте-Карло застосовується для моделювання реалізацій фінансових втрат. Така декомпозиція дозволяє гнучко модифікувати окремі елементи моделі, адаптувати її до різних типів даних та забезпечує масштабованість обчислень.

Запропонована архітектура створює основу для подальшої деталізації кожного з етапів реалізації моделі Cyber Value-at-Risk, зокрема опису моделювання частоти та тяжкості кіберінцидентів, процедури байєсівського оцінювання параметрів і алгоритмічної інтеграції Monte Carlo та МСМС в єдину обчислювальну схему [34] [35].

4.2 Реалізація моделювання частоти та тяжкості кіберінцидентів

У межах реалізації моделі Cyber Value-at-Risk моделювання кіберризику ґрунтується на поділі загального процесу втрат на дві стохастичні складові: частоту виникнення кіберінцидентів та тяжкість фінансових втрат, пов’язаних із кожним окремим інцидентом. Такий підхід дозволяє формалізувати процес формування збитків і забезпечує гнучкість моделі щодо адаптації до різних типів даних та сценаріїв.

Моделювання частоти кіберінцидентів здійснюється шляхом генерації випадкової кількості інцидентів N протягом фіксованого часово́го горизонту. У даній реалізації часовий горизонт відповідає одному звітному періоду, що дозволяє інтерпретувати кожну ітерацію моделювання як окремий сценарій розвитку подій за цей період. Значення N генерується згідно з обраним законом розподілу частоти, параметри якого визначаються на попередньому етапі байєсівського оцінювання.

Для кожного згенерованого інциденту формується величина фінансового збитку S_i, яка описується розподілом тяжкості втрат. Генерація значень S_i виконується незалежно для кожного інциденту відповідно до заданого параметричного розподілу, що відображає емпірично спостережувану асиметрію та наявність важкого правого хвоста у розподілах кіберзбитків. Такий підхід дозволяє врахувати можливість рідкісних, але надзвичайно великих фінансових втрат.

Після генерації частоти та тяжкості інцидентів для конкретної ітерації обчислюється сукупний фінансовий збиток як сума індивідуальних втрат. Одна ітерація моделювання, таким чином, відповідає одному можливому сценарію реалізації кіберризику за заданий період часу. Повторення цієї процедури в межах великої кількості ітерацій дозволяє сформувати емпіричний розподіл сукупних збитків.

Важливою особливістю реалізації є те, що параметри розподілів частоти та тяжкості не фіксуються жорстко, а визначаються як випадкові величини, отримані з апостеріорних розподілів на основі методів MCMC. Це означає, що кожен сценарій моделювання враховує не лише випадковість кіберінцидентів, але й невизначеність у параметрах самої моделі.

Така схема моделювання частоти та тяжкості інцидентів забезпечує формування реалістичного розподілу фінансових втрат, який надалі використовується для оцінювання квантильних показників ризику, зокрема Cyber Value-at-Risk, а також для аналізу впливу різних сценаріїв і захисних заходів на рівень кіберризику.

4.3 Байєсівська оцінка параметрів із використанням MCMC

Одним із ключових етапів реалізації моделі обчислення Cyber Value-at-Risk є оцінювання параметрів розподілів частоти та тяжкості кіберінцидентів. У практичних умовах фінансові установи стикаються з обмеженістю, неповнотою та високою варіативністю історичних даних про кіберінциденти, що унеможливлює застосування класичних методів параметричної оцінки без суттєвих спотворень результатів. У зв'язку з цим у межах даного дослідження використано байєсівський підхід до оцінювання параметрів із застосуванням методів марковських ланцюгів Монте-Карло.

Байєсівський підхід дозволяє розглядати параметри розподілів частоти атак та тяжкості фінансових втрат як випадкові величини, для яких формується апостеріорний розподіл на основі поєднання наявних даних і апріорних припущень. Такий підхід є принципово важливим у контексті кіберризику, оскільки дозволяє явно врахувати невизначеність параметрів, а не обмежуватися їх фіксованими точковими оцінками.

У реалізованій моделі оцінювання параметрів виконується окремо для кожного типу кіберзагроз. Для кожного класу атак формується апостеріорний розподіл параметрів, що описують інтенсивність інцидентів, а також параметри розподілу тяжкості збитків. Оцінювання здійснюється за допомогою алгоритмів MCMC, які генерують вибірку значень параметрів, узгоджених із заданою ймовірнісною моделлю та наявними даними. Отримана вибірка використовується надалі як вхід для імітаційного моделювання фінансових втрат методом Монте-Карло.

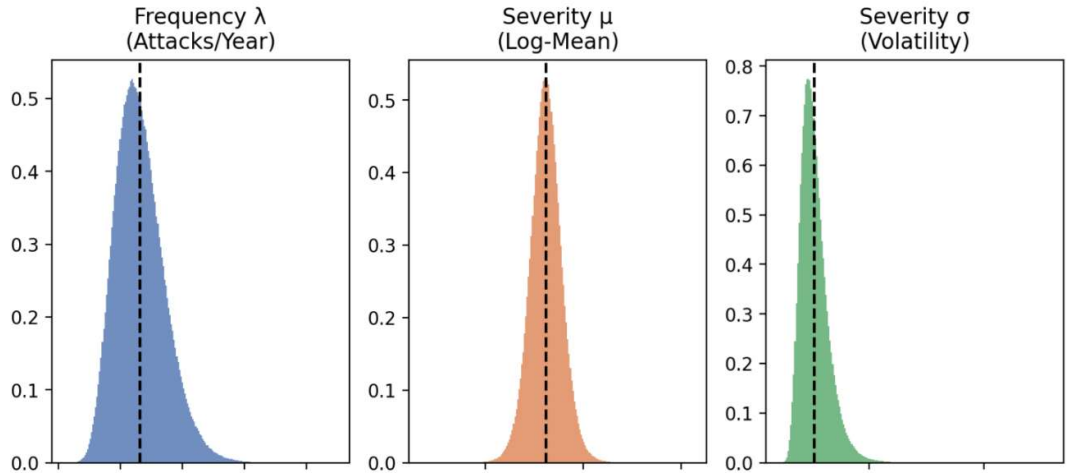

Рисунок 4.2 – Апостеріорні розподіли параметрів частоти та тяжкості для DDoS-атак

На рисунку 4.2 наведено апостеріорні розподіли параметрів частоти та тяжкості для DDoS-атак. Видно, що всі оцінювані параметри характеризуються ненульовою дисперсією та чітко вираженою модальною структурою. Це свідчить про досягнення збіжності марковських ланцюгів і підтверджує, що параметри моделі не можуть бути адекватно описані фіксованими значеннями без урахування невизначеності. Така поведінка апостеріорних розподілів є очікуваною для кіберризиків, які характеризуються високою мінливістю та наявністю рідкісних, але значущих подій.

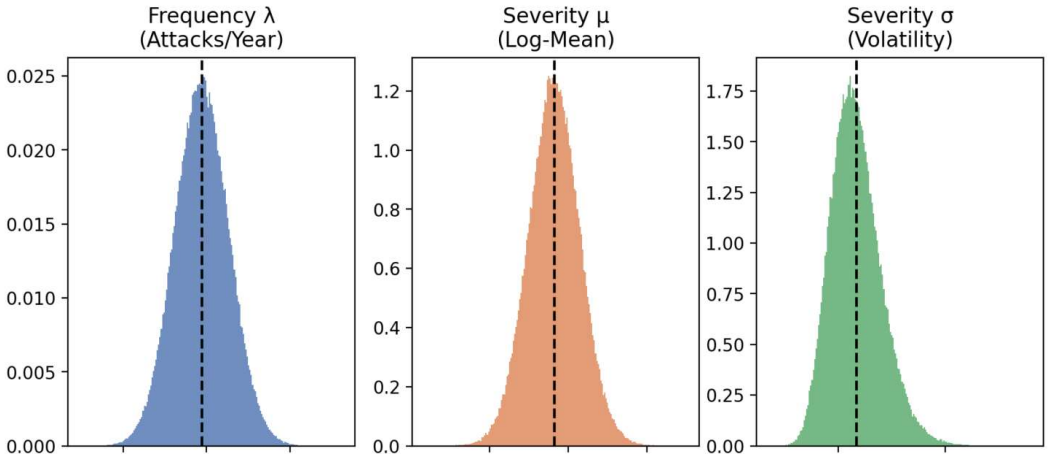

Рисунок 4.3 – Апостеріорні розподіли параметрів частоти та тяжкості для фішингових атак

Аналогічні результати отримано для фішингових атак, що показано на рисунку 4.3. Апостеріорні розподіли параметрів мають іншу форму та ширину порівняно з DDoS-атаками, що відображає відмінності у статистичній природі різних типів кіберзагроз. Це підтверджує доцільність окремого моделювання різних класів атак і виключає можливість їх коректного опису в межах єдиної універсальної параметричної моделі.

Для забезпечення коректності байєсівського оцінювання в реалізації передбачено автоматичний контроль збіжності алгоритмів MCMC. Для кожного типу атак алгоритм виконується до досягнення заданого порогу похибки, після чого формування вибірки параметрів припиняється. Інформація про процес збіжності наведена на рисунку 4.4.

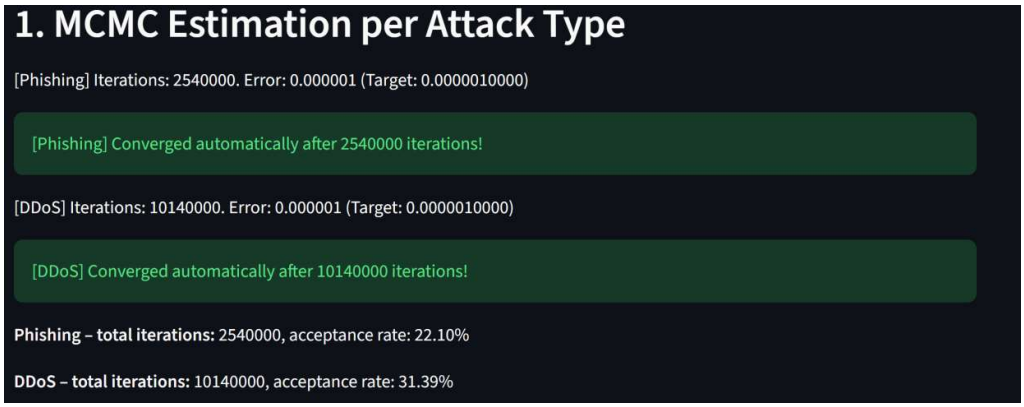

Рисунок 4.4 – Інформація про збіжність алгоритму MCMC для різних типів атак

Результати оцінювання параметрів за допомогою методів MCMC демонструють різну динаміку збіжності для окремих типів кіберзагроз. Зокрема, для фішингових атак алгоритм досяг збіжності після 2 540 000 ітерацій із коефіцієнтом прийняття 22,10 %, тоді як для DDoS-атак процес оцінювання потребував 10 140 000 ітерацій, а коефіцієнт прийняття становив 31,39 %.

Значно більша кількість ітерацій, необхідна для досягнення збіжності у випадку DDoS-атак, пояснюється складнішою структурою параметричного простору та вищою чутливістю моделі до змін параметрів тяжкості збитків.

DDoS-атаки характеризуються ширшим діапазоном можливих фінансових наслідків і більш вираженою важкохвостою поведінкою розподілів, що ускладнює навігацію марковського ланцюга та потребує більшої кількості кроків для стабілізації апостеріорного розподілу.

Коефіцієнт прийняття (acceptance rate) є одним із ключових показників якості роботи алгоритму Метрополіса–Гастінгса. Він відображає частку запропонованих кроків у просторі параметрів, які були прийняті в процесі побудови марковського ланцюга. Надто низькі значення коефіцієнта прийняття свідчать про надмірно агресивні кроки пропозиційного розподілу, тоді як надто високі значення вказують на повільне дослідження простору параметрів.

Отримані у межах даного дослідження значення коефіцієнта прийняття перебувають у рекомендованому для алгоритмів МСМС діапазоні. Для фішингових атак acceptance rate на рівні близько 22 % свідчить про ефективний компроміс між швидкістю дослідження параметричного простору та стабільністю ланцюга. У випадку DDoS-атак вищий коефіцієнт прийняття (31,39 %) відображає необхідність більш дрібних кроків у просторі параметрів через складнішу форму апостеріорного розподілу, що є типовим для моделей із вираженою важкохвостою поведінкою.

Отже, різниця у кількості ітерацій та коефіцієнтах прийняття для різних типів атак не є недоліком реалізації, а навпаки — підтверджує адаптивність алгоритму МСМС до статистичних властивостей конкретного класу кіберзагроз. Досягнення збіжності за заданим критерієм похибки для обох типів атак свідчить про коректність реалізованої процедури байєсівського оцінювання параметрів і забезпечує надійну основу для подальшого імітаційного моделювання фінансових втрат методом Монте-Карло та обчислення показника Cyber Value-at-Risk.

4.4 Аналіз агрегованого розподілу фінансових втрат та оцінка Cyber Value-at-Risk

Після байєсівської оцінки параметрів частоти та тяжкості кіберінцидентів із використанням методів MCMC, наступним етапом реалізації моделі стало імітаційне моделювання агрегованих фінансових втрат методом Монте-Карло. На цьому етапі для кожної симуляції випадковим чином генерувалася кількість інцидентів відповідно до апостеріорного розподілу параметрів частоти, а також величини збитків для кожного інциденту на основі апостеріорних розподілів параметрів тяжкості. Сумування цих збитків формувало одну реалізацію річних фінансових втрат.

4.4.1 Порівняння розподілів втрат для окремих типів атак

На рисунку 4.5 наведено порівняння емпіричних розподілів річних втрат для фішингових та DDoS-атак у лінійній шкалі.

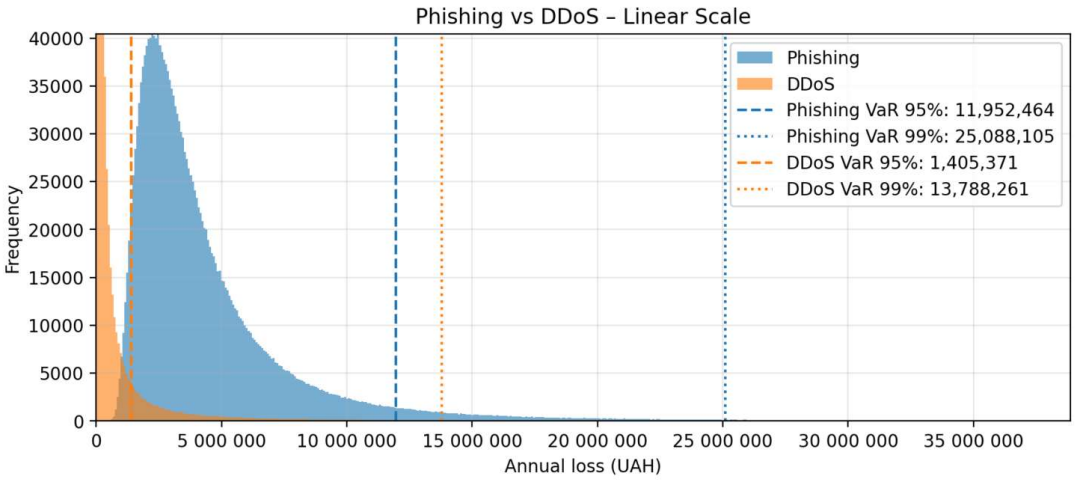

Рисунок 4.5 – Порівняння розподілів річних втрат для фішингових та DDoS-атак (лінійна шкала)

Видно, що фішингові атаки формують ширший розподіл із більшою концентрацією ймовірності у середньому діапазоні втрат, тоді як DDoS-атаки характеризуються значно меншою середньою величиною збитків, але з наявністю екстремальних сценаріїв.

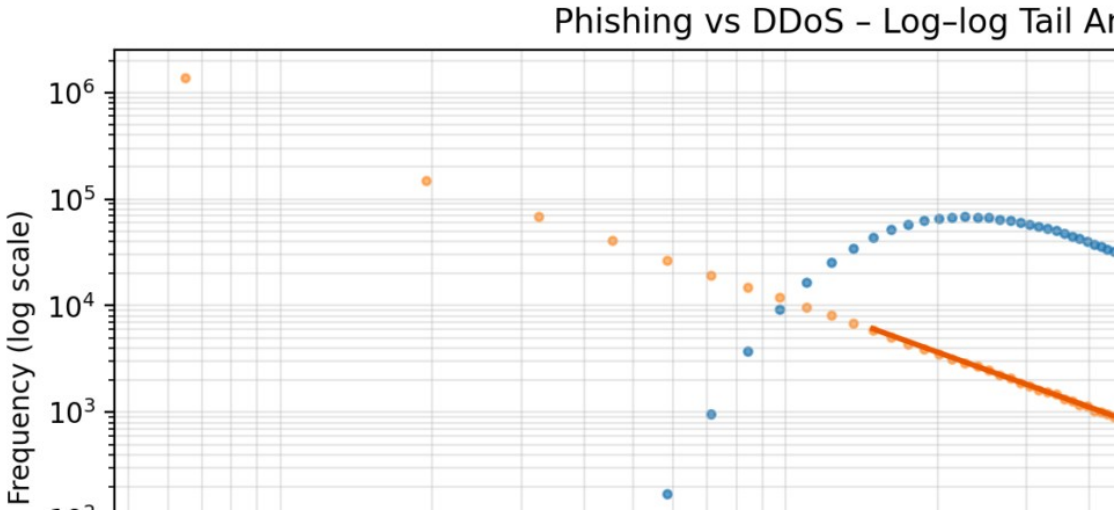

Рисунок 4.6 – Аналіз верхніх хвостів розподілів втрат для фішингових та DDoS-атак (log–log масштаб)

Для детальнішого аналізу поведінки верхніх хвостів розподілів фінансових втрат на рисунку 4.6 ті самі дані подано у логарифмічній шкалі. Лінійна структура емпіричних точок у log–log масштабі в області великих значень збитків свідчить про наявність важкохвостих властивостей розподілів для обох типів атак. Оцінка нахилу хвостів показує, що для фішингових атак спостерігається крутіший спад частоти великих втрат (tail slope ≈ −3.18), що вказує на швидше зменшення ймовірності екстремальних значень. Натомість для DDoS-атак хвіст розподілу є більш «важким» (tail slope ≈ −1.71), що означає повільніший спад і, відповідно, вищу відносну ймовірність виникнення надзвичайно великих фінансових збитків. Це підтверджує, що хоча DDoS-атаки можуть траплятися рідше, їх потенційний економічний вплив у крайніх сценаріях є значно більш загрозливим, що має принципове значення для оцінювання верхніх квантилів у моделі Cyber Value-at-Risk.

4.4.2 Оцінка CyVaR та аналіз агрегованого розподілу фінансових втрат

У результаті імітаційного моделювання фінансових втрат методом Монте-Карло з використанням апостеріорних розподілів параметрів, отриманих за допомогою MCMC, було розраховано ключові кількісні показники

кіберризику на основі моделі Cyber Value-at-Risk. Отримані значення CyVaR дозволяють оцінити потенційні втрати фінансової установи в екстремальних сценаріях з рівнями довіри 95% та 99%, а також порівняти внесок окремих типів кіберзагроз у формування сукупного ризику.

Подальші результати відображають як очікувані річні втрати (Expected Annual Loss), так і значення CyVaR для фішингових атак, DDoS-атак та їх агрегованого впливу:

- Phishing – Expected Annual Loss: *4,848,637 UAH*
- Phishing – CyVaR 95%: *11,952,464 UAH*
- Phishing – CyVaR 99%: *25,088,105 UAH*
- DDoS – Expected Annual Loss: *556,760,172 UAH*
- DDoS – CyVaR 95%: *1,405,371 UAH*
- DDoS – CyVaR 99%: *13,788,261 UAH*
- Total – Expected Annual Loss: *561,608,809 UAH*
- Total – CyVaR 95%: *13,869,374 UAH*
- Total – CyVaR 99%: *37,023,384 UAH*

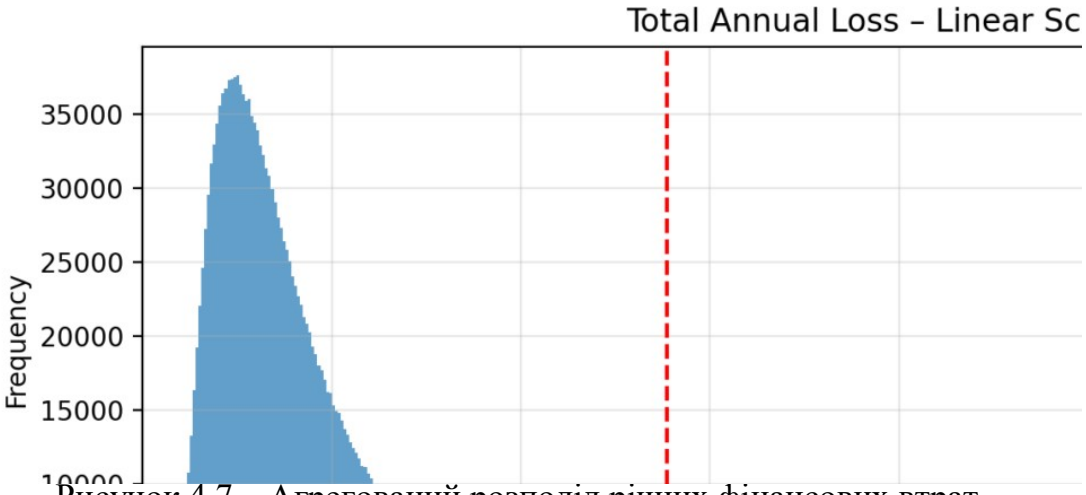

Рисунок 4.7 – Агрегований розподіл річних фінансових втрат (лінійна шкала)

На рисунку 4.7 наведено агрегований розподіл річних фінансових втрат, сформований у результаті імітаційного моделювання методом Монте-Карло з урахуванням апостеріорних розподілів параметрів, отриманих за допомогою

MCMC. Розподіл побудовано як суму втрат від фішингових та DDoS-атак, що дозволяє оцінити сукупний кіберризик для фінансової установи протягом одного року.

У лінійній шкалі розподіл має виражену асиметрію з довгим правим хвостом, що свідчить про наявність рідкісних, але потенційно катастрофічних сценаріїв збитків. Вертикальними пунктирними лініями на графіку відмічено значення CyVaR на рівнях довіри 95% та 99%. Отримані оцінки становлять відповідно 13,87 млн грн для $CyVaR_{0.95}$ та 37,02 млн грн для $CyVaR_{0.99}$, що демонструє суттєве зростання потенційних втрат у верхніх квантилях розподілу.

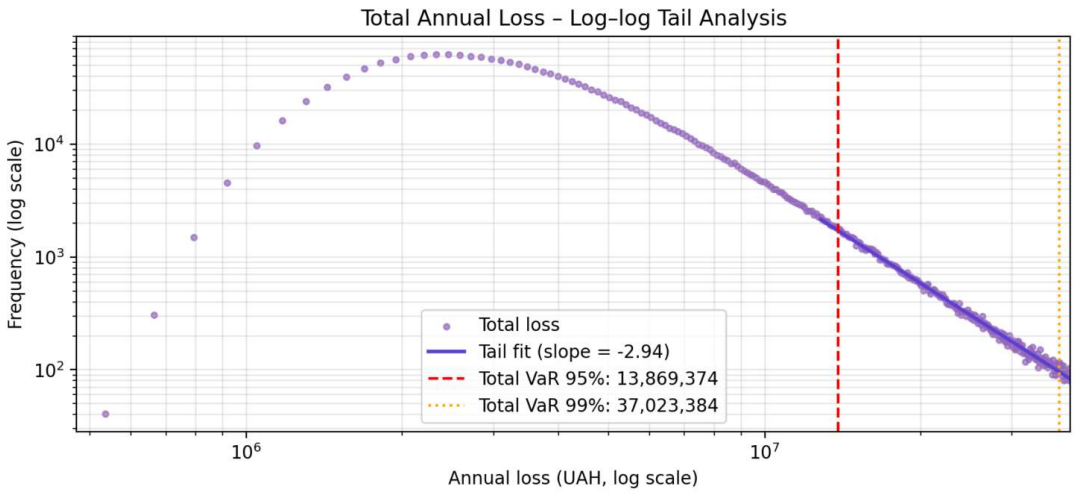

Рисунок 4.8 – Верхній хвіст агрегованого розподілу фінансових втрат (log–log аналіз)

Для детального аналізу екстремальних сценаріїв фінансових втрат на рисунку 4.8 наведено логарифмічне представлення верхнього хвоста агрегованого розподілу річних збитків. Використання log–log масштабу дозволяє дослідити асимптотичну поведінку розподілу у зоні великих значень втрат, яка є критично важливою для оцінювання кіберризиків у фінансовому секторі.

Отриманий вигляд емпіричних точок у log–log просторі демонструє наближену лінійну структуру в області верхнього хвоста, що є характерною ознакою важкохвостих розподілів. Оцінка нахилу хвоста агрегованого

розподілу становить приблизно −2.94, що вказує на степеневий характер спадання ймовірності великих втрат. Подібні значення параметра хвоста є типовими для фінансових, операційних та кіберризиків, для яких показник степеня зазвичай перебуває у діапазоні $2 < \alpha < 4$.

Отримані результати узгоджуються з висновками, представленими у попередніх дослідженнях авторів, зокрема у роботі «Оцінювання ймовірності фінансових втрат фінансової установи внаслідок кіберзагроз методом Монте-Карло» Заріцького О. В. та Гальчинського Л. Ю. [11], де було показано, що фінансові втрати від кіберінцидентів у діяльності фінансових установ характеризуються асиметричними розподілами з довгими правими хвостами. У зазначеній статті наголошується, що саме екстремальні події, а не середні значення збитків, формують ключові ризикові характеристики системи та визначають потребу в резервуванні капіталу.

З точки зору теорії екстремальних значень, така поведінка агрегованого розподілу є типовою для розподілів класу Парето та узагальненого розподілу Парето (Generalized Pareto Distribution, GPD) [36], які широко застосовуються для моделювання екстремальних фінансових та кібернетичних ризиків. Важкохвостий характер означає, що ймовірність виникнення надзвичайно великих збитків зменшується значно повільніше, ніж у випадку експоненційних або нормальних розподілів, що робить класичні підходи до оцінювання ризику непридатними для аналізу верхніх квантилів.

Водночас отримане значення нахилу хвоста (≈ -2.94) свідчить про скінченність математичного сподівання, але про високу чутливість до одиничних екстремальних інцидентів. Саме така комбінація властивостей є характерною для кіберризиків у фінансовому секторі, де більшість інцидентів мають обмежений вплив, але поодинокі події можуть призводити до значних системних втрат. Аналогічна інтерпретація хвостових властивостей розподілу наводиться у вже згаданій роботі Заріцького О. В. та Гальчинського Л. Ю. [11], де підкреслюється роль екстремальних значень у формуванні сукупного кіберризику.

Отже, результати імітаційного моделювання підтверджують, що агрегований кіберризик формується передусім поведінкою верхнього хвоста розподілу фінансових втрат. Саме ця частина розподілу визначає значення Cyber Value-at-Risk на високих рівнях довіри та є критичною з точки зору управління капіталом, оцінювання кіберстійкості та обґрунтування інвестицій у заходи кіберзахисту. Отримані результати логічно доповнюють і розвивають підходи, запропоновані у попередніх дослідженнях авторів, підтверджуючи доцільність використання моделей, орієнтованих на аналіз екстремальних фінансових втрат.

4.5 Реалізація та моделювання впливу контролів ІБ у моделі CyVaR

Після побудови базової моделі Cyber Value-at-Risk та оцінювання агрегованого розподілу фінансових втрат, наступним етапом дослідження стало моделювання впливу заходів кіберзахисту на рівень кіберризику фінансової установи. З цією метою в рамках реалізованої моделі було впроваджено механізм what-if аналізу, який дозволяє кількісно оцінити, яким чином окремі мітигаційні контроли впливають на частоту виникнення кіберінцидентів та/або тяжкість фінансових наслідків.

На відміну від традиційного якісного підходу до оцінювання ефективності заходів захисту, запропонована реалізація дозволяє інтегрувати контроли безпосередньо у стохастичну модель CyVaR, що забезпечує оцінку їх впливу не лише на середні втрати, але й на поведінку верхніх квантилів розподілу.

4.5.1 Формалізація контролів ІБ у кількісній моделі

У рамках what-if сценарію контроли задаються у вигляді мультиплікативних коефіцієнтів, які впливають на параметри частоти та тяжкості атак:

для прикладу фішингових атак:

- зниження частоти на 5% (frequency × 0.95),
- тяжкість збитків не змінюється (severity × 1.00);

для прикладу DDoS-атак:

- частота атак не змінюється (frequency × 1.00),
- зменшення тяжкості збитків на 10% (severity × 0.90).

Такий підхід відповідає реальній практиці впровадження кіберзахисту, де окремі заходи (наприклад, антифішингові тренінги або фільтрація трафіку) по-різному впливають на ймовірність атаки та масштаби її наслідків [37] [38].

Після застосування відповідних коефіцієнтів апостеріорні розподіли параметрів використовуються повторно в імітаційному моделюванні методом Монте-Карло для формування нового розподілу річних фінансових втрат.

4.5.2 Фінансові показники ризику з урахуванням контролів

Результати моделювання з урахуванням заходів безпеки наведено у вигляді оновлених показників Expected Annual Loss та Cyber Value-at-Risk.

Для фішингових атак отримано такі значення:

- Expected Annual Loss зменшився до 4,61 млн грн,
- $CyVaR_{0.95}$ становить 11,36 млн грн,
- $CyVaR_{0.99}$ — 23,93 млн грн.

Для DDoS-атак:

- Expected Annual Loss становить 309,77 млн грн,
- $CyVaR_{0.95}$ знизився до 1,27 млн грн,
- $CyVaR_{0.99}$ — до 12,70 млн грн.

Агрегований ризик для фінансової установи з урахуванням контролів характеризується такими значеннями:

- *Total Expected Annual Loss — 309,78 млн грн,*
- *Total $CyVaR_{0.95}$ — 13,16 млн грн,*
- *Total $CyVaR_{0.99}$ — 34,89 млн грн.*

Порівняння з базовим сценарієм без контролів свідчить про систематичне зменшення значень CyVaR, особливо у верхніх квантилях, що є критично важливим з точки зору кіберстійкості.

4.5.3 Порівняння розподілів втрат «до» та «після» впровадження контролів

На рисунку 4.9 наведено порівняння агрегованих розподілів річних фінансових втрат фінансової установи у базовому сценарії та після впровадження заходів ІБ. Порівняння здійснюється на основі результатів імітаційного моделювання методом Монте-Карло з використанням однакової кількості симуляцій, що забезпечує коректність зіставлення.

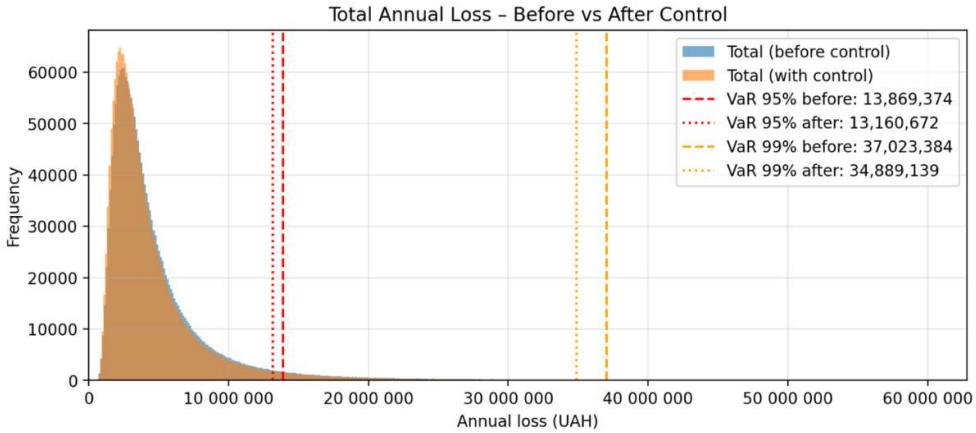

Рисунок 4.9 – порівняння агрегованих розподілів річних фінансових втрат до та після впровадження додаткових заходів ІБ

Графічний аналіз показує, що після застосування контролів основна маса розподілу зміщується ліворуч, що свідчить про зниження типових значень річних фінансових втрат. Водночас найбільш важливим з точки зору управління кіберризиком є зміна поведінки правого хвоста розподілу, оскільки саме він визначає ймовірність реалізації екстремальних, катастрофічних сценаріїв.

Кількісно вплив контролів на верхні квантилі розподілу характеризується такими результатами:

- значення $CyVaR_{0.95}$ зменшилося на 708 тис. грн, що відповідає приблизно 5,1% зниженню ризику на рівні 95% довіри;
- значення $CyVaR_{0.99}$ зменшилося на 2,13 млн грн, або приблизно 5,8%.

Показник $CyVaR_{0.95}$ відображає рівень втрат, який з імовірністю 95% не буде перевищений протягом року, і використовується для оцінки «серйозних, але правдоподібних» сценаріїв. Відповідно, $CyVaR_{0.99}$ характеризує вже екстремальні сценарії, які реалізуються з малою імовірністю, але можуть мати критичні наслідки для фінансової стійкості установи.

Отримані результати свідчать, що впроваджені мітигаційні заходи впливають не лише на середній рівень збитків, а й суттєво знижують ризик реалізації найбільш небезпечних сценаріїв, які формують правий хвіст розподілу. Це є принципово важливим, оскільки саме ці сценарії визначають потребу в резервуванні капіталу та рівень кіберстійкості фінансової установи.

4.5.4 Економічна ефективність мітигаційних заходів

Для оцінювання доцільності впровадження заходів кіберзахисту в рамках дослідження використано показники економічної ефективності, які дозволяють зіставити отримане зниження ризику з витратами на реалізацію контролів. Сукупні річні витрати на впровадження мітигаційних заходів у розглянутому сценарії становлять 22 тис. грн.

Показник ROSI (Return on Security Investment), розрахований на основі Expected Annual Loss, має негативне значення. Це пояснюється тим, що середні втрати у важкохвостих розподілах є нестабільними та можуть істотно змінюватися під впливом одиничних великих інцидентів. Відповідно, показники, що базуються виключно на математичному сподіванні, не завжди коректно відображають реальну цінність заходів кіберзахисту в контексті екстремальних ризиків [39] [40].

Натомість використання Ra (Risk-adjusted Return on Security Investment) дозволяє оцінити ефективність контролів з урахуванням саме верхніх квантилів розподілу втрат:

- $RaROSI_{0.95}$ = 31,21 означає, що кожна гривня, інвестована в заходи захисту, забезпечує понад 31 гривню зниження ризику на рівні $CyVaR_{0.95}$;

- $RaROSI_{0.99}$ = 96,01 свідчить про ще вищу ефективність заходів у контексті екстремальних сценаріїв.

З позиції управління саме екстремальними кіберризиками, впроваджені мітигаційні заходи є економічно обґрунтованими, навіть попри відносно невеликий вплив на середні значення втрат.

Отримані результати підтверджують, що оцінювання ефективності заходів кіберзахисту доцільно здійснювати не лише на основі середніх значень втрат, а передусім через аналіз поведінки верхнього хвоста розподілу фінансових втрат, який визначає значення Cyber Value-at-Risk. Саме ці екстремальні сценарії є критичними для фінансової стійкості установи та потребують формалізованого кількісного аналізу.

Інтеграція можливості обрахунку впливу контролів ІБ у модель CyVaR дозволяє перейти від описового аналізу кіберзагроз до ризик-орієнтованого підходу до прийняття управлінських рішень. Реалізована модель забезпечує можливість проведення what-if аналізу, в межах якого оцінюється вплив різних сценаріїв впровадження контролів на рівень фінансового ризику та економічну доцільність інвестицій у кіберзахист.

Таким чином, модель Cyber Value-at-Risk у поєднанні з байєсівською оцінкою параметрів та імітаційним моделюванням може розглядатися як інструмент підтримки прийняття рішень для керівництва фінансової установи. Вона дозволяє обґрунтовано визначати доцільність інвестування у заходи кібербезпеки, пріоритизувати контролі за їх впливом на зниження екстремальних втрат та підвищувати рівень кіберстійкості фінансової установи в цілому [41].

Висновки до розділу 4

У розділі реалізовано прикладну обчислювальну модель Cyber Value-at-Risk, побудовану як багаторівнева стохастична система, що інтегрує байєсівське оцінювання параметрів (MCMC), імітаційне моделювання втрат (Monte Carlo) та розрахунок ризикових метрик. Запропонована архітектура забезпечує логічне розділення етапів оцінювання невизначених параметрів і

генерації сценаріїв збитків, що підвищує гнучкість, масштабованість і відтворюваність обчислень.

У межах реалізації кіберризик формалізовано через дві стохастичні компоненти — частоту інцидентів і тяжкість фінансових наслідків — із подальшим формуванням емпіричного розподілу річних сукупних втрат. Принциповою особливістю моделі є використання параметрів не як фіксованих значень, а як випадкових величин з апостеріорних розподілів, що дозволяє коректно врахувати невизначеність, зумовлену обмеженістю та варіативністю даних про кіберінциденти.

Результати MCMC-оцінювання показали, що різні типи атак мають відмінні статистичні властивості та потребують окремого параметричного опису. Отримані апостеріорні розподіли характеризуються ненульовою дисперсією, а також відмінностями у формі та ширині для фішингових і DDoS-атак, що підтверджує доцільність диференційованого моделювання класів загроз. Аналіз збіжності алгоритмів MCMC засвідчив коректність байєсівської процедури оцінювання параметрів і адаптивність до складності параметричного простору для різних типів атак.

Імітаційне моделювання методом Монте-Карло дозволило отримати емпіричні розподіли річних втрат і кількісно оцінити поведінку їх верхніх хвостів. Log–log аналіз підтвердив важкохвосту природу втрат як для окремих типів атак, так і для агрегованого розподілу, що є критичним для коректного оцінювання верхніх квантилів. На основі змодельованого агрегованого розподілу визначено значення CyVaR на рівнях довіри 95% та 99%, які відображають масштаб потенційних екстремальних збитків і можуть бути використані як практична метрика кіберстійкості фінансової установи.

Окремо реалізовано механізм what-if аналізу для моделювання впливу контролів інформаційної безпеки на параметри частоти та/або тяжкості інцидентів. Порівняння розподілів «до» та «після» впровадження контролів показало зміщення розподілу втрат у бік менших значень і, що є найбільш важливим, зменшення правого хвоста, який визначає екстремальні сценарії. Це

підтверджено зниженням значень CyVaR у верхніх квантилях, що свідчить про підвищення кіберстійкості установи.

Економічну ефективність заходів кіберзахисту проаналізовано через Risk-adjusted ROSI, що орієнтується на зниження ризику саме у верхніх квантилях розподілу. Показано, що за важкохвостих розподілів показники, засновані на середніх значеннях, можуть бути недостатньо інформативними, тоді як RaROSI демонструє суттєву ефективність контролів у контексті зменшення екстремальних втрат. У підсумку реалізована модель CyVaR може розглядатися як інструмент підтримки прийняття рішень, який дозволяє кількісно оцінювати кіберризик, порівнювати сценарії та обґрунтовувати інвестиції в кіберзахист з урахуванням найбільш небезпечних сценаріїв.

5 ПРОГРАМНА РЕАЛІЗАЦІЯ МОДЕЛІ CYBER VALUE-AT-RISK У ВИГЛЯДІ ВЕБЗАСТОСУНКУ

У межах даної магістерської роботи кількісна модель оцінювання кіберризиків, побудована на основі байєсівської оцінки параметрів, методів марковських ланцюгів Монте-Карло та імітаційного моделювання методом Монте-Карло, була реалізована у вигляді веб-орієнтованого програмного застосунку. Розроблений веб-застосунок не вводить додаткових спрощень, а безпосередньо реалізує математичний апарат, описаний у попередніх розділах роботи.

Основною метою створення веб-застосунку є забезпечення зручного інтерфейсу для запуску обчислювальних процедур, аналізу результатів моделювання та проведення what-if сценаріїв без необхідності прямої взаємодії з програмним кодом. Таким чином, веб-застосунок виступає як прикладна надбудова над кількісною моделлю Cyber Value-at-Risk та слугує інструментом підтримки прийняття управлінських рішень.

Функціонально веб-застосунок реалізує повний цикл оцінювання кіберризику, який відповідає математичній послідовності, викладеній у розділах 3–4 даної роботи. Загальна логіка його роботи включає такі етапи:

- байєсівське оцінювання параметрів частоти та тяжкості кіберінцидентів із використанням методів MCMC;
- формування апостеріорних розподілів параметрів моделей;
- імітаційне моделювання агрегованих фінансових втрат методом Монте-Карло;
- обчислення показників Expected Annual Loss та Cyber Value-at-Risk;
- моделювання впливу заходів ІБ у форматі what-if сценаріїв;
- аналіз економічної ефективності інвестицій у заходи кіберзахисту.

Усі обчислення виконуються відповідно до формальних математичних моделей, наведених у теоретичній частині, а веб-інтерфейс забезпечує лише їх параметризацію та візуалізацію результатів.

Для забезпечення наочності та інтерпретованості результатів веб-застосунок формує набір графіків та таблиць, які безпосередньо відображають етапи обчислень. Доцільним є розміщення таких ілюстрацій у роботі:

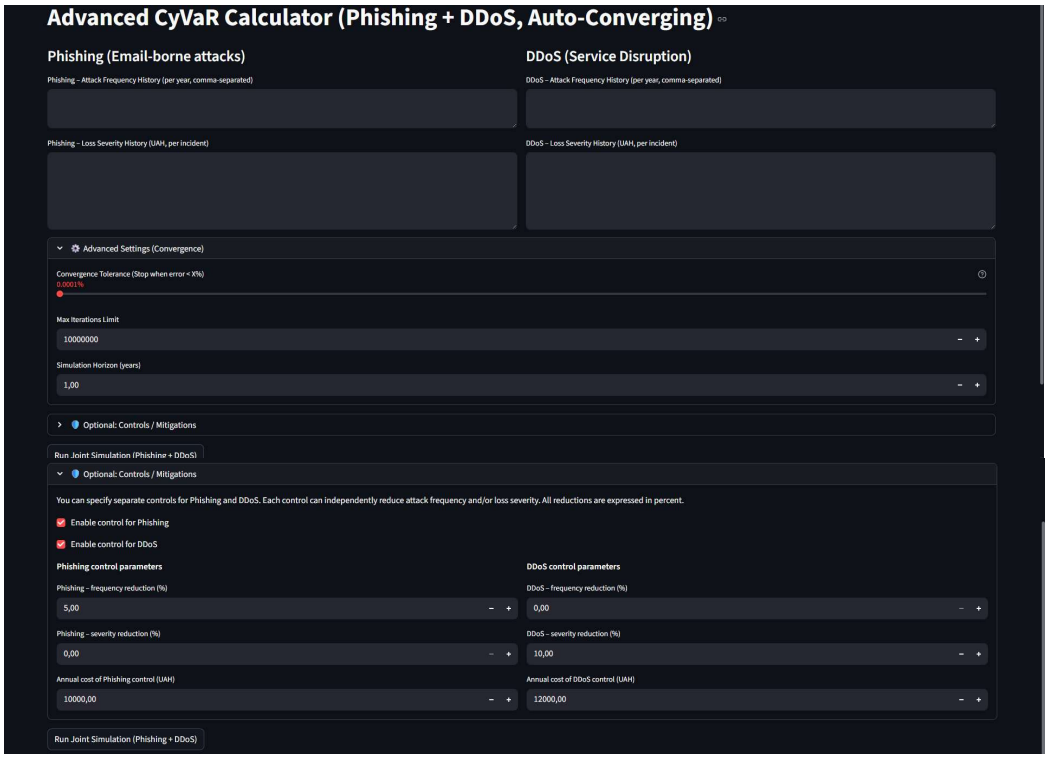

Рисунок 5.1 – Загальний вигляд вебінтерфейсу застосунку з основними блоками параметризації моделей

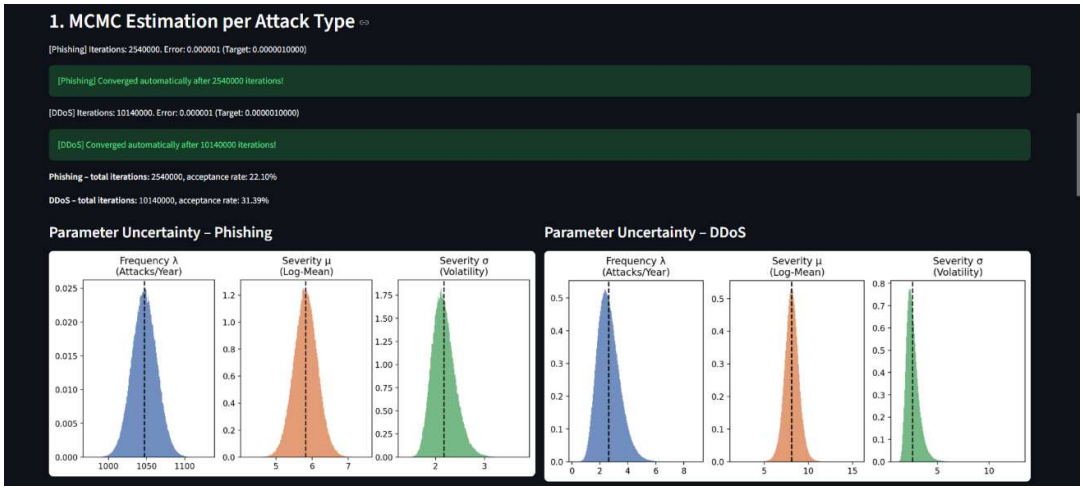

Рисунок 5.2 – Візуалізація апостеріорних розподілів параметрів частоти та тяжкості атак

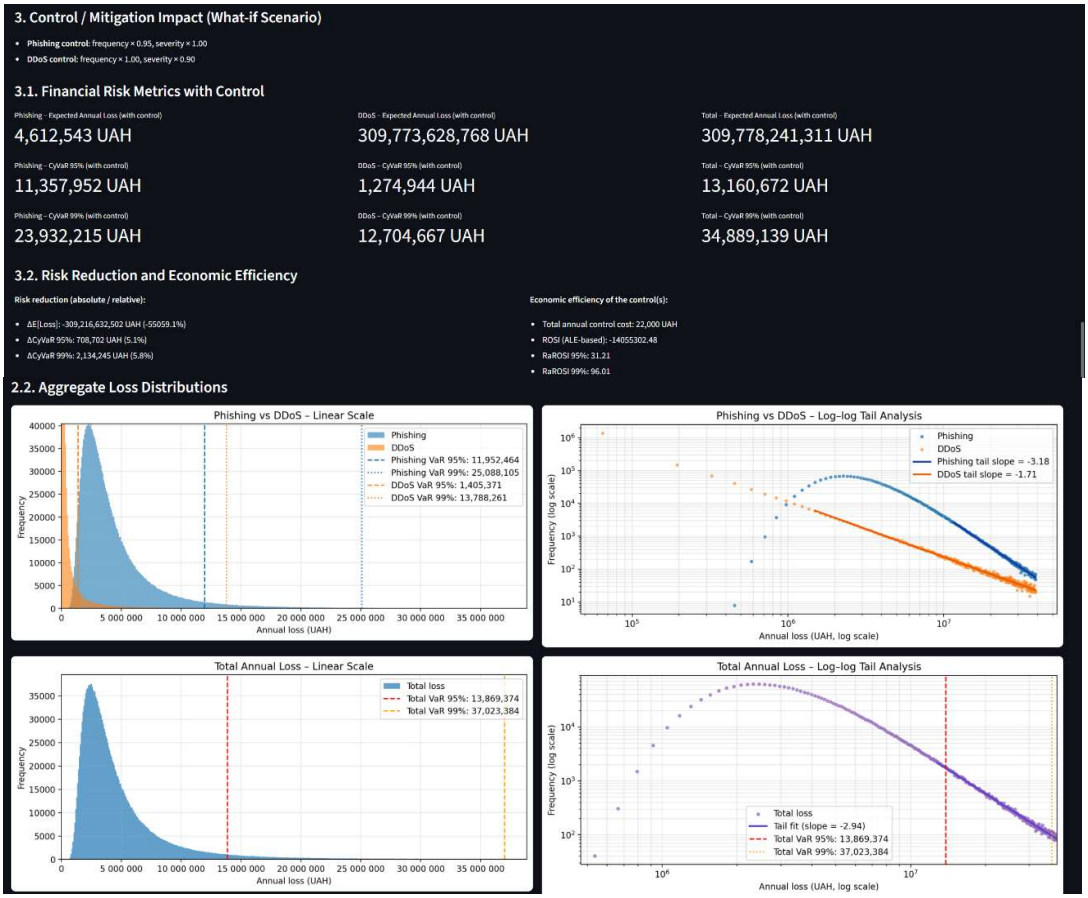

Рисунок 5.3 – Результати імітаційного моделювання фінансових втрат та оцінки CyVaR

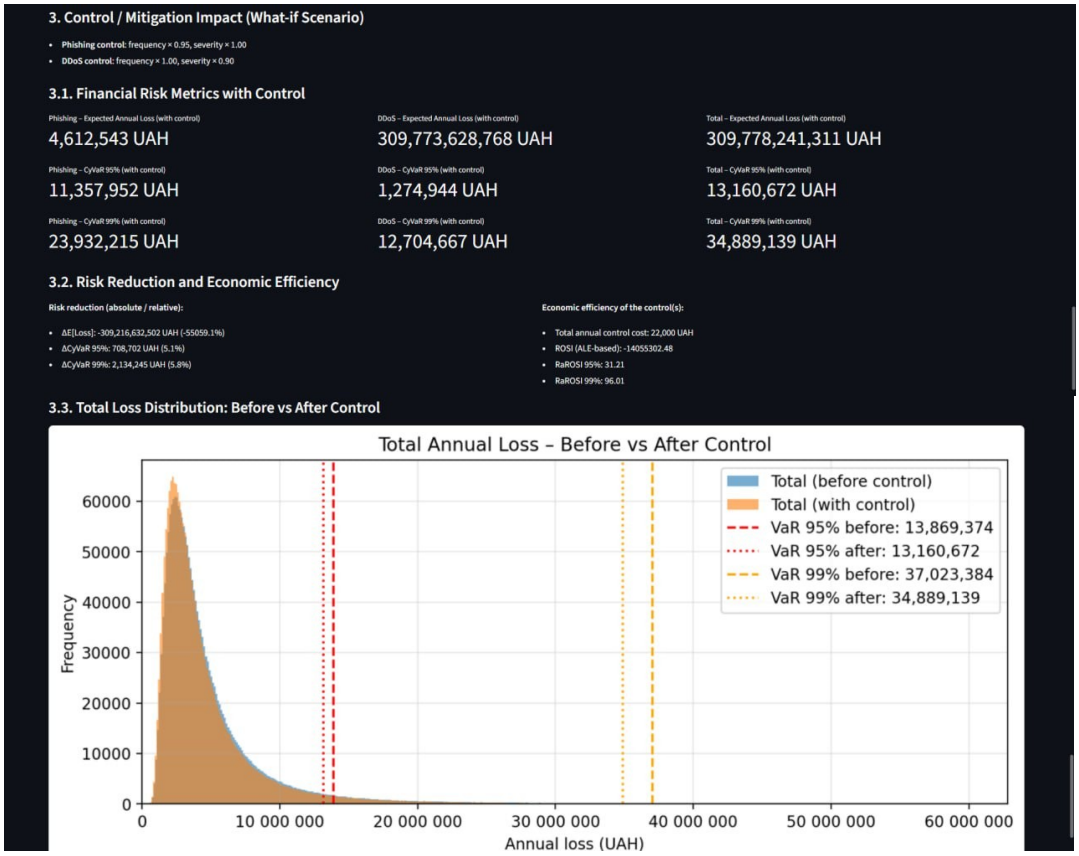

Рисунок 5.4 – Порівняння розподілів втрат до та після впровадження заходів кіберзахисту

Такий порядок розміщення ілюстрацій забезпечує логічну відповідність між описом алгоритмів, результатами моделювання та їх візуальним представленням.

Отже, у межах роботи було реалізовано вебзастосунок, який є прикладною реалізацією кількісної моделі Cyber Value-at-Risk. Усі обчислювальні процедури в застосунку відповідають математичному апарату, описаному у теоретичній та методичній частинах роботи, а вебінтерфейс виконує роль зручного інструменту доступу до результатів моделювання.

Розроблений вебзастосунок дозволяє застосовувати модель CyVaR на практиці як інструмент підтримки прийняття рішень, зокрема для оцінювання доцільності інвестування у заходи кіберзахисту, аналізу сценаріїв та підвищення рівня кіберстійкості фінансової установи.

Висновки до розділу 5

У розділі представлено програмну реалізацію моделі Cyber Value-at-Risk у форматі вебзастосунку, який безпосередньо відтворює математичний апарат, описаний у попередніх розділах, без додаткових спрощень. Вебінтерфейс забезпечує зручну параметризацію моделей, запуск обчислювальних процедур та наочну візуалізацію результатів, що усуває потребу у прямій роботі з програмним кодом.

Функціонально застосунок підтримує повний цикл оцінювання кіберризику: байєсівське оцінювання параметрів (MCMC), імітаційне моделювання втрат (Monte Carlo), розрахунок Expected Annual Loss та CyVaR, проведення what-if сценаріїв і оцінку економічної ефективності заходів кіберзахисту. Таким чином, розроблений вебзастосунок може використовуватися як практичний інструмент підтримки прийняття рішень для аналізу кіберризиків і обґрунтування інвестицій у кібербезпеку у фінансових установах.

ВИСНОВКИ

У магістерській роботі було досліджено проблему кількісного оцінювання кіберризиків у фінансовому секторі з акцентом на аналіз екстремальних фінансових втрат та забезпечення кіберстійкості фінансових установ. Актуальність обраної тематики зумовлена зростанням інтенсивності та складності кіберзагроз, збільшенням цифрової залежності фінансових процесів, а також обмеженістю традиційних підходів до оцінювання ризиків, які не враховують важкохвосту природу кіберзбитків і невизначеність параметрів моделей.

У теоретичній частині роботи проведено аналіз еволюції підходів до оцінювання ризиків — від якісних і напівкількісних методів до сучасних кількісних моделей. Показано, що класичні підходи, які ґрунтуються на експертних оцінках або спрощених шкалах ризику, є недостатніми для прийняття обґрунтованих управлінських рішень у фінансовому секторі. Особливу увагу приділено концепції Cyber Value-at-Risk як інструменту кількісної оцінки кіберризику, який дозволяє аналізувати не лише середні втрати, а й екстремальні сценарії, що визначають потребу в резервуванні капіталу та рівень кіберстійкості організації.

У роботі обґрунтовано, що кіберризики мають стохастичну природу та характеризуються складною структурою, яка формується комбінацією випадкової кількості інцидентів і випадкової тяжкості їх наслідків. Показано, що емпіричні розподіли фінансових втрат від кіберінцидентів є далекими від нормального закону та демонструють важкохвості властивості, характерні для степеневих законів, зокрема розподілів типу Парето та узагальненого розподілу Парето (GPD). Така поведінка розподілів підтверджує доцільність застосування методів теорії екстремальних значень та орієнтації аналізу саме на верхні квантилі розподілу втрат.

У прикладній частині роботи реалізовано повну кількісну модель оцінювання кіберризиків на основі CyVaR, яка поєднує байєсівську оцінку параметрів, методи марковських ланцюгів Монте-Карло та імітаційне

моделювання методом Монте-Карло. Для оцінювання параметрів частоти та тяжкості кіберінцидентів використано алгоритм Метрополіса–Гастінгса, що дозволило сформувати апостеріорні розподіли параметрів та врахувати невизначеність, зумовлену обмеженістю історичних даних. Проведений аналіз збіжності MCMC-процедур та показників acceptance rate підтвердив коректність і стабільність отриманих оцінок.

На основі апостеріорних розподілів параметрів виконано масштабне імітаційне моделювання агрегованих фінансових втрат, що дало змогу побудувати емпіричні розподіли річних збитків для окремих типів атак (фішингових та DDoS), а також їх сумарного впливу. Отримані результати показали істотні відмінності у структурі ризику різних типів загроз та підтвердили, що саме поведінка правого хвоста розподілу визначає величини CyVaR на рівнях довіри 95% і 99%. Проведений log–log аналіз верхніх хвостів продемонстрував важкохвосту природу агрегованого розподілу, що узгоджується з результатами попередніх досліджень у сфері фінансових та кіберризиків.

Окрему увагу в роботі приділено аналізу впливу заходів кіберзахисту на рівень ризику. Запропоновано формалізацію мітигаційних контролів у вигляді мультиплікативних коефіцієнтів, які впливають на параметри частоти та тяжкості атак. Реалізований what-if аналіз дозволив кількісно оцінити, як впровадження конкретних заходів інформаційної безпеки змінює розподіли фінансових втрат та значення CyVaR. Отримані результати показали, що навіть помірні за масштабом контролі можуть забезпечувати суттєве зниження екстремальних ризиків, що є критично важливим для фінансової стійкості установи.

Для оцінювання економічної доцільності впровадження заходів кіберзахисту використано показники ROSI та RaROSI. Показано, що традиційні метрики, засновані на середніх значеннях втрат, можуть давати хибні або нестабільні оцінки у випадку важкохвостих розподілів. Натомість ризик-орієнтовані показники RaROSI, які базуються на значеннях CyVaR, дозволяють

адекватно оцінити ефективність інвестицій у контексті екстремальних сценаріїв і можуть бути використані як інструмент підтримки прийняття управлінських рішень.

Практичним результатом роботи стала реалізація програмного веб-додатку, який інкапсулює розроблену математичну модель та забезпечує зручний інтерфейс для проведення розрахунків CyVaR, аналізу розподілів втрат і оцінювання впливу заходів кіберзахисту. Додаток дозволяє змінювати параметри моделі, виконувати what-if аналіз і візуалізувати результати у вигляді графіків та числових показників, що підвищує практичну цінність дослідження та робить модель придатною для використання у реальних умовах фінансових установ.

Загалом результати магістерської роботи підтверджують, що поєднання байєсівських методів оцінювання параметрів, імітаційного моделювання та концепції Cyber Value-at-Risk дозволяє побудувати гнучку, стійку та практично орієнтовану систему кількісного аналізу кіберризиків. Запропонований підхід може бути використаний для підвищення рівня кіберстійкості фінансових установ, обґрунтування інвестицій у кіберзахист та прийняття рішень у умовах високої невизначеності. Подальші дослідження можуть бути спрямовані на розширення моделі за рахунок урахування залежностей між інцидентами, інтеграції зовнішніх Threat Intelligence-даних та адаптації під регуляторні вимоги фінансового сектору.

Перелік джерел посилань

1. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII
2. Національний банк України. Постанова № 95 від 28.09.2017 "Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України"
3. Харламова, К., & Гальчинський, Л. (2022). Оцінювання кіберстійкості об’єктів критичної інфраструктури України. Collection of scientific papers «SCIENTIA», (November 11, 2022; Vilnius,Lithuania), 118-120.
4. IBM Security. Cost of a Data Breach Report 2024. — IBM Corp., 2024
5. Taleb N. N. The Black Swan: The Impact of the Highly Improbable. — New York : Random House – 2007.
6. Knight, Frank H., Risk, Uncertainty and Profit - 1921p
7. Dowd K. Measuring Market Risk. — Chichester : John Wiley & Sons, 2005.
8. Orlando A., et al. Modeling Cyber Risk Loss Distributions Using Extreme Value Theor. Risks. — 2019. — Vol. 7, No. 4. — AArticle 184.
9. Embrechts P., Klüppelberg C., Mikosch T. Modelling Extremal Events for Insurance and Finance. — Berlin : Springer, 1997. — 648 p.
10. Eling M., Wirfs J. Cyber Risk: Too Big to Insure? Risk Transfer Options for a Changing Landscape // Institute of Insurance Economics. — St. Gallen, 2016.
11. Заріцький О. В., & Гальчинський Л. Ю. «Оцінювання ймовірності фінансових втрат фінансової установи внаслідок кіберінцидентів на основі кількісних методів аналізу ризику» Collection of Scientific Papers «SCIENTIA», (December 5, 2025; Montreal, Canada) — 375-384.
12. World Economic Forum. Global Cybersecurity Outlook 2023. — Geneva : WEF, 2023.
13. Razavi H., et al. Quantifying the Financial Impact of Cyber Security Attacks on Banks: A Big Data Analytics Approach // IEEE Access. — 2023. — Vol. 11.
14. CSIRT-NBU, Звіт про кіберзагрози в банківському секторі України.

15. ISO/IEC 27005:2018. Information technology — Security techniques — Information security risk management.
16. Урсол, О., & Гальчинський, Л. (2022). ОЦІНЮВАННЯ РИЗИКУ КІБЕРЗАГРОЗ ПІДПРИЄМСТВА З МЕТОЮ ВИЗНАЧЕННЯ НЕОБХІДНИХ ВИТРАТ ДЛЯ ПЕВНОГО РІВНЯ КІБРЕЗБЕЗПЕКИ. Collection of Scientific Papers «SCIENTIA», (June 10, 2022; Sydney, Australia), 57–63
17. Robert C. P., Casella G. Monte Carlo Statistical Methods. — 2004.
18. Basel Committee on Banking Supervision. Basel III: Finalising post-crisis reforms. — BIS, 2017.
19. Christian Locher, Methodologies for Evaluating Information Security Investments - What Basel II Can Change in the Financial Industry, Association for Information Systems, AIS Electronic Library (AISeL), 2005.
20. NIST SP 800-30 Rev.1. Guide for Conducting Risk Assessments. — Gaithersburg : NIST, 2012.
21. Hubbard D. W., Seiersen R. How to Measure Anything in Cybersecurity Risk. — Hoboken : Wiley, 2016.
22. FAIR Institute. Factor Analysis of Information Risk (FAIR) Framework Documentation. — 2023.
23. Hong Kong Monetary Authority. Cyber Resilience Assessment Framework. — Hong Kong, 2016.
24. J.P. Morgan, RiskMetrics, Value At Risk – 1994
25. Jorion, Philippe., Value at Risk: The New Benchmark for Managing Financial Risk (3rd ed.). McGraw-Hill – 2006
26. Jorion P. Value at Risk: The New Benchmark for Managing Financial Risk. — New York : McGraw-Hill, 2007.
27. Beckström, Rod and Alyce Campbell, eds, 1995, “An Introduction to VAR”, Palo Alto, CA: CATS Software, Inc.

28. McNeil A. J., Frey R., Embrechts P. Quantitative Risk Management: Concepts, Techniques and Tools. — Princeton : Princeton University Press, 2015. — 538p.
29. Coles S. An Introduction to Statistical Modeling of Extreme Values. — London: Springer, 2001. — 208 p.
30. Ross S. M. Introduction to Probability Models. — Academic Press, 2019.
31. Glasserman P. Monte Carlo Methods in Financial Engineering. — ew York : Springer, 2004.
32. Hastings W. K. Monte Carlo Sampling Methods Using Markov Chains and Their Applications — 1970.
33. Metropolis N., Rosenbluth A. W., Rosenbluth M. N., Teller A. H., Teller E. Equation of State Calculations by Fast Computing Machines. — 1953.
34. Урсол, О. І. Оцінювання рівня загроз на рівні інвестицій в кібербезпеку для виробничої інфраструктури : магістерська дис. : 125 Кібербезпека / Урсол Олексій Ігорович. – Київ, 2022. – 85 с.
35. Заріцький, О. В. Оцінка рівня кібер-ризиків для об’єктів державного сектору України з метою подальшого планування інвестицій в інформаційну безпеку : дипломна робота бакалавра : 125 Кібербезпека / Заріцький Олександр Васильович. – Київ, 2024. – 78 с.
36. Lee, S., & Kim, J. H. T. (2019). Exponentiated generalized Pareto distribution: Properties and applications towards extreme value theory. Communications in Statistics - Theory and Methods, 48(8), 2014–2038. https://doi.org/10.1080/03610926.2018.1441418
37. NIST SP 800-53 Rev.5. Security and Privacy Controls for Information Systems and Organizations. — Gaithersburg : NIST, 2020.
38. Bodeau, D.J.; Graubart, R.D.; McQuaid, R.M.; Woodill, J. (2018). Cyber Resiliency Metrics, Measures of Effectiveness,and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods;Technical Report; Mitre Corp Bedford Ma Bedford United States: McLean, VA, USA.

39. Rainer Bohme, Security Metrics and Security Investment Models
40. Gordon L. A., Loeb M. P. The Economics of Information Security Investment // ACM Transactions on Information and System Security. — 2002. — Vol. 5, No. 4. — P. 438–457.
41. Мінімальні вимоги до капіталу під операційний ризик https://bank.gov.ua/admin_uploads/article/Operational_risk_2019-10_pr.pdf?v=7

Додаток А

Код веб-додатку

```
import numpy as np
from math import lgamma
import matplotlib.pyplot as plt
from matplotlib.ticker import FuncFormatter
from scipy.stats import linregress
from scipy.stats import genpareto
from pymcmcstat.MCMC import MCMC
import streamlit as st


# ============================================
# 1. Bayesian Core: Poisson + Lognormal
# ============================================

LOG_SQRT_2PI = 0.5 * np.log(2 * np.pi)


def log_posterior_calc(theta, n_attacks, losses):
    """
    Log-posterior for one attack type:
    - Poisson for annual attack counts
    - Lognormal for loss severities
    """
    loglam, mu, logsig = theta
    lam = np.exp(loglam)
    sig = np.exp(logsig)

    # Gaussian priors on parameters (weakly informative)
    lp = (
        -0.5 * (loglam / 1.5) ** 2
        - 0.5 * ((mu - 10.0) / 5.0) ** 2
        - 0.5 * (logsig / 1.0) ** 2
    )

    if lam <= 0 or sig <= 0:
        return -np.inf

    # Likelihood: Poisson for annual counts
    ll_pois = np.sum(
        n_attacks * loglam - lam - np.array([lgamma(k + 1) for k in
n_attacks])
    )

    # Likelihood: Lognormal for severities
    if len(losses) == 0:
        ll_logn = 0.0
    elif np.any(losses <= 0):
        return -np.inf
    else:
        logx = np.log(losses)
        ll_logn = -np.sum(
            (logx - mu) ** 2 / (2 * sig ** 2) + logsig + LOG_SQRT_2PI
        )
```

```
    return lp + ll_pois + ll_logn


def make_ssfun(n_attacks, losses):
    """
    Wrapper for pymcmcstat: returns -2 * log-posterior.
    """

    def ssfun(theta, data):
        lp = log_posterior_calc(theta, n_attacks, losses)
        return -2.0 * lp

    return ssfun


# ============================================
# 2. Auto-Converging DRAM MCMC (one attack type)
# ============================================


def run_auto_mcmc(
    n_attacks,
    losses,
    batch_size=5000,
    max_iter=200000,
    tol=0.01,
    label="",
):
    """
    Auto-converging DRAM MCMC for ONE attack type (Phishing / DDoS).

    Convergence logic:
      * run in batches;
      * after each batch, compare mean(theta) over all samples
        vs previous batch;
      * stop when relative max error < tol.
    """
    # Initial guesses
    current_theta0 = [0.0, 10.0, 0.0]
    current_qcov = np.diag([0.5, 2.0, 0.5])

    total_chain = None
    converged = False
    iteration_count = 0

    status_text = st.empty()
    metric_text = st.empty()
    progress_bar = st.progress(0)

    while iteration_count < max_iter:
        mc = MCMC(rngseed=None)
        mc.data.add_data_set(x=np.array([0]), y=np.array([0]))

        mc.parameters.add_model_parameter(
            name="loglam",
            theta0=current_theta0[0],
            minimum=-10,
            maximum=10,
```

```
        )
        mc.parameters.add_model_parameter(
            name="mu",
            theta0=current_theta0[1],
            minimum=0,
            maximum=25,
        )
        mc.parameters.add_model_parameter(
            name="logsig",
            theta0=current_theta0[2],
            minimum=-5,
            maximum=5,
        )

        mc.simulation_options.define_simulation_options(
            nsimu=batch_size,
            updatesigma=False,
            method="dram",
            qcov=current_qcov,
            adaptint=0,
            verbosity=0,
            waitbar=False,
        )

        mc.model_settings.define_model_settings(
            sos_function=make_ssfun(n_attacks, losses)
        )

        mc.run_simulation()

        batch_chain = mc.simulation_results.results["chain"]

        # Acceptance rate for this batch
        unique_moves = np.unique(batch_chain, axis=0).shape[0]
        batch_acc_rate = unique_moves / batch_size

        # Simple step-size controller
        if batch_acc_rate > 0.40:
            current_qcov = current_qcov * 1.5
            action = "Increasing step size "
        elif batch_acc_rate < 0.20:
            current_qcov = current_qcov * 0.8
            action = "Decreasing step size "
        else:
            action = "Step size optimal "

        metric_text.text(
            f"[{label}] Batch acceptance rate: {batch_acc_rate:.2%} |
{action}"
        )

        # Append batch to full chain
        if total_chain is None:
            total_chain = batch_chain
        else:
            total_chain = np.vstack((total_chain, batch_chain))

        iteration_count += batch_size
```

```
        progress_bar.progress(min(iteration_count / max_iter, 1.0))

        # Convergence check
        if iteration_count >= 2 * batch_size:
            mean_all = np.mean(total_chain, axis=0)
            mean_prev = np.mean(total_chain[:-batch_size], axis=0)

            rel_error = np.abs(
                (mean_all - mean_prev) / (mean_prev + 1e-9)
            )
            max_error = np.max(rel_error)

            status_text.text(
                f"[{label}] Iterations: {iteration_count}. "
                f"Error: {max_error:.6f} (Target: {tol:.10f})"
            )

            if max_error < tol:
                converged = True
                break
        else:
            status_text.text(
                f"[{label}] Iterations: {iteration_count}. Warmup..."
            )

        current_theta0 = batch_chain[-1]

    progress_bar.empty()
    metric_text.empty()

    if converged:
        st.success(
            f"[{label}] Converged automatically after {iteration_count}
iterations!"
        )
    else:
        st.warning(
            f"[{label}]   Stopped   by   iteration   limit   ({max_iter}
iterations)."
        )

    unique_steps = np.unique(total_chain, axis=0).shape[0]
    acc_rate = unique_steps / total_chain.shape[0]

    # Simple burn-in
    burnin = int(len(total_chain) * 0.2)
    final_chain = total_chain[burnin:]

    return {
        "lam_samples": np.exp(final_chain[:, 0]),
        "mu_samples": final_chain[:, 1],
        "sig_samples": np.exp(final_chain[:, 2]),
        "acc_rate": acc_rate,
        "iterations": iteration_count,
    }


# ============================================
```

```
# 3. Monte Carlo Simulation (with controls)
# ==========================================


def simulate_loss_distribution(
    mcmc_res,
    n_years=1,
    n_sims=None,
    rngseed=101,
    freq_factor=1.0,
    sev_factor=1.0,
):
    """
    Monte-Carlo simulation for ONE attack type.

    Parameters
    ----------
    mcmc_res : dict
        Output of run_auto_mcmc for a single attack type.
    n_years : float
        Time horizon in years.
    n_sims : int or None
        Number of simulated paths (if None – use all posterior samples).
    freq_factor : float
        Multiplicative factor applied to attack frequency (λ).
        Example: 0.7 means -30% frequency due to control.
    sev_factor : float
        Multiplicative factor applied to loss severity.
        Example: 0.6 means -40% loss amount due to control.
    """
    rng = np.random.default_rng(rngseed)
    lams = mcmc_res["lam_samples"]
    mus = mcmc_res["mu_samples"]
    sigs = mcmc_res["sig_samples"]

    freq_factor = max(freq_factor, 0.0)
    sev_factor = max(sev_factor, 0.0)

    n_total = len(lams)
    if n_sims is None or n_sims > n_total:
        n_sims = n_total

    idx = rng.choice(n_total, size=n_sims, replace=False)
    lams = lams[idx]
    mus = mus[idx]
    sigs = sigs[idx]

    annual_losses = np.zeros(n_sims)

    for i in range(n_sims):
        # Frequency affected by control
        n_events = rng.poisson(lams[i] * n_years * freq_factor)
        if n_events > 0:
            # Severity affected by control
            loss_events = rng.lognormal(mus[i], sigs[i], size=n_events) *
sev_factor
            annual_losses[i] = np.sum(loss_events)
```

```
    return annual_losses


# ============================================
# 4. Visualization & Stats Helpers
# ============================================

def plot_posteriors(res, title_prefix=""):
    """
    Plot posterior distributions for λ, μ, σ for one attack type.
    """
    st.subheader(f"Parameter Uncertainty - {title_prefix}")
    fig, axes = plt.subplots(1, 3, figsize=(10, 4))

    # Lambda
    axes[0].hist(
        res["lam_samples"],
        bins=200,
        density=True,
        color="#4C72B0",
        alpha=0.8,
    )
    axes[0].axvline(np.mean(res["lam_samples"]), color="k", linestyle="--
")
    axes[0].set_title("Frequency λ\n(Attacks/Year)")

    # Mu
    axes[1].hist(
        res["mu_samples"],
        bins=200,
        density=True,
        color="#DD8452",
        alpha=0.8,
    )
    axes[1].axvline(np.mean(res["mu_samples"]), color="k", linestyle="--
")
    axes[1].set_title("Severity μ\n(Log-Mean)")

    # Sigma
    axes[2].hist(
        res["sig_samples"],
        bins=200,
        density=True,
        color="#55A868",
        alpha=0.8,
    )
    axes[2].axvline(np.mean(res["sig_samples"]), color="k", linestyle="--
")
    axes[2].set_title("Severity σ\n(Volatility)")

    st.pyplot(fig)


def describe_losses(label, losses):
    """
    Compute expected loss and CyVaR metrics for a loss distribution.
    """
    var_95 = np.quantile(losses, 0.95)
```

```
    var_99 = np.quantile(losses, 0.99)
    expected_loss = np.mean(losses)

    return {
        "label": label,
        "E": expected_loss,
        "VaR95": var_95,
        "VaR99": var_99,
    }


# ============================================
# 5. Main Streamlit UI – Phishing & DDoS
# ============================================

st.set_page_config(layout="wide", page_title="CyVaR Auto – Two Attack
Types")
st.title("Advanced CyVaR Calculator (Phishing + DDoS, Auto-Converging)")

# Input: attack histories
col_f1, col_f2 = st.columns(2)

with col_f1:
    st.markdown("### Phishing (Email-borne attacks)")
    ph_n_input = st.text_area(
        "Phishing – Attack Frequency History (per year, comma-
separated)",
        "enter your attack frequency data here",
        height=100,
    )
    ph_l_input = st.text_area(
        "Phishing – Loss Severity History (UAH, per incident)",
        "enter your losses data for this type of attack here",
        height=170,
    )

with col_f2:
    st.markdown("### DDoS (Service Disruption)")
    dd_n_input = st.text_area(
        "DDoS – Attack Frequency History (per year, comma-separated)",
        "enter your attack frequency data here",
        height=100,
    )
    dd_l_input = st.text_area(
        "DDoS – Loss Severity History (UAH, per incident)",
        "enter your losses data for this type of attack here",
        height=170,
    )

# Advanced settings: convergence / horizon
with st.expander("Advanced Settings (Convergence)", expanded=True):
    tol_input_pct = st.slider(
        "Convergence Tolerance (Stop when error < X%)",
        min_value=0.0001,
        max_value=5.00,
        value=0.50,
        step=0.001,
        format="%.4f%%",
```

```
        help="Lower value = higher precision = more time. 0.5% is usually
enough.",
    )
    tol_input = tol_input_pct / 100.0

    max_iter_input = st.number_input(
        "Max Iterations Limit", value=10000000, step=1000000
    )

    horizon_years = st.number_input(
        "Simulation Horizon (years)",
        value=1.0,
        min_value=0.1,
        max_value=10.0,
        step=0.1,
    )

# Control / mitigation scenario inputs

with st.expander("Optional: Controls / Mitigations", expanded=False):
    st.markdown(
        "You can specify separate controls for Phishing and DDoS. "
        "Each control can independently reduce attack frequency and/or "
        "loss severity. All reductions are expressed in percent."
    )

    ph_ctrl_enabled   =   st.checkbox("Enable   control   for   Phishing",
value=False)
    dd_ctrl_enabled = st.checkbox("Enable control for DDoS", value=False)

    col_ctrl1, col_ctrl2 = st.columns(2)

    # Defaults (no control)
    ph_freq_reduction_pct = 0.0
    ph_sev_reduction_pct = 0.0
    ph_control_cost = 0.0

    dd_freq_reduction_pct = 0.0
    dd_sev_reduction_pct = 0.0
    dd_control_cost = 0.0

    with col_ctrl1:
        if ph_ctrl_enabled:
            st.markdown("**Phishing control parameters**")
            ph_freq_reduction_pct = st.number_input(
                "Phishing - frequency reduction (%)",
                min_value=0.0,
                max_value=100.0,
                value=30.0,
                step=1.0,
            )
            ph_sev_reduction_pct = st.number_input(
                "Phishing - severity reduction (%)",
                min_value=0.0,
                max_value=100.0,
                value=20.0,
                step=1.0,
            )
```

```
            ph_control_cost = st.number_input(
                "Annual cost of Phishing control (UAH)",
                min_value=0.0,
                value=200_000.0,
                step=10_000.0,
            )

    with col_ctrl2:
        if dd_ctrl_enabled:
            st.markdown("**DDoS control parameters**")
            dd_freq_reduction_pct = st.number_input(
                "DDoS - frequency reduction (%)",
                min_value=0.0,
                max_value=100.0,
                value=30.0,
                step=1.0,
            )
            dd_sev_reduction_pct = st.number_input(
                "DDoS - severity reduction (%)",
                min_value=0.0,
                max_value=100.0,
                value=20.0,
                step=1.0,
            )
            dd_control_cost = st.number_input(
                "Annual cost of DDoS control (UAH)",
                min_value=0.0,
                value=300_000.0,
                step=10_000.0,
            )

    total_control_cost = ph_control_cost + dd_control_cost


# ============================================
# 6. Run simulation
# ============================================

if st.button("Run Joint Simulation (Phishing + DDoS)"):
    try:
        # Parse inputs
        n_ph = np.fromstring(ph_n_input, sep=",")
        l_ph = np.fromstring(ph_l_input, sep=",")
        n_dd = np.fromstring(dd_n_input, sep=",")
        l_dd = np.fromstring(dd_l_input, sep=",")

        if len(n_ph) == 0 or len(l_ph) == 0:
            st.error("Provide both frequency and severity history for
Phishing.")
            st.stop()
        if len(n_dd) == 0 or len(l_dd) == 0:
            st.error("Provide both frequency and severity history for
DDoS.")
            st.stop()

        # Run MCMC per attack type
        st.markdown("## 1. MCMC Estimation per Attack Type")
```

```
mcmc_ph = run_auto_mcmc(
    n_attacks=n_ph,
    losses=l_ph,
    batch_size=5000,
    max_iter=max_iter_input,
    tol=tol_input,
    label="Phishing",
)

mcmc_dd = run_auto_mcmc(
    n_attacks=n_dd,
    losses=l_dd,
    batch_size=5000,
    max_iter=max_iter_input,
    tol=tol_input,
    label="DDoS",
)

st.write(
    f"**Phishing – total iterations:** {mcmc_ph['iterations']}, "
    f"acceptance rate: {mcmc_ph['acc_rate']:.2%}"
)
st.write(
    f"**DDoS – total iterations:** {mcmc_dd['iterations']}, "
    f"acceptance rate: {mcmc_dd['acc_rate']:.2%}"
)

# Posterior plots
col_p1, col_p2 = st.columns(2)
with col_p1:
    plot_posteriors(mcmc_ph, "Phishing")
with col_p2:
    plot_posteriors(mcmc_dd, "DDoS")

# Monte-Carlo per attack type + joint distribution
st.markdown("---")
st.subheader("2. Monte-Carlo Simulation of Annual Losses")

# Same number of paths for both attack types
n_sims_joint = min(
    len(mcmc_ph["lam_samples"]), len(mcmc_dd["lam_samples"])
)

# Baseline (no control) simulations
losses_ph = simulate_loss_distribution(
    mcmc_ph,
    n_years=horizon_years,
    n_sims=n_sims_joint,
    rngseed=101,
)
losses_dd = simulate_loss_distribution(
    mcmc_dd,
    n_years=horizon_years,
    n_sims=n_sims_joint,
    rngseed=202,
)

losses_total = losses_ph + losses_dd
```

```
        stats_ph = describe_losses("Phishing", losses_ph)
        stats_dd = describe_losses("DDoS", losses_dd)
        stats_total = describe_losses("Total (Phishing + DDoS)",
losses_total)

        st.markdown("### 2.1. Financial Risk Metrics")

        c1, c2, c3 = st.columns(3)

        c1.metric(
            "Phishing – Expected Annual Loss",
            f"{stats_ph['E']:,.0f} UAH",
        )
        c1.metric(
            "Phishing – CyVaR 95%",
            f"{stats_ph['VaR95']:,.0f} UAH",
        )
        c1.metric(
            "Phishing – CyVaR 99%",
            f"{stats_ph['VaR99']:,.0f} UAH",
        )

        c2.metric(
            "DDoS – Expected Annual Loss",
            f"{stats_dd['E']:,.0f} UAH",
        )
        c2.metric(
            "DDoS – CyVaR 95%",
            f"{stats_dd['VaR95']:,.0f} UAH",
        )
        c2.metric(
            "DDoS – CyVaR 99%",
            f"{stats_dd['VaR99']:,.0f} UAH",
        )

        c3.metric(
            "Total – Expected Annual Loss",
            f"{stats_total['E']:,.0f} UAH",
        )
        c3.metric(
            "Total – CyVaR 95%",
            f"{stats_total['VaR95']:,.0f} UAH",
        )
        c3.metric(
            "Total – CyVaR 99%",
            f"{stats_total['VaR99']:,.0f} UAH",
        )

        # 2.2. Aggregate loss distributions (4 plots)
        st.markdown("### 2.2. Aggregate Loss Distributions")

        # Common X-axis limit: show body + tail; ensure all VaR lines
fit.
        q_x = 0.992

        all_losses = np.concatenate([losses_ph, losses_dd, losses_total])
        limit_x = np.quantile(all_losses, q_x)
```

```
# keep VaR99 visible with small margin
limit_x = max(
    limit_x,
    stats_ph["VaR99"] * 1.05,
    stats_dd["VaR99"] * 1.05,
    stats_total["VaR99"] * 1.05,
)

# Row 1: Phishing vs DDoS (linear + log)
row1_col1, row1_col2 = st.columns(2)

# 1A) Linear scale
with row1_col1:
    fig_pd_lin, ax_pd_lin = plt.subplots(figsize=(10, 4))

    ax_pd_lin.hist(
        losses_ph[losses_ph <= limit_x],
        bins=500,
        alpha=0.6,
        label="Phishing",
    )
    ax_pd_lin.hist(
        losses_dd[losses_dd <= limit_x],
        bins=500,
        alpha=0.6,
        label="DDoS",
    )

    hist_ph, _ = np.histogram(
        losses_ph[losses_ph <= limit_x],
        bins=500,
    )
    hist_dd, _ = np.histogram(
        losses_dd[losses_dd <= limit_x],
        bins=500,
    )

    ymax = np.quantile(
        np.concatenate([hist_ph, hist_dd]),
        0.995   # 99.5%
    )
    ax_pd_lin.set_ylim(0, ymax)


    # Phishing VaR lines
    ax_pd_lin.axvline(
        stats_ph["VaR95"],
        color="tab:blue",
        linestyle="--",
        label=f"Phishing VaR 95%: {stats_ph['VaR95']:,.0f}",
    )
    ax_pd_lin.axvline(
        stats_ph["VaR99"],
        color="tab:blue",
        linestyle=":",
        label=f"Phishing VaR 99%: {stats_ph['VaR99']:,.0f}",
    )
```

```
            # DDoS VaR lines
            ax_pd_lin.axvline(
                stats_dd["VaR95"],
                color="tab:orange",
                linestyle="--",
                label=f"DDoS VaR 95%: {stats_dd['VaR95']:,.0f}",
            )
            ax_pd_lin.axvline(
                stats_dd["VaR99"],
                color="tab:orange",
                linestyle=":",
                label=f"DDoS VaR 99%: {stats_dd['VaR99']:,.0f}",
            )

            ax_pd_lin.set_title("Phishing vs DDoS – Linear Scale")
            ax_pd_lin.set_xlabel("Annual loss (UAH)")
            ax_pd_lin.set_ylabel("Frequency")
            ax_pd_lin.set_xlim(0, limit_x)
            ax_pd_lin.xaxis.set_major_formatter(
                FuncFormatter(lambda x, p: f"{x:,.0f}".replace(",", " "))
            )
            ax_pd_lin.legend()
            ax_pd_lin.grid(alpha=0.3)
            st.pyplot(fig_pd_lin)

        # 2A) Log-log scale (Phishing vs DDoS)
        with row1_col2:
            fig_pd_log, ax_pd_log = plt.subplots(figsize=(10, 4))

            bins_scatter = 300

            # Remove zero / negative values explicitly (required for log-
log)
            ph_vals = losses_ph[(losses_ph > 0) & (losses_ph <= limit_x)]
            dd_vals = losses_dd[(losses_dd > 0) & (losses_dd <= limit_x)]

            # Use common bin edges
            combined = np.concatenate([ph_vals, dd_vals])
            edges = np.histogram_bin_edges(combined, bins=bins_scatter)

            ph_hist, _ = np.histogram(ph_vals, bins=edges)
            dd_hist, _ = np.histogram(dd_vals, bins=edges)

            x_centers = 0.5 * (edges[:-1] + edges[1:])

            # Masks: log-log cannot show zeros
            ph_mask = (ph_hist > 0) & (x_centers > 0)
            dd_mask = (dd_hist > 0) & (x_centers > 0)

            # Scatter
            ax_pd_log.scatter(
                x_centers[ph_mask], ph_hist[ph_mask],
                s=8, alpha=0.70, label="Phishing"
            )
            ax_pd_log.scatter(
                x_centers[dd_mask], dd_hist[dd_mask],
                s=8, alpha=0.55, label="DDoS"
```

```
            )

            # Tail approximation (log-log linear fit)
            from scipy.stats import linregress

            tail_q = 0.95  # start tail from VaR95

            # Phishing tail
            x_thr_ph = np.quantile(ph_vals, tail_q)
            tail_mask_ph = (x_centers >= x_thr_ph) & ph_mask

            log_x_ph = np.log(x_centers[tail_mask_ph])
            log_y_ph = np.log(ph_hist[tail_mask_ph])

            slope_ph, intercept_ph, _, _, _ = linregress(log_x_ph,
log_y_ph)

            x_fit_ph = np.linspace(
                x_centers[tail_mask_ph].min(),
                x_centers[tail_mask_ph].max(),
                100
            )
            y_fit_ph = np.exp(intercept_ph) * x_fit_ph ** slope_ph

            ax_pd_log.plot(
                x_fit_ph, y_fit_ph,
                color="#1434A4",
                linewidth=2,
                label=f"Phishing tail slope = {slope_ph:.2f}"
            )

            # DDoS tail
            x_thr_dd = np.quantile(dd_vals, tail_q)
            tail_mask_dd = (x_centers >= x_thr_dd) & dd_mask

            log_x_dd = np.log(x_centers[tail_mask_dd])
            log_y_dd = np.log(dd_hist[tail_mask_dd])

            slope_dd, intercept_dd, _, _, _ = linregress(log_x_dd,
log_y_dd)

            x_fit_dd = np.linspace(
                x_centers[tail_mask_dd].min(),
                x_centers[tail_mask_dd].max(),
                100
            )
            y_fit_dd = np.exp(intercept_dd) * x_fit_dd ** slope_dd

            ax_pd_log.plot(
                x_fit_dd, y_fit_dd,
                color="#EC5800",
                linewidth=2,
                label=f"DDoS tail slope = {slope_dd:.2f}"
            )

            # Axes: log-log
            ax_pd_log.set_xscale("log")
            ax_pd_log.set_yscale("log")
```

```
            ax_pd_log.set_title("Phishing   vs   DDoS   -   Log-log   Tail
Analysis")
            ax_pd_log.set_xlabel("Annual loss (UAH, log scale)")
            ax_pd_log.set_ylabel("Frequency (log scale)")

            ax_pd_log.grid(alpha=0.3, which="both")
            ax_pd_log.legend()
            st.pyplot(fig_pd_log)


        # Row 2: Total (linear + log)
        row2_col1, row2_col2= st.columns(2)

        # 1B) Linear scale
        with row2_col1:
            fig_tot_lin, ax_tot_lin = plt.subplots(figsize=(10, 4))

            ax_tot_lin.hist(
                losses_total[losses_total <= limit_x],
                bins=500,
                alpha=0.7,
                label="Total loss",
            )

            ax_tot_lin.axvline(
                stats_total["VaR95"],
                color="red",
                linestyle="--",
                label=f"Total VaR 95%: {stats_total['VaR95']:,.0f}",
            )
            ax_tot_lin.axvline(
                stats_total["VaR99"],
                color="orange",
                linestyle="--",
                label=f"Total VaR 99%: {stats_total['VaR99']:,.0f}",
            )

            ax_tot_lin.set_title("Total Annual Loss - Linear Scale")
            ax_tot_lin.set_xlabel("Annual loss (UAH)")
            ax_tot_lin.set_ylabel("Frequency")
            ax_tot_lin.set_xlim(0, limit_x)
            ax_tot_lin.xaxis.set_major_formatter(
                FuncFormatter(lambda x, p: f"{x:,.0f}".replace(",", " "))
            )
            ax_tot_lin.legend()
            ax_tot_lin.grid(alpha=0.3)
            st.pyplot(fig_tot_lin)

        # 2B) Logarithmic Y scale
        with row2_col2:
            fig_tot_log, ax_tot_log = plt.subplots(figsize=(10, 4))

            bins_scatter = 300

            tot_vals = losses_total[losses_total <= limit_x]

            hist_tot, edges = np.histogram(tot_vals, bins=bins_scatter)
```

```
x_centers = 0.5 * (edges[:-1] + edges[1:])

# log-log cannot show zeros
mask = hist_tot > 0

ax_tot_log.scatter(
    x_centers[mask],
    hist_tot[mask],
    s=10,
    alpha=0.7,
    label="Total loss",
    color="tab:purple"
)

# Tail approximation (log-log linear fit)
from scipy.stats import linregress

tail_q = 0.95  # start tail from VaR95

x_thr = np.quantile(tot_vals, tail_q)
tail_mask = (x_centers >= x_thr) & mask

log_x = np.log(x_centers[tail_mask])
log_y = np.log(hist_tot[tail_mask])

slope, intercept, _, _, _ = linregress(log_x, log_y)

x_fit = np.linspace(
    x_centers[tail_mask].min(),
    x_centers[tail_mask].max(),
    100
)
y_fit = np.exp(intercept) * x_fit ** slope

ax_tot_log.plot(
    x_fit,
    y_fit,
    linewidth=2,
    color="#5D3FD3",
    label=f"Tail fit (slope = {slope:.2f})"
)

# VaR lines (visual clamp only)
def clamp_v(v, vmax):
    return min(v, vmax)

ax_tot_log.axvline(
    clamp_v(stats_total["VaR95"], limit_x),
    color="red",
    linestyle="--",
    label=f"Total VaR 95%: {stats_total['VaR95']:,.0f}",
)
ax_tot_log.axvline(
    clamp_v(stats_total["VaR99"], limit_x),
    color="orange",
    linestyle=":",
    label=f"Total VaR 99%: {stats_total['VaR99']:,.0f}",
)
```

```
            ax_tot_log.set_title("Total Annual Loss - Log-log Tail
Analysis")
            ax_tot_log.set_xlabel("Annual loss (UAH, log scale)")
            ax_tot_log.set_ylabel("Frequency (log scale)")
            ax_tot_log.set_xscale("log")
            ax_tot_log.set_yscale("log")

            # IMPORTANT: log-x can't include 0
            x_min = max(np.min(tot_vals[tot_vals > 0]), 1.0)   # safe
floor (1 UAH)
            ax_tot_log.set_xlim(x_min, limit_x)

            from matplotlib.ticker import LogLocator,
LogFormatterSciNotation
            ax_tot_log.xaxis.set_major_locator(LogLocator(base=10,
numticks=6))

ax_tot_log.xaxis.set_major_formatter(LogFormatterSciNotation())

            ax_tot_log.grid(alpha=0.3, which="both")
            ax_tot_log.legend()
            st.pyplot(fig_tot_log)


        # ============================================
        # 3. Control / mitigation impact (what-if)
        # ============================================

        has_control_effect = any(
            [
                ph_ctrl_enabled,
                dd_ctrl_enabled,
                total_control_cost > 0.0,
            ]
        )

        if has_control_effect:
            st.markdown("---")
            st.subheader("3. Control / Mitigation Impact (What-if
Scenario)")

            # Convert percentage reductions into multiplicative factors
            ph_freq_factor = (
                max(0.0, 1.0 - ph_freq_reduction_pct / 100.0)
                if ph_ctrl_enabled
                else 1.0
            )
            ph_sev_factor = (
                max(0.0, 1.0 - ph_sev_reduction_pct / 100.0)
                if ph_ctrl_enabled
                else 1.0
            )
            dd_freq_factor = (
                max(0.0, 1.0 - dd_freq_reduction_pct / 100.0)
                if dd_ctrl_enabled
                else 1.0
            )
```

```
            dd_sev_factor = (
                max(0.0, 1.0 - dd_sev_reduction_pct / 100.0)
                if dd_ctrl_enabled
                else 1.0
            )

            st.markdown(
                f"-      **Phishing      control**:      frequency      ×
{ph_freq_factor:.2f}, "
                f"severity × {ph_sev_factor:.2f}  \n"
                f"- **DDoS control**: frequency × {dd_freq_factor:.2f}, "
                f"severity × {dd_sev_factor:.2f}"
            )

            # Re-simulate losses under the control scenario
            losses_ph_ctrl = simulate_loss_distribution(
                mcmc_ph,
                n_years=horizon_years,
                n_sims=n_sims_joint,
                rngseed=501,
                freq_factor=ph_freq_factor,
                sev_factor=ph_sev_factor,
            )
            losses_dd_ctrl = simulate_loss_distribution(
                mcmc_dd,
                n_years=horizon_years,
                n_sims=n_sims_joint,
                rngseed=502,
                freq_factor=dd_freq_factor,
                sev_factor=dd_sev_factor,
            )
            losses_total_ctrl = losses_ph_ctrl + losses_dd_ctrl

            stats_ph_ctrl  =  describe_losses("Phishing  (with  control)",
losses_ph_ctrl)
            stats_dd_ctrl   =   describe_losses("DDoS   (with   control)",
losses_dd_ctrl)
            stats_total_ctrl = describe_losses(
                "Total (with control)", losses_total_ctrl
            )

            # New CyVaR metrics after control
            st.markdown("### 3.1. Financial Risk Metrics with Control")

            c1_ctrl, c2_ctrl, c3_ctrl = st.columns(3)

            c1_ctrl.metric(
                "Phishing – Expected Annual Loss (with control)",
                f"{stats_ph_ctrl['E']:,.0f} UAH",
            )
            c1_ctrl.metric(
                "Phishing – CyVaR 95% (with control)",
                f"{stats_ph_ctrl['VaR95']:,.0f} UAH",
            )
            c1_ctrl.metric(
                "Phishing – CyVaR 99% (with control)",
                f"{stats_ph_ctrl['VaR99']:,.0f} UAH",
            )
```

```
            c2_ctrl.metric(
                "DDoS – Expected Annual Loss (with control)",
                f"{stats_dd_ctrl['E']:,.0f} UAH",
            )
            c2_ctrl.metric(
                "DDoS – CyVaR 95% (with control)",
                f"{stats_dd_ctrl['VaR95']:,.0f} UAH",
            )
            c2_ctrl.metric(
                "DDoS – CyVaR 99% (with control)",
                f"{stats_dd_ctrl['VaR99']:,.0f} UAH",
            )

            c3_ctrl.metric(
                "Total – Expected Annual Loss (with control)",
                f"{stats_total_ctrl['E']:,.0f} UAH",
            )
            c3_ctrl.metric(
                "Total – CyVaR 95% (with control)",
                f"{stats_total_ctrl['VaR95']:,.0f} UAH",
            )
            c3_ctrl.metric(
                "Total – CyVaR 99% (with control)",
                f"{stats_total_ctrl['VaR99']:,.0f} UAH",
            )

            # Risk reduction and ROSI / RaROSI

            st.markdown("### 3.2. Risk Reduction and Economic
Efficiency")

            # Baseline values (without control)
            E_before = stats_total["E"]
            VaR95_before = stats_total["VaR95"]
            VaR99_before = stats_total["VaR99"]

            # After control
            E_after = stats_total_ctrl["E"]
            VaR95_after = stats_total_ctrl["VaR95"]
            VaR99_after = stats_total_ctrl["VaR99"]

            # Absolute risk reduction
            dE = E_before - E_after
            dVaR95 = VaR95_before - VaR95_after
            dVaR99 = VaR99_before - VaR99_after

            # Relative reduction in %
            dE_pct = dE / E_before * 100 if E_before > 0 else 0.0
            dVaR95_pct = dVaR95 / VaR95_before * 100 if VaR95_before > 0
else 0.0
            dVaR99_pct = dVaR99 / VaR99_before * 100 if VaR99_before > 0
else 0.0

            # Classic ROSI and risk-adjusted ROSI (RaROSI)
            if total_control_cost > 0:
                rosi_ale = (dE - total_control_cost) / total_control_cost
```

```
                raro_95    =    (dVaR95    -    total_control_cost)    /
total_control_cost
                raro_99    =    (dVaR99    -    total_control_cost)    /
total_control_cost
            else:
                rosi_ale = np.nan
                raro_95 = np.nan
                raro_99 = np.nan

            col_rr1, col_rr2 = st.columns(2)

            with col_rr1:
                st.markdown("**Risk reduction (absolute / relative):**")
                st.write(
                    f"- ΔE[Loss]: {dE:,.0f} UAH ({dE_pct:.1f}%)  \n"
                    f"- ΔCyVaR 95%: {dVaR95:,.0f} UAH ({dVaR95_pct:.1f}%)
\n"
                    f"-      ΔCyVaR      99%:      {dVaR99:,.0f}      UAH
({dVaR99_pct:.1f}%)"
                )

            with col_rr2:
                st.markdown("**Economic efficiency of the control(s):**")
                if total_control_cost > 0:
                    st.write(
                        f"-      Total      annual      control      cost:
{total_control_cost:,.0f} UAH  \n"
                        f"- ROSI (ALE-based): {rosi_ale:.2f}  \n"
                        f"- RaROSI 95%: {raro_95:.2f}  \n"
                        f"- RaROSI 99%: {raro_99:.2f}"
                    )
                else:
                    st.info(
                        "Control cost is set to 0 – ROSI / RaROSI metrics
are not "
                        "defined. Please specify a non-zero annual cost
to evaluate "
                        "investment efficiency."
                    )

            # Visual comparison of total loss distribution
            st.markdown("### 3.3. Total Loss Distribution: Before vs
After Control")

            fig_ctrl, ax_ctrl = plt.subplots(figsize=(10, 4))

            limit_x_ctrl = np.quantile(
                np.concatenate([losses_total, losses_total_ctrl]), 0.995
            )

            ax_ctrl.hist(
                losses_total[losses_total <= limit_x_ctrl],
                bins=500,
                alpha=0.6,
                label="Total (before control)",
            )
            ax_ctrl.hist(
                losses_total_ctrl[losses_total_ctrl <= limit_x_ctrl],
```

```
                bins=500,
                alpha=0.6,
                label="Total (with control)",
            )

            ax_ctrl.axvline(
                VaR95_before,
                color="red",
                linestyle="--",
                label=f"VaR 95% before: {VaR95_before:,.0f}",
            )
            ax_ctrl.axvline(
                VaR95_after,
                color="red",
                linestyle=":",
                label=f"VaR 95% after: {VaR95_after:,.0f}",
            )

            ax_ctrl.axvline(
                VaR99_before,
                color="orange",
                linestyle="--",
                label=f"VaR 99% before: {VaR99_before:,.0f}",
            )
            ax_ctrl.axvline(
                VaR99_after,
                color="orange",
                linestyle=":",
                label=f"VaR 99% after: {VaR99_after:,.0f}",
            )

            ax_ctrl.set_title("Total Annual Loss - Before vs After
Control")
            ax_ctrl.set_xlabel("Annual loss (UAH)")
            ax_ctrl.set_ylabel("Frequency")
            ax_ctrl.set_xlim(0, limit_x_ctrl)
            ax_ctrl.xaxis.set_major_formatter(
                FuncFormatter(lambda x, p: f"{x:,.0f}".replace(",", " "))
            )
            ax_ctrl.legend()
            ax_ctrl.grid(alpha=0.3)
            st.pyplot(fig_ctrl)

    except Exception as e:
        st.error(f"Calculation Error: {e}")
```