

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

Навчально-науковий інститут «Інститут інформаційних технологій в економіці»

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМНИЙ АНАЛІЗ»

Галузь знань 12 «Інформаційні технології»

Спеціальність 124 «Системний аналіз»

Форма навчання: очна(денна)
очна (денна), заочна, дистанційна

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему «Оцінювання рівня економічної безпеки підприємства у кіберпросторі»

здобувача Кобякова Іллі Петровича

(підпис)

Науковий керівник: к.е.н, доц. Потапенко С. Д.

(підпис)

Робота допущена до захисту перед екзаменаційною комісією

з атестації здобувачів вищої освіти (ЕК)

Завідувач кафедри: д.ф.-м.н., проф. Джалладова І.А.

(підпис)

Київ 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ІМЕНІ ВАДИМА ГЕТЬМАНА

Навчально-науковий інститут «Інститут інформаційних технологій в економіці»

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМНИЙ АНАЛІЗ»

СПЕЦІАЛЬНІСТЬ 124 «СИСТЕМНИЙ АНАЛІЗ»

ПОГОДЖЕНО

ЗАТВЕРДЖУЮ

Керівник проєктної групи (гарант)
освітньо-професійної програми

Завідувач кафедри системного
аналізу та кібербезпеки

(підпис) Галіцин В.К.

(підпис) Джалладова І.А.

_____ 20__ р.

_____ 20__ р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувачу вищої освіти Кобякову Іллі Петровичу

денної форми навчання

на підготовку кваліфікаційної бакалаврської роботи

на тему «Оцінювання рівня економічної безпеки підприємства у кіберпросторі»

Тему затверджено наказом ректора Університету від «_____» _____ 20__ р. № _____

Кваліфікаційна бакалаврська робота виконується на матеріалах ТОВ «ХВР РІВНЕ»

План кваліфікаційної бакалаврської роботи

Розділ 1. Теоретико-методичні основи оцінювання економічної безпеки підприємства у кіберпросторі

Розділ 2. Оцінювання економічної безпеки підприємств в умовах цифрової трансформації

Розділ 3. Стратегії та моделі забезпечення економічної безпеки в кіберпросторі

Об'єкт дослідження: процес забезпечення економічної безпеки підприємства в умовах цифрової трансформації та кіберпростору.

Предмет дослідження: методи та підходи до оцінювання рівня економічної безпеки підприємства в умовах цифрової трансформації та кіберзагроз, а також розробка практичних рекомендацій для підвищення цього рівня.

Мета кваліфікаційної бакалаврської роботи: впровадження методики оцінювання рівня економічної безпеки підприємства у кіберпросторі в умовах цифрової трансформації, а також розробка рекомендацій щодо підвищення цього рівня.

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

У розділі 1. Дослідити сучасний стан наукової думки щодо економічної безпеки підприємства. Виконати огляд сучасних теоретичних підходів до визначення та оцінки економічної безпеки підприємств. Визначити можливості інтеграції засобів кібербезпеки в загальну систему економічної безпеки підприємства.

У розділі 2. Провести аналіз поточного стану економічної безпеки підприємств в кіберпросторі на основі переддипломної практики. Виконати ідентифікацію основних кіберзагроз для економічної безпеки підприємств. Здійснити оцінювання ефективності заходів безпеки підприємств у кіберпросторі.

У розділі 3. Сформулювати рекомендації щодо підвищення рівня економічної безпеки підприємств у кіберпросторі. Виконати огляд можливостей економіко-математичного моделювання та прогнозування рівня економічної безпеки підприємства. Сформулювати пропозиції щодо впровадження інтеграційної методики оцінювання економічної безпеки підприємства у кіберпросторі.

Завдання підготував

науковий керівник

(підпис)

С. Д. Потапенко

«____» _____ 20__ р.

Завдання одержав

здобувач

(підпис)

І. П. Кобяков

«____» _____ 20__ р.

Реферат

Кваліфікаційна бакалаврська робота на тему «Оцінювання рівня економічної безпеки підприємства у кіберпросторі» складається з 51 сторінок, включаючи 3 розділи, 1 ілюстрацію, 8 таблиць та 28 джерел згідно із списком використаних джерел.

«Оцінювання рівня економічної безпеки підприємства в кіберпросторі»

Об'єкт дослідження

Об'єктом дослідження є процес забезпечення економічної безпеки підприємства в умовах цифрової трансформації та кіберпростору.

Предмет дослідження

Предметом дослідження є методи та підходи до оцінювання рівня економічної безпеки підприємства в умовах цифрової трансформації та кіберзагроз, а також розробка практичних рекомендацій для підвищення цього рівня.

Мета та завдання

Метою роботи є огляд та аналіз впровадження методики оцінювання рівня економічної безпеки підприємства у кіберпросторі в умовах цифрової трансформації, а також розробка рекомендацій щодо підвищення цього рівня. Для досягнення цієї мети було поставлено наступні завдання:

- Здійснити комплексний аналіз сучасних методів оцінювання економічної безпеки.
- Ідентифікувати основні кіберзагрози, що впливають на економічну безпеку підприємства.
- Спрогнозувати результати методів з урахуванням нових цифрових ризиків та можливостей.

Методи дослідження

У процесі дослідження були використані логічний аналіз, індукція та дедукція, формалізація та узагальнення, математичне моделювання, теоретичне обґрунтування, методи експертних оцінок.

Результати дослідження

Результати проведених аналітичних і розрахункових процедур мають значення для досліджуваної бази практики. Це включає конкретні рекомендації для підвищення рівня економічної безпеки підприємств в умовах цифрової трансформації, що можуть бути впроваджені в практику. Отримані результати можуть бути використані для конкретних підприємств, галузей або економіки в цілому, що дозволить ефективно протидіяти кіберзагрозам, підвищити стабільність та конкурентоспроможність підприємств, забезпечити їх фінансову стійкість та захист активів.

Рік виконання кваліфікаційної магістерської роботи 2024.

Рік захисту роботи 2024.

Ключові слова

Економічна безпека, кіберзагрози, цифрова трансформація, методи оцінювання, підприємства, захист даних, фінансова стабільність.

Цей реферат надає короткий огляд кваліфікаційної бакалаврської роботи, яка присвячена актуальним питанням економічної безпеки підприємств у кіберпросторі, описуючи основні методи, результати та рекомендації для покращення захисту підприємств в умовах сучасних викликів цифровізації.

Відгук

про кваліфікаційну бакалаврську роботу здобувача навчально-наукового інституту «Інститут інформаційних технологій в економіці» освітньо-професійної програми «Системний аналіз»

Кобякова Іллі Петровича

на тему «Оцінювання рівня економічної безпеки підприємства у кіберпросторі»

1. Актуальність теми кваліфікаційної бакалаврської роботи полягає у тому, що у зв'язку з посиленням кіберзагроз на національному рівні, українські підприємства стикаються з необхідністю вдосконалення своїх систем безпеки та впровадження нових методів захисту. З огляду на це, вміння користуватися методами оцінювання рівня економічної безпеки підприємств у кіберпросторі є не лише актуальною, але й необхідною умовою для стабільного розвитку економіки країни в цілому.
2. Позитивні риси кваліфікаційної роботи полягають у тому, що здобувач ґрунтовно дослідив сучасний стан наукової думки щодо економічної безпеки підприємства, висвітлив особливості теоретичних підходів до вивчення та оцінки економічної безпеки, детально описано практичні аспекти інтеграції кібербезпеки в загальну систему економічної безпеки підприємства.
3. Наявність самостійних розробок автора полягають в аналізі поточного стану економічної безпеки підприємств в кіберпросторі на основі виконаних завдань переддипломної практики, ідентифікації основних кіберзагроз для економічної безпеки підприємств, яке було досліджено, в самостійно виконаному оцінюванні ефективності загроз економічної безпеки, які існують для підприємства.
4. Цінність теоретичних висновків та практичних рекомендацій полягають у наданні підприємству рекомендацій щодо прийняття ефективних управлінських рішень стосовно обрання стратегії та побудови моделі ефективності організації економічної безпеки діяльності підприємства у кіберпросторі.
5. Наявність недоліків: Подана до захисту робота містила ряд недоліків редакційного характеру, які були усунуті та не мали негативного впливу на зміст виконаної роботи.
6. Загальна оцінка кваліфікаційної бакалаврської роботи та її допущення до захисту перед ЕК. Теоретичні та практичні матеріали, що викладені у роботі, відповідають вимогам до робіт такого рівня, робота заслуговує на високу оцінку а її автор заслуговує на присвоєння освітньо-кваліфікаційного рівня бакалавр з освітньо-професійної програми «Системний аналіз». Робота може бути допущеною до захисту перед екзаменаційною комісією.

Науковий керівник: доцент кафедри системного аналізу та кібербезпеки КНЕУ ім В. Гетьмана

Потапенко С. Д

Рецензія

на кваліфікаційну бакалаврську роботу здобувача вищої освіти

Кобякова Іллі Петровича

Тема: «Оцінювання рівня економічної безпеки підприємства в кіберпросторі»

Тема оцінювання рівня економічної безпеки підприємства у кіберпросторі є надзвичайно актуальною в умовах зростаючої кіберзагрози. У сучасному світі цифрових технологій захист економічних інтересів підприємства від кібератак стає важливим аспектом стабільного функціонування бізнесу. Ця робота вирішує ключові питання безпеки пов'язані з ефективністю заходів захисту в умовах цифрової трансформації.

Якість проведеного дослідження висока. Автор продемонстрував глибоке розуміння теми, використовуючи сучасні методи аналізу, такі як метод експертних оцінок для визначення рівня економічної безпеки. Дослідження базувалося на реальних даних та експертних оцінках, що забезпечило надійність результатів.

Однією з позитивних рис роботи є детальне розкриття теми та використання сучасних методів аналізу. Автор акцентував увагу на важливості інтеграції кібербезпеки в загальну систему економічної безпеки підприємства, що підкреслює актуальність і соціальну значущість дослідження. Використання реальних оцінок експертів для підвищення рівня безпеки підприємств також є сильною стороною роботи.

Хоча робота виконана на високому рівні, є декілька аспектів, які могли б бути вдосконалені. Наприклад, більш детальний опис методології збору експертних оцінок та критеріїв вибору експертів міг би надати дослідженню додаткової глибини. Було б корисно також розглянути додаткові аспекти кібербезпеки та їх вплив на економічну безпеку підприємств, щоб підсилити аналіз.

Практична значимість висновків і рекомендацій є дуже високою. Запропоновані рекомендації щодо регулярних аудитів безпеки, моніторингу кіберзагроз та інтеграції кібербезпеки можуть значно підвищити рівень економічної безпеки підприємств. Використання інноваційних технологій дозволить підприємствам краще захистити свої активи та адаптувати стратегії до ринкових змін, забезпечуючи конкурентну перевагу.

Місце роботи та посада рецензента



(підпис, ПІБ)

Місце печатки організації, де працює рецензент

ЗМІСТ

ВСТУП	3
РОЗДІЛ 1 ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ ОЦІНЮВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА У КІБЕРПРОСТОРІ.....	6
1.1 Сучасний стан наукової думки щодо економічної безпеки підприємства. 6	
1.2 Теоретичні підходи до визначення та оцінки економічної безпеки....	9
РОЗДІЛ 2 ОЦІНЮВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ.....	20
2.1 Аналіз поточного стану економічної безпеки підприємств в кіберпросторі на основі переддипломної практики.....	20
2.2 Ідентифікація основних кіберзагроз для економічної безпеки підприємств	24
2.3 Оцінка ефективності існуючих заходів безпеки.	33
РОЗДІЛ 3 СТРАТЕГІЇ ТА МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ В КІБЕРПРОСТОРІ	38
3.1 Рекомендацій щодо підвищення рівня економічної безпеки підприємств у кіберпросторі	38
3.2 Огляд можливостей економіко-математичного моделювання та прогнозування рівня економічної безпеки підприємства	42
ВИСНОВКИ	48
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	50

ВСТУП

Актуальність теми. У сучасному світі стрімкий розвиток інформаційних технологій призводить до значного зростання кіберзагроз, що ставить під загрозу економічну безпеку підприємств. Кіберзлочинність стає все більш витонченою, що вимагає від компаній значних зусиль для захисту своїх даних і фінансових ресурсів. Економічні втрати від кіберзлочинів можуть досягати мільярдів доларів, що робить питання кібербезпеки вкрай актуальним для підприємств будь-якого розміру та галузі. Враховуючи важливість кібербезпеки для збереження фінансової стабільності та репутації компаній, оцінювання рівня економічної безпеки підприємства у кіберпросторі є надзвичайно актуальним.

Особливо це стосується України, де розвиток цифровізації потребує ефективних механізмів захисту від кіберзагроз. У зв'язку з посиленням кіберзагроз на національному рівні, українські підприємства стикаються з необхідністю вдосконалення своїх систем безпеки та впровадження нових методів захисту. З огляду на це, вміння користуватися методами оцінювання рівня економічної безпеки підприємств у кіберпросторі є не лише актуальною, але й необхідною умовою для стабільного розвитку економіки країни в цілому.

Аналіз останніх досліджень і публікацій. У сучасній економічній літературі приділяється значна увага питанням економічної безпеки підприємств в умовах цифрової трансформації та розробці методик оцінки її рівня.

Стаття Самойленко Ю., Брітченко І., Левченко І. та ін. (2022) акцентує увагу на зміні пріоритетів економічної безпеки з матеріальних активів на цифрові. Автори пропонують впровадження поняття "цифрова безпека підприємства", що відображає нові економічні реалії та необхідність модернізації підходів до забезпечення економічної безпеки в умовах цифровізації [1].

Жанна Шило (2022) у своїй статті проводить детальний аналіз існуючих підходів до оцінки рівня економічної безпеки підприємства. Вона наголошує на важливості своєчасної оцінки економічної безпеки для забезпечення стабільної діяльності компанії. Шило пропонує методичний підхід, що базується на узагальненні декількох різних підходів та складається з послідовних етапів оцінки [2].

Обидві статті вказують на важливість комплексного підходу до оцінки економічної безпеки підприємства в умовах сучасних викликів. Вони підкреслюють, що цифрова трансформація бізнесу вимагає нових підходів до забезпечення економічної безпеки, що враховують новітні ризики та можливості, пов'язані з використанням інформаційних та комунікаційних технологій. Однак, незважаючи на значний прогрес у цій галузі, залишаються невирішеними питання інтеграції

цифрової безпеки у загальну систему економічної безпеки підприємств, що потребує подальших досліджень і розробок.

Мета і завдання дослідження. Метою даної кваліфікаційної роботи є огляда та аналіз впровадження методики оцінювання рівня економічної безпеки підприємства у кіберпросторі в умовах цифрової трансформації, а також розробка рекомендацій щодо підвищення цього рівня. Для досягнення цієї мети необхідно здійснити комплексний аналіз сучасних методів оцінювання економічної безпеки, ідентифікувати основні кіберзагрози, що впливають на економічну безпеку підприємства, та спробувати спрогнозувати результати методів з урахуванням нових цифрових ризиків та можливостей.

Об'єкт дослідження. Об'єктом дослідження є процес забезпечення економічної безпеки підприємства в умовах цифрової трансформації та кіберпростору.

Предмет дослідження. Предметом дослідження є методи та підходи до оцінювання рівня економічної безпеки підприємства в умовах цифрової трансформації та кіберзагроз, а також розробка практичних рекомендацій для підвищення цього рівня.

Методи дослідження. У процесі дослідження були використані декілька різних методів:

1. Логічний аналіз
2. Індукція та дедукція
3. Формалізація та узагальнення
4. Математичне моделювання
5. Теоретичне обґрунтування

Теоретична, методична та практична значущість отриманих результатів. Прикладне значення:

Отримані результати проведених аналітичних і розрахункових процедур мають безпосереднє значення для досліджуваної бази практики. Це включає конкретні рекомендації для підвищення рівня економічної безпеки підприємств в умовах цифрової трансформації, що можуть бути впроваджені в практику. Результати дослідження можуть бути використані для конкретних підприємств, галузей або економіки в цілому, що дозволить ефективно протидіяти кіберзагрозам, підвищити стабільність та конкурентоспроможність підприємств, забезпечити їх фінансову стійкість та захист активів.

Теоретико-методичне значення:

Робота має також важливе теоретико-методичне значення. У ході дослідження були здійснені узагальнення, виділені ключові характеристики економічної безпеки в

умовах цифрової трансформації, сформовані алгоритми для оцінювання рівня безпеки підприємств, розвинуті нові ідеї та запропонований методичний підхід до інтеграції цифрової безпеки в загальну систему економічної безпеки. Ці результати можуть бути застосовані не лише для розв'язання проблем конкретних підприємств, але й для інших подібних проблем або компаній, галузей, економік і процесів.

Інформаційна база дослідження. Основну частину використаної літератури складають праці вітчизняних та зарубіжних науковців і практиків, аналіз наукових статей, монографій, дисертаційних досліджень, які висвітлюють питання економічної безпеки підприємств, цифрової трансформації та кібербезпеки. Також у роботі використовувались фінансові звіти підприємств деякі нормативно-правові акти, а також інтернет-джерела. Така інформаційна база дає змогу зберегти комплексний підхід до дослідження і дозволяє враховувати різні аспекти економічної безпеки підприємств у цифрову епоху кіберзагроз.

РОЗДІЛ 1

ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ ОЦІНЮВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА У КІБЕРПРОСТОРІ

1.1 Сучасний стан наукової думки щодо економічної безпеки підприємства.

Економічна безпека підприємства є багатогранним поняттям, яке розглядається в контексті захисту підприємства від різноманітних загроз та забезпечення його стабільного функціонування та розвитку. Згідно з К. С. Зайченко та Н. І. Діма, економічна безпека підприємства немає якогось чіткого, стандартизованого визначення, на яке можна було б покладатися в різних життєвих ситуаціях[3]. Тому із цим поняттям потрібно бути обережним і завжди брати до уваги контекст. До прикладу одне із використовуваних раніше визначень має в собі ключову ознаку «Комплекс заходів» і звучить так – *Економічна безпека підприємства - комплекс організаційно-управлінських, технологічних, технічних, профілактичних і маркетингових заходів, спрямованих на кількісну і якісну реалізацію захисту інтересів підприємства від зовнішніх та внутрішніх загроз.* [4]. І в той же час А. Штангрет зосереджується саме на складовій підприємства. В цьому випадку визначення виглядає так:

Економічна безпека підприємства – головна ознака економічної безпеки підприємства полягає в тому, щоб гарантувати його стабільне та максимально ефективне функціонування сьогодні і високий потенціал розвитку в майбутньому[5].

Виходячи із різноманітності цього поняття впливає, що економічна безпека підприємства є складним та багатогранним явищем. Вона охоплює різні аспекти діяльності підприємства, включаючи фінансову, кадрову, технічну, інформаційну, екологічну та правову безпеку. Така мультиаспектність поняття вимагає різноманітних наукових підходів, адже кожен підхід акцентує увагу на певних аспектах, які в свою чергу викликають реакцію у вигляді різних пріоритетів та методах досліджень. Тому під час досліджень не варто нехтувати комплексним підходом до вивчення цього визначення.

У тій ж роботі К. С. Зайченко та Н. І. Діма було виділено основні структурні елементи економічної безпеки – див. Табл 1.1

Таблиця 1.1 – Структурні елементи економічної безпеки

Структурний елемент	Сутність та роль
Інформаційна безпека	Захист внутрішньої інформації, комерційної таємниці та забезпечення необхідного рівня інформаційного забезпечення всіх підрозділів підприємства.
Техніко-технологічна безпека	Забезпечення технологічної автономії та конкурентоспроможності технічного потенціалу підприємства.
Кадрова та інтелектуальна безпека	Заходи для підвищення кваліфікації персоналу та його інтелектуального потенціалу, а також захист від внутрішніх загроз, пов'язаних з персоналом.
Фінансова безпека	Рациональне використання корпоративних ресурсів, забезпечення фінансової стійкості та ліквідності підприємства.
Організаційно-управлінська безпека	Ефективна організація управління та реалізація цілей підприємства.
Політико-правова безпека	Захист персоналу, капіталу, майна та комерційних інтересів підприємства.
Екологічна безпека	Мінімізація негативних впливів виробничої діяльності на навколишнє середовище.
Силова безпека	Правовий захист всіх аспектів діяльності підприємства.

Джерело: розроблено автором на основі [3],[4],[5]

Провівши аналіз структурних елементів економічної безпеки підприємства, представлених в таблиці, можна зробити кілька важливих висновків, що відображають сучасний стан та потреби підприємств у забезпеченні своєї безпеки.

Економічна безпека підприємства є складною системою, що складається з багатьох взаємопов'язаних елементів, кожен з яких відіграє критично важливу роль у забезпеченні стабільного та ефективного функціонування підприємства. До цих елементів відносяться інформаційна, техніко-технологічна, кадрова та інтелектуальна, фінансова, організаційно-управлінська, силова, екологічна та політико-правова безпека.

Кожен з елементів економічної безпеки залежить від впливу як зовнішніх, так і внутрішніх факторів. Інформаційна безпека, наприклад, залежить від рівня технологій та заходів захисту, тоді як кадрова безпека залежить від кваліфікації та мотивації персоналу. Відповідно, для ефективного забезпечення економічної безпеки необхідно враховувати широкий спектр факторів, які можуть впливати на підприємство.

Забезпечення економічної безпеки вимагає комплексного підходу, який включає заходи з управління ризиками, забезпечення ресурсами, організацію управлінських процесів та впровадження технологій. Жоден із структурних елементів не може забезпечити повну безпеку підприємства окремо; необхідна синергія всіх елементів. Наприклад, фінансова безпека тісно пов'язана з техніко-технологічною та кадровою безпекою, оскільки ефективність використання ресурсів залежить від рівня кваліфікації персоналу та технічного потенціалу підприємства.

В умовах цифрової трансформації особливого значення набувають інформаційна та техніко-технологічна безпека. Захист інформації, технологічна автономія та конкурентоспроможність технічного потенціалу є ключовими факторами для успішного функціонування підприємства. Організаційно-управлінська безпека є визначальною умовою реалізації та досягнення цілей підприємства, оскільки ефективне управління забезпечує координацію всіх елементів економічної безпеки та сприяє підвищенню загальної ефективності підприємства. Екологічна безпека стає все більш важливою в умовах зростаючої уваги до екологічних аспектів діяльності підприємств, а політико-правова безпека забезпечує правовий захист діяльності підприємства в умовах сучасного регульованого економічного середовища.

Таким чином, для забезпечення високого рівня економічної безпеки підприємства необхідно враховувати та інтегрувати всі зазначені структурні елементи. Комплексний підхід, що включає інформаційні, техніко-технологічні, кадрові, фінансові, організаційно-управлінські, силові, екологічні та політико-правові аспекти, дозволить підприємству ефективно протидіяти загрозам та забезпечувати стабільний розвиток в умовах сучасного динамічного середовища.

Також при розгляді сучасної літератури на цю тему варто виділити роботу А. Мілка, О. Артюх-Пасюта і Ж. Кононенко. У своїй роботі вони виділили різноманіття методологічних підходів у дослідженні оцінювання рівня економічної безпеки підприємств у сучасних умовах. У статті представлено різні підходи до оцінки рівня економічної безпеки підприємства, які включають ресурсно-функціональний, індикаторний, прибутково-інвестиційний, тривимірний, програмно-цільовий, метод прогнозування банкрутства, економіко-математичний, системний та підхід теорії економічних ризиків. Ресурсно-функціональний підхід зводиться до розрахунку сукупного критерію економічної безпеки як середньозваженого значення часткових функціональних критеріїв. Індикаторний підхід порівнює фактичні показники діяльності підприємства з граничними значеннями, що відповідають певному рівню безпеки. Прибутково-інвестиційний підхід порівнює обсяги валових інвестицій з необхідними для забезпечення економічної безпеки коштами. Тривимірний підхід розраховує середньозважене значення рівня поточної, тактичної та стратегічної безпеки. Програмно-цільовий підхід інтегрує сукупність показників, що визначають

рівень економічної безпеки, використовуючи методи кластерного і багатовимірного аналізу. Методи прогнозування банкрутства ідентифікують симптоми фінансової кризи. Економіко-математичний підхід базується на функціональній залежності рівня економічної безпеки від показників діяльності. Системний підхід використовує статичний і динамічний аналіз, враховуючи всі внутрішні і зовнішні зв'язки підприємства. Підхід теорії економічних ризиків моделює можливі загрози та аналізує їх ризики, невизначеність та ймовірність. Кожен з цих підходів надає унікальні методи і критерії для комплексної оцінки економічної безпеки підприємства[6].

Знову ж таки, результати аналізу показують, наскільки об'ємним є питання оцінювання рівня економічної безпеки, адже окрім великого різноманіття трактування цього поняття, ми можемо зустріти у літературі і різні методи роботи у цій сфері. Тому ще раз варто наголосити, що комплексність оцінки потребує і комплексних підходів, саме через це і виникає потреба у використанні великої кількості методів. Різні методи дозволяють адаптувати оцінку до специфіки підприємства, галузі, ринку або економічного середовища, забезпечуючи адаптивність до конкретних умов і ситуацій. Крім того, різноманітність методів відображає інтеграцію різних наукових підходів, що підкреслює необхідність комплексного аналізу для повного розуміння та забезпечення економічної безпеки.

Варто звернути увагу на те, що роботи у сучасному науковому світі на цю тему розглядають здебільшого оцінку економічної безпеки підприємства в цілому, рідко в умовах сучасності, і у якості виключення в умовах кіберпростору. Це ще раз доводить наскільки актуальним є це дослідження, зосереджене саме на специфічних аспектах економічної безпеки підприємства в умовах цифрової трансформації та кіберзагроз. Таке дослідження заповнює значну прогалину в науковій літературі та практиці, надаючи підприємствам інструменти для оцінки та підвищення їхньої економічної безпеки в умовах сучасних викликів.

1.2 Теоретичні підходи до визначення та оцінки економічної безпеки.

Економічна безпека підприємства є багатограним поняттям, яке включає захист від різних внутрішніх і зовнішніх загроз, що можуть негативно вплинути на його стабільне функціонування та розвиток. У сучасній науковій літературі виділяються класичні та сучасні підходи до визначення та оцінки економічної безпеки.

Класичні підходи

Класичні підходи до економічної безпеки підприємства зосереджуються на захисті матеріальних та фінансових ресурсів підприємства. Основними аспектами, що розглядаються в рамках класичних підходів, є:

1. Фінансова безпека:
 - Забезпечення фінансової стабільності підприємства.
 - Захист від фінансових ризиків, включаючи неплатоспроможність та банкрутство.
 - Баланс і якість фінансових інструментів і технологій.
2. Кадрова безпека:
 - Збереження та розвиток кваліфікованих кадрів.
 - Захист від внутрішніх загроз, пов'язаних з персоналом.
 - Підвищення кваліфікації працівників та запобігання втраті ключових співробітників.
3. Техніко-технологічна безпека:
 - Високий технічний та технологічний рівень виробництва.
 - Своєчасне виявлення та усунення загроз (наприклад, природних катастроф, пожеж, несанкціонованого доступу).
4. Інформаційна безпека:
 - Захист внутрішньої інформації та комерційної таємниці.
 - Забезпечення необхідного рівня інформаційного забезпечення всіх підрозділів підприємства.
5. Екологічна безпека:
 - Мінімізація негативних впливів виробничої діяльності на навколишнє середовище.
 - Дотримання екологічних норм і стандартів.
6. Комерційна безпека:
 - Ефективна організація і управління процесами збуту.
 - Задоволення споживчого попиту і отримання комерційного прибутку.
7. Політико-правова безпека:
 - Захист від негативних впливів політичного та правового середовища.
 - Планування і реалізація заходів, спрямованих на забезпечення безпеки підприємства[7].

Класичні підходи до економічної безпеки підприємства підкреслюють важливість комплексного захисту різних аспектів діяльності підприємства. Вони включають як внутрішні, так і зовнішні заходи, спрямовані на забезпечення

стабільності та стійкості підприємства в умовах економічної невизначеності та ризиків.

Сучасні підходи

У тій ж роботі А. Мілка розглянуто різні сучасні методологічні підходи до оцінки рівня економічної безпеки підприємства, зокрема:

1. Ресурсно-функціональний підхід:
 - Оцінка рівня економічної безпеки підприємства як середньозваженого значення часткових функціональних критеріїв безпеки.
2. Індикаторний підхід:
 - Встановлення рівня безпеки шляхом порівняння фактичних показників діяльності підприємства з граничними значеннями цих показників.
3. Прибутково-інвестиційний підхід:
 - а. Порівняння обсягу валових інвестицій з необхідними для забезпечення економічної безпеки коштами.
4. Тривимірний підхід:
 - Розрахунок середньозваженого значення рівня поточної, тактичної та стратегічної безпеки.
5. Програмно-цільовий підхід:
 - Інтеграція сукупності показників, що визначають рівень економічної безпеки підприємства, використовуючи методи кластерного і багатовимірного аналізу.
6. Методи прогнозування банкрутства:
 - Ідентифікація симптомів фінансової кризи підприємства та оцінка рівня поточної платоспроможності.
7. Економіко-математичний підхід:
 - Оцінка рівня економічної безпеки на основі функціональної залежності від показників діяльності підприємства, включаючи методи експертних оцінок, регресійного і дисперсійного аналізу, експоненціального згладжування, теорії нечітких систем та багатовимірного статистичного аналізу.
8. Системний підхід:
 - Використання статичного і динамічного аналізу стану підприємства з урахуванням усіх внутрішніх та зовнішніх зв'язків і взаємозалежностей.
9. Підхід теорії економічних ризиків:
 - Побудова механізму економічної безпеки підприємства на основі моделювання можливих загроз та їх аналізу, розрахунок ризиків, невизначеностей та ймовірностей для різних загроз.

Ці підходи дозволяють комплексно оцінювати рівень економічної безпеки підприємства, враховуючи сучасні виклики та загрози, що виникають в умовах цифрової трансформації та глобалізації[6].

Далі варто розглянути саме методологічні підходи до оцінки. На мою думку варто зупинитись саме на індикаторному методі, методі моделювання та прогнозування і методі експертних оцінок.

Індикаторний метод є одним з найбільш поширених методів оцінки економічної безпеки підприємства. Він базується на аналізі сукупності індикаторів, які відображають різні аспекти діяльності підприємства. Спочатку вибираються ключові індикатори, що характеризують фінансову стабільність, техніко-технологічний рівень, кадровий потенціал та інформаційну безпеку. Зібрані дані про фактичні значення цих індикаторів порівнюються з нормативними значеннями, встановленими на основі галузевих стандартів або рекомендацій експертів.

Після цього проводиться розрахунок інтегрального показника, який є середньозваженим значенням обраних індикаторів. Це дозволяє отримати загальну оцінку рівня економічної безпеки підприємства. Такий підхід забезпечує можливість оперативного моніторингу стану підприємства та виявлення його сильних і слабких сторін. На основі аналізу результатів визначаються основні загрози та ризики, а також розробляються заходи для їх мінімізації.

Індикаторний метод надає кількісну оцінку рівня економічної безпеки, що робить його особливо цінним для прийняття управлінських рішень. Він дозволяє підприємствам ефективно управляти своїми ресурсами та забезпечувати стійкий розвиток в умовах сучасного економічного середовища.

Якщо ж спробувати математично інтерпретувати індикаторний метод, то отримаємо наступне:

Вибір індикаторів: Нехай $I_1, I_2, I_3, \dots, I_n$ – обрані індикатори, що характеризують різні аспекти економічної безпеки підприємства. Далі зібрані значення індикаторів нормалізуються відносно їх граничних нормативних значень.

$$N_i = \frac{X_i}{X_{normi}}$$

де X_i – значення індикатора, X_{normi} – нормативне значення індикатора i

Далі йде розрахунок інтегрального показника рівня економічної безпеки S розраховується як середньозважене значення нормалізованих індикаторів

$$S = \sum_{i=1}^n \omega_i N_i,$$

де, ω_i – ваговий коефіцієнт індикатора i , який визначає важливість цього індикатора в загальній оцінці

Якщо ж перейти до інтерпретації, то отримане значення S порівнюється з нормативним значенням для визначення рівня економічної безпеки. Якщо $S \geq 1$ івень економічної безпеки вважається задовільним. Якщо ж навпаки, то, відповідно, необхідно вжити заходів для підвищення безпеки[8].

Метод моделювання та прогнозування є ключовим інструментом для оцінки економічної безпеки підприємства, що дозволяє аналізувати можливі загрози та прогнозувати їхній вплив. Цей метод базується на використанні економіко-математичних моделей, які дозволяють створювати сценарії розвитку подій та оцінювати наслідки різних ризиків. Важливим аспектом є врахування як внутрішніх, так і зовнішніх факторів, які можуть впливати на діяльність підприємства.

Одним з основних підходів в моделюванні є використання регресійного аналізу для визначення залежності між різними економічними показниками та рівнем економічної безпеки. Це дозволяє виявити ключові фактори, що впливають на безпеку, та оцінити їхній внесок у загальну картину. Також широко застосовуються методи дисперсійного аналізу, експоненціального згладжування, теорії нечітких множин та багатовимірною статистичного аналізу, які дозволяють врахувати складні нелінійні взаємозв'язки між показниками.

Прогнозування базується на аналізі історичних даних та побудові моделей, які дозволяють передбачати майбутні значення ключових індикаторів економічної безпеки. Це дозволяє підприємству завчасно виявляти потенційні загрози та розробляти стратегії для їхнього уникнення або мінімізації негативних наслідків. Важливим етапом є валідація моделей, що забезпечує їхню точність та надійність. Таким чином, метод моделювання та прогнозування є незамінним інструментом для стратегічного планування та управління ризиками на підприємстві[9].

Математичний зміст методі моделювання та прогнозування доволі складний і потребує детального розгляду, це не є темою роботи, тому для ознайомлення див. джерело [9].

Метод експертної оцінки є одним з важливих інструментів для аналізу економічної безпеки підприємства, особливо в умовах невизначеності та відсутності достатньої кількості статистичних даних. Цей метод базується на знаннях та досвіді фахівців, які здатні надати якісну оцінку ризиків і загроз, що впливають на економічну безпеку підприємства. Експерти можуть бути внутрішніми (працівники підприємства) або зовнішніми (консультанти, науковці).

Основна процедура методу експертної оцінки включає кілька етапів. Спочатку формується група експертів, які мають відповідну кваліфікацію та досвід. Потім визначаються ключові аспекти економічної безпеки, що потребують оцінки. Експерти проводять аналіз та оцінку цих аспектів на основі своїх знань, після чого результати узагальнюються та інтерпретуються. Результати експертних оцінок можуть бути представлені у вигляді рейтингових шкал, балів або інших кількісних показників.

Перевагою методу експертної оцінки є можливість врахування суб'єктивних факторів і складних ситуацій, які важко піддаються кількісному аналізу. Крім того, цей метод дозволяє швидко отримати оцінку ризиків без необхідності довготривалого збору даних. Однак, варто враховувати, що результати можуть бути суб'єктивними та залежати від компетенції експертів, тому важливо забезпечити високий рівень кваліфікації та різноманітності думок серед експертної групи[10].

Математична інтерпретація метода експертного оцінювання може виглядати різними способами, для прикладу часто використовують коефіцієнт Спірмена. Коефіцієнт Спірмена, або ранговий коефіцієнт кореляції Спірмена, є статистичним показником, який використовується для оцінки монотонного зв'язку між двома змінними. Він вимірює, наскільки добре відносини між двома наборами даних можуть бути описані за допомогою монотонної функції[14].

Формула для розрахунку коефіцієнта Спірмена:

$$p = 1 - \frac{6 \sum d_i^2}{n(n^2 - 1)}$$

Де p — коефіцієнт кореляції Спірмена, d_i — різниця між рангами відповідних змінних, n — кількість спостережень.

Коефіцієнт Спірмена використовують для перевірки узгодженості думок експертів, так само як і коефіцієнт Пірсона. Коефіцієнт Пірсона, або коефіцієнт кореляції Пірсона, є показником лінійної залежності між двома змінними. Він варіюється від -1 до 1, де 1 означає ідеальну позитивну лінійну кореляцію, -1 означає ідеальну негативну лінійну кореляцію, а 0 означає відсутність лінійної кореляції[15].

Також варто розглянути Інтеграційний підхід до оцінювання економічної безпеки підприємства в умовах цифрової трансформації передбачає поєднання різних методів та інструментів для отримання комплексної оцінки. Цей підхід враховує як кількісні, так і якісні аспекти, що забезпечує всебічне розуміння стану економічної безпеки.

Одним з ключових елементів інтеграційного підходу є використання кластерного аналізу, який дозволяє групувати схожі показники та виявляти основні тенденції. Це допомагає ідентифікувати сильні та слабкі сторони підприємства, а

також визначити основні загрози та ризики. Наприклад, кластерний аналіз може бути застосований для сегментації фінансових, техніко-технологічних, кадрових та інформаційних аспектів безпеки.

Багатовимірний аналіз дозволяє враховувати взаємозв'язки між різними показниками та їх вплив на загальний рівень економічної безпеки. Цей метод використовує математичні моделі для визначення комплексного інтегрального показника безпеки, який враховує різні фактори та їх вагомість. Багатовимірний аналіз дозволяє оцінити вплив кожного фактора на загальну картину безпеки та виявити основні ризики.

Для забезпечення комплексності оцінки використовуються також методи експертних оцінок, які дозволяють враховувати суб'єктивні думки фахівців щодо різних аспектів економічної безпеки. Це допомагає забезпечити глибше розуміння складних та багатогранних аспектів, які важко виміряти кількісно.

Інтеграція різних методів дозволяє створити більш точну та надійну оцінку рівня економічної безпеки підприємства. Вона допомагає підприємствам вчасно виявляти та реагувати на загрози, що виникають у зв'язку з цифровою трансформацією та іншими змінами в зовнішньому середовищі. Це забезпечує стійкий розвиток підприємства та його конкурентоспроможність у сучасних умовах[2], [11].

1.3. Інтеграція кібербезпеки в загальну систему економічної безпеки підприємства

Інтеграція кібербезпеки в загальну систему економічної безпеки підприємства є критично важливою в умовах сучасної цифрової трансформації. Кібербезпека забезпечує захист інформаційних систем, даних та цифрових активів підприємства від кібератак, несанкціонованого доступу та інших кіберзагроз. Це включає впровадження технологічних рішень, таких як антивірусне програмне забезпечення, брандмауери, системи виявлення та запобігання вторгненням (IDS/IPS), а також регулярні оновлення програмного забезпечення для усунення вразливостей. Для ефективної інтеграції кібербезпеки необхідно проводити регулярні аудити безпеки та оцінки ризиків. Це дозволяє виявляти потенційні слабкі місця в системах підприємства та своєчасно усувати їх. Крім того, важливо розробляти плани реагування на інциденти, які визначають дії підприємства у випадку кібератаки або порушення безпеки. Це забезпечує оперативне виявлення та нейтралізацію загроз, мінімізуючи їх вплив на діяльність підприємства. Інтеграція кібербезпеки в загальну систему економічної безпеки також передбачає тісну співпрацю між різними

підрозділами підприємства. Фінансові, технічні, кадрові та інші підрозділи повинні працювати разом для забезпечення всебічного захисту від загроз. Це дозволяє створити єдину, інтегровану систему, яка охоплює всі аспекти діяльності підприємства і забезпечує його стійкість та захищеність в умовах сучасного цифрового середовища.

Для прикладу Стендер С. В., Фротер О. С., Снітко Ю. М. у своїй роботі для дослідження використовували загальнонаукові та спеціальні методи, включаючи аналітичний, феноменологічний, історичний методи, а також системно-структурний підхід. Зокрема, феноменологічні методи допомогли дослідити унікальні особливості кіберзахисту економіки України, а історичний метод дозволив аналізувати першопричини кіберзагроз в країні. У статті визначено, що інформаційна безпека є ключовим компонентом економічної безпеки. Вона розглядається як спосіб забезпечення та захисту інформації в соціально-економічних системах. Метою статті є дослідження та обґрунтування необхідності регулювання питання захисту економіки від кіберзагроз в сучасних умовах України. І в цілому Стаття присвячена дослідженню важливих аспектів кібербезпеки в умовах цифрової трансформації економіки України. У статті пропонується створити ефективну систему державного регулювання кібербезпеки, а також оптимізувати кадровий склад у сфері кібербезпеки. Автори наголошують на необхідності розробки математичної моделі, яка дозволить комплексно оцінити стан цифрової трансформації та кіберзахисту економіки. У перспективі рекомендується створення ефективної організаційно-технічної моделі національної системи кібербезпеки, стимулювання інноваційної діяльності та оптимізація національного законодавства у цій сфері.

Таким чином, стаття підкреслює критичну важливість інтеграції кібербезпеки в загальну систему економічної безпеки України. Це забезпечить стійкість національної економіки в умовах цифрової трансформації та глобальних викликів, сприяючи захисту національних інтересів та забезпеченню стабільного розвитку[12].

Також особливо важливо оглянути основні критерії безпеки сучасного цифрового підприємства. Стаття «Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану» досліджує важливі аспекти забезпечення кібербезпеки для суб'єктів господарювання в умовах сучасних викликів, зокрема під час воєнного стану[13]. Автори зосереджуються на необхідності адаптації та впровадження нових технологічних та управлінських підходів для захисту інформаційних систем і даних підприємств. У статті визначено основні критерії безпеки сучасного цифрового підприємництва. Серед них особливу увагу приділено шифруванню даних як при зберіганні, так і при передачі. Шифрування повинно відбуватися на клієнтському рівні, при цьому доступ до ключів шифрування має бути тільки у клієнта. Важливо,

щоб фактичні дані не передавалися по відкритих каналах, а компанія контролювала сховище зашифрованої інформації та ключі доступу до неї.

Шифрування є ключовим компонентом забезпечення кібербезпеки, оскільки дозволяє захистити дані від несанкціонованого доступу та зловмисних дій.

Шифрування даних повинно відбуватися на клієнтському рівні, тобто на рівні кінцевих користувачів. Це означає, що дані шифруються ще до того, як вони покидають пристрій користувача, і залишаються зашифрованими протягом усього процесу зберігання і передачі. Такий підхід забезпечує високий рівень безпеки, оскільки навіть якщо зловмисник отримає доступ до даних, він не зможе їх розшифрувати без відповідного ключа.

Ключі шифрування повинні бути доступні лише клієнту. Це означає, що лише власник даних має доступ до ключів шифрування і, відповідно, до можливості розшифрування даних. Це значно підвищує безпеку, оскільки навіть адміністратори систем або треті сторони, які мають доступ до збережених або переданих даних, не можуть їх розшифрувати без ключа.

Автори підкреслюють важливість того, щоб фактичні дані не передавалися по відкритих каналах пошти. Відкриті канали є вразливими до перехоплення і зловмисних дій, тому використання таких каналів для передачі конфіденційних даних неприпустиме. Натомість, слід використовувати захищені канали передачі даних, які забезпечують шифрування даних на всіх етапах їхнього переміщення.

Контроль сховища зашифрованої інформації та ключів доступу до неї також є важливим аспектом кібербезпеки. Компанія повинна забезпечувати надійне зберігання зашифрованих даних і ключів шифрування, а також мати чіткі процедури доступу та управління цими ключами. Це включає регулярні перевірки безпеки, моніторинг доступу та швидке реагування на можливі інциденти.

Узагальнюючи, шифрування даних на клієнтському рівні з доступом до ключів лише у клієнта, використання захищених каналів передачі даних і надійний контроль сховищ зашифрованої інформації є критично важливими для забезпечення високого рівня кібербезпеки підприємств у сучасних умовах цифрової трансформації та воєнного стану.

Отож, варто перейти до основної частини цього розділу, а саме оцінки доцільності впровадження інтеграції кібербезпеки в підприємстві. Варто зрозуміти, що у цього підходу є як свої плюси, так і мінуси. Тому далі вони будуть розглянуті.

Плюси:

- Підвищення загального рівня безпеки. Інтеграція кібербезпеки забезпечує захист не лише фізичних, фінансових та організаційних активів підприємства, але й інформаційних, що створює комплексний захист від різних загроз.
- Покращення управління ризиками. Завдяки інтеграції кібербезпеки можна ефективніше ідентифікувати, оцінювати та управляти ризиками, що стосуються інформаційних систем та даних підприємства.
- Збільшення довіри з боку клієнтів та партнерів. Високий рівень кібербезпеки підвищує довіру до підприємства з боку клієнтів та партнерів, що може сприяти зростанню бізнесу та зміцненню репутації.
- Запобігання фінансовим втратам. Інтеграція кібербезпеки допомагає запобігти фінансовим втратам, пов'язаним з кібератаками, такими як витік даних, шантаж та інші форми кіберзлочинності.
- Підвищення ефективності бізнес-процесів. Інтегровані системи кібербезпеки можуть автоматизувати багато процесів, що дозволяє знизити кількість помилок та підвищити загальну ефективність управління підприємством.

Мінуси:

- Значні фінансові витрати. Впровадження та підтримка систем кібербезпеки вимагає значних фінансових ресурсів, що може бути обтяжливим для малого та середнього бізнесу.
- Складність інтеграції. Процес інтеграції кібербезпеки в загальну систему економічної безпеки може бути складним і вимагати значних часових та кадрових ресурсів.
- Необхідність постійного оновлення. Кібербезпека потребує постійного оновлення технологій та процедур для захисту від нових загроз, що вимагає безперервного моніторингу та інвестицій.
- Ризик внутрішніх загроз. Незважаючи на зовнішні заходи безпеки, існує ризик внутрішніх загроз, таких як недобросовісні працівники або випадкові помилки персоналу.
- Можливість помилкових спрацювань систем безпеки. Системи кібербезпеки можуть іноді помилково ідентифікувати легітимні дії як загрози, що може призвести до затримок у роботі та зниження продуктивності.

Інтеграція кібербезпеки в загальну систему економічної безпеки підприємства є важливим і необхідним кроком для забезпечення комплексного захисту від різних загроз в умовах цифрової трансформації. Плюси інтеграції, такі як підвищення загального рівня безпеки, покращення управління ризиками, збільшення довіри з боку клієнтів та партнерів, запобігання фінансовим втратам і підвищення ефективності бізнес-процесів, значно переважають можливі мінуси. Хоча впровадження інтегрованої системи кібербезпеки може вимагати

значних фінансових витрат, складності інтеграції, необхідності постійного оновлення та ризику внутрішніх загроз, ці виклики можна подолати за допомогою стратегічного планування, належного управління ресурсами та регулярного навчання персоналу.

Враховуючи важливість кібербезпеки у сучасному бізнес-середовищі та потенційні втрати від кібератак, інтеграція кібербезпеки є виправданою та доцільною. Прийняття цього кроку дозволить підприємствам забезпечити стійкість і конкурентоспроможність у довгостроковій перспективі, мінімізуючи ризики та захищаючи свої активи.

РОЗДІЛ 2

ОЦІНЮВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

2.1 Аналіз поточного стану економічної безпеки підприємств в кіберпросторі на основі переддипломної практики

Метод експертного оцінювання є ефективним інструментом для аналізу економічної безпеки підприємства в кіберпросторі. Він дозволяє отримати якісну оцінку стану безпеки на основі знань та досвіду фахівців у цій галузі. В якості прикладу використання методів експертного оцінювання була вибрана компанія ТОВ «ХВР РІВНЕ». В якості експертів будуть виступати люди, які працюють в компанії вже досить довго і стикались із різними ситуаціями, знаходили виходи із них в тому числі із кібератаками.

1. Головатий Павло – перший експерт. Team Leader, безпосередній керівник відділу, в якому я проходив практику.
2. Миронюк Юрій – другий експерт. Team Leader Legacy – відповідальний за коректуру роботи команди моделерів
3. Потапчук Тарас – третій експерт. Coach – ментор, який допомагає і наставляє новачків в компанії
4. Олександр Корольов – четвертий експерт. Coach - ментор, який допомагає і наставляє новачків в компанії.

Експертам було запропоновані такі фактори для надання оцінок:

1. Захист мережі: Ефективність використання брандмауерів, VPN та інших засобів захисту мережі.
2. Політики безпеки: Наявність та дотримання внутрішніх політик кібербезпеки.
3. Системи виявлення та реагування на загрози: Використання IDS/IPS та інших систем моніторингу.
4. Автоматизація безпеки: Рівень впровадження автоматизованих систем для запобігання та реагування на кіберзагрози.
5. Кваліфікація персоналу: Рівень знань і навичок співробітників у сфері кібербезпеки.
6. Управління вразливостями: Процеси виявлення, оцінки та усунення вразливостей.
7. Контроль доступу: Ефективність управління правами доступу до критичних систем та даних.

8. Захист даних: Використання шифрування, резервного копіювання та інших методів захисту даних.
9. Моніторинг та аналіз: Безперервний моніторинг систем та аналіз журналів подій.
- 10.Інцидент-менеджмент: Процеси реагування на кіберінциденти, включаючи планування та навчання персоналу.

В якості шкали оцінювання було обрано оцінювання від 1 до 10. Експертами проранжовано фактори по їх важливості. Результати зведені у таблицю (див. Табл. 2.1.)

Табл. 2.1 – Оцінки експертів

Експерти	Фактори									
	1	2	3	4	5	6	7	8	9	10
Головатий Павло	4	3	10	2	1	1	10	7	1	1
Миронюк Юрій	2	1	9	3	4	2	9	5	4	2
Потапчук Тарас	3	2	10	1	2	3	10	5	2	3
Корольов Олександр	2	5	8	5	3	7	8	5	1	1

*Примітка: Нумерація факторів відповідає запропонованому списку вище
Таблиця була сформована на основі оцінок експертів*

Далі визначимо ступіть узгодженості думок експертів за допомогою коефіцієнта конкордації.

Розрахуємо суми рангів, призначених експертами кожному підприємству (розраховуємо по стовпчиках) (див. Табл. 2.2):

Табл. 2.2 – Знаходження суми рангів

Експерти	Фактори									
	1	2	3	4	5	6	7	8	9	10
Головатий Павло	7	6	9,5	5	2,5	2,5	9,5	8	2,5	2,5
Миронюк Юрій	3	1	9,5	5	6,5	3	9,5	8	6,5	3
Потапчук Тарас	6	3	9,5	1	3	6	9,5	8	3	6
Корольов Олександр	3	6	9,5	6	4	8	9,5	6	1,5	1,5
S_j	19	16	38	17	16	19,5	38	30	13,5	13

Розрахуємо відхилення суми рангів від середньої суми d_j (див. Табл. 2.3):

$$\frac{\sum_{j=1}^n S_j}{n} = \frac{220}{10} = 22$$

Отже. 22 – середня сума рангів

Табл. 2.3 – Суми рангів

Експерти	Фактори										Сума
	1	2	3	4	5	6	7	8	9	10	
1	7	6	9,5	5	2,5	2,5	9,5	8	2,5	2,5	
2	3	1	9,5	5	6,5	3	9,5	8	6,5	3	
3	6	3	9,5	1	3	6	9,5	8	3	6	
4	3	6	9,5	6	4	8	9,5	6	1,5	1,5	
S _j	19	16	38	17	16	19,5	38	30	13,5	13	220
d _j	3	6	-16	5	6	2,5	-16	-8	8,5	9	
d _j ²	9	36	256	25	36	6,25	256	64	72,25	81	841,5

Розрахуємо кількість груп однакових рангів для кожного експерта:

$$L_1 = (2,5; 2,5; 2,5; 2,5), (9,5; 9,5),$$

$$L_2 = (3; 3; 3), (6,5; 6,5), (9,5; 9,5),$$

$$L_3 = (3; 3; 3), (6; 6; 6), (9,5; 9,5),$$

$$L_4 = (1,5; 1,5), (6; 6; 6), (9,5; 9,5).$$

$$\text{Таким чином, } L = L_1 + L_2 + L_3 + L_4 = 11$$

Розрахуємо результати T_i – кількість зв'язаних рангів в кожній групі:

$$\text{для 1 – о експерта: } L=2; T_1 = (4^2 - 4) + (2^2 - 2) = 14$$

$$\text{для 2 – о експерта: } L=3; T_2 = (3^3 - 3) + (2^3 - 2) + (2^3 - 2) = 32$$

$$\text{для 3 – о експерта: } L=3; T_3 = (3^3 - 3) + (3^3 - 3) + (2^3 - 2) = 50$$

$$\text{для 4 – о експерта: } L=3; T_4 = (2^3 - 2) + (3^3 - 3) + (2^3 - 2) = 32$$

$$\text{Сума } T = 14 + 32 + 50 + 32 = 128.$$

Розрахуємо коефіцієнт конкордації:

$$\begin{aligned}
 W &= \frac{841,5}{\frac{1}{12} [4^2(10^3 - 10) - 4 * 128]} = \frac{841,5}{\frac{1}{12} [16 * (1000 - 10) - 512]} = \\
 &= \frac{841,5}{\frac{1}{12} [15840 - 512]} = \frac{841,5}{\frac{1}{12} * 15328} = \frac{841,5}{1277,33} = 0,659 = 65,9\%
 \end{aligned}$$

Значення 0,659 вказує на високу ступінь узгодженості думок експертів.

Отже, можна зробити висновок, що думки експертів досить добре узгоджені між собою. Це означає, що експерти мають високий рівень згоди у вирішенні питань або оцінці ситуацій в рамках дослідження чи експертизи. Для більш точного аналізу оцінок визначимо ступінь узгодженості думок експертів за допомогою коефіцієнта кореляції Пірсона (див. Табл 2.4)

Табл. 2.4 – Знаходження коефіцієнту кореляції Пірсона

Експерти	Фактори										Сума
	1	2	3	4	5	6	7	8	9	10	
Головатий Павло	7	6	9,5	5	2,5	2,5	9,5	8	2,5	2,5	55
Корольов Олександр	3	6	9,5	6	4	8	9,5	6	1,5	1,5	55
Добуток	21	36	90,25	30	10	20	90,25	48	3,75	3,75	353
1 ²	49	36	90,25	25	6,25	6,25	90,25	64	6,25	6,25	379,5
4 ²	9	36	90,25	36	16	64	90,25	36	2,25	2,25	382

$$p = \frac{10 * 353 - 55 * 55}{\sqrt{(10 * 379,5 - 55^2) * (10 * 382 - 55^2)}} = \frac{505}{782,4} = 0,645$$

Значення 0,645 вказує на досить високу позитивну лінійну залежність між думками експертів.

Отже, можна зробити висновок, що між думками експертів існує досить сильна позитивна кореляція. Це означає, що зі зростанням значень однієї змінної зазвичай зростають і значення іншої змінної, і навпаки, і цей зв'язок є високим.

Кореляцію думок двох інших експертів визначимо за допомогою критерія Спірмена (див. Табл. 2.5)

Табл. 2.5 – Критерій Спірмена

Експерти	Фактори									
	1	2	3	4	5	6	7	8	9	10
2	3	1	9,5	5	6,5	3	9,5	8	6,5	3
3	6	3	9,5	1	3	6	9,5	8	3	6
d=x-y	-3	-2	0	4	3,5	-3	0	0	3,5	-3
d ²	9	4	0	16	12,25	9	0	0	12,25	9

Тоді:

$$\sum_{1}^{t=10} d^2 = 9 + 4 + 0 + 16 + 12,25 + 9 + 0 + 0 + 12,25 + 9 = 71,5$$

$$R = 1 - \frac{6 \sum_{1}^{t=10} d^2}{10(10^2 - 1)} = 1 - \frac{6 \cdot 71,5}{10 \cdot 99} = 0,56$$

Значення 0,56 вказує на помірну позитивну зв'язок між рангами двох змінних.

Результати оцінки свідчать про середній рівень узгодженості думок експертів. Експерти відзначили задовільний рівень кібербезпеки за більшістю критеріїв, однак є потреба в удосконаленні систем виявлення та реагування на загрози, а також в підвищенні рівня автоматизації безпеки. Рекомендується проводити регулярне навчання персоналу, оновлювати політики безпеки та впроваджувати сучасні технології для покращення загального рівня захисту підприємства в кіберпросторі.

Варто розуміти, що це не єдиний спосіб оцінки рівня економічної безпеки в кіберпросторі. В першому розділі були описані декілька із них.

2.2 Ідентифікація основних кіберзагроз для економічної безпеки підприємств

Для початку потрібно визначитись із визначенням поняття кіберзагроз, саме це є ключем для розуміння питання.

Кіберзагрози - це потенційні небезпеки, що загрожують комп'ютерним системам, мережам або даним організацій. Вони можуть включати крадіжку приватних даних, інтелектуальної власності, конфіденційних бізнес-планів, а також порушення роботи критичних ІТ-систем. Кіберзагрози здійснюються через несанкціонований доступ або атаки на інформаційні ресурси з метою отримання вигоди або досягнення політичних цілей. До таких загроз можуть відноситися як організовані злочинні групи, так і національні військові кібервідділи, які використовують кібер-атаки як операційну стратегію[16].

Сучасні кіберзагрози є все більш складними та різноманітними. Останні роки стали свідками значних інцидентів, таких як атаки з використанням рансомвару

WannaCry та NotPetya, які завдали значної шкоди компаніям у всьому світі. Атака на ланцюги постачання через вразливості в програмному забезпеченні SolarWinds продемонструвала, наскільки вразливими можуть бути навіть найбільші компанії.

Ефективна ідентифікація кіберзагроз вимагає використання різних методів збору та аналізу інформації. Моніторинг мережевого трафіку, аналіз логів серверів та мережевого обладнання, а також використання інструментів розвідки загроз дозволяють виявити потенційні загрози на ранніх стадіях. Інструменти, такі як SIEM-системи (Splunk, IBM QRadar), антивірусні програми (Symantec, McAfee) та системи виявлення вторгнень (Snort, Suricata), забезпечують необхідні засоби для ефективного управління кібербезпекою.

Оцінка ризиків кіберзагроз включає визначення ймовірності їх виникнення та потенційних збитків для підприємства. Використання моделей оцінки ризиків, таких як якісна та кількісна оцінка, дозволяє визначити найбільш критичні загрози та розробити відповідні заходи для їх мінімізації. Кількісні моделі, засновані на статистичних даних та математичних розрахунках, забезпечують більш точну оцінку ризиків та допомагають у прийнятті обґрунтованих рішень.

Кіберзагрози можна класифікувати за різними критеріями. Ось декілька основних категорій:

- За типом атаки: Можна виділити кілька типів атак, таких як шкідливе програмне забезпечення (malware), фішинг, атаки типу "людина посередині" (MitM), атаки на відмову в обслуговуванні (DDoS), та ін'єкційні атаки (SQL injection).
- За метою атаки: Наприклад, крадіжка даних, шантаж (ransomware), викрадення облікових даних (credential harvesting), або саботаж.
- За джерелом загрози: Внутрішні загрози (інсайдери), зовнішні загрози (хакери, конкуренти), або національно-державні актори.

Поточні кіберзагрози є дуже різноманітними і складними. Наприклад, ботнети використовуються для здійснення DDoS-атак, тоді як ransomware блокує доступ до даних, вимагаючи викуп за їх розблокування. Інші загрози включають фішинг, який

часто використовується для крадіжки облікових даних, та атаки на ланцюги постачання, де шкідливий код вводиться на стадії розробки програмного забезпечення.

Для оцінки рівня економічної безпеки підприємства в кіберпросторі важливо ідентифікувати ті кіберзагрози, які становлять найбільшу небезпеку для фінансової стабільності та безперервності бізнес-процесів тому варто зупинитися детальніше на класифікації існуючих кіберзагроз.

Перший з відомих нам кіберзагроз – це Ransomware (Шантаж). Стаття "Ransomware Evolution, Target and Safety Measures" надає детальний огляд еволюції, цілей та заходів безпеки, пов'язаних із шкідливим програмним забезпеченням типу ransomware[17]. Ransomware - це тип шкідливого програмного забезпечення, яке блокує доступ до даних жертви шляхом їх шифрування або блокує доступ до комп'ютерної системи. Зловмисники вимагають викуп за розблокування даних або системи. Еволюція ransomware розпочалася з AIDS Trojan у 1989 році і досягла свого піку в останні роки з такими відомими варіантами, як CryptoLocker, WannaCry та NotPetya.

Crypto-Ransomware шифрує файли на комп'ютері жертви і вимагає викуп за ключ розшифрування, тоді як Locker-Ransomware блокує доступ до комп'ютера, не шифруючи файли, але забороняючи доступ до системи.

Ransomware спрямоване на різні типи користувачів та систем. Індивідуальні користувачі часто стають мішенню через свою меншу обізнаність про заходи безпеки і схильність до оплати викупу. Корпоративні мережі є привабливою мішенню через цінність збережених даних і готовність компаній платити викуп для відновлення доступу до критично важливої інформації. Атаки на медичні установи, поліцію та інші екстрені служби можуть мати катастрофічні наслідки, що змушує їх швидше платити викуп.

Серед відомих випадків атак можна виділити Hollywood Presbyterian Medical Center, який у лютому 2016 року був атакований Locky ransomware, що паралізувало

його роботу на два тижні. У травні 2017 року WannaCry вразив понад 200 000 комп'ютерів у більш ніж 150 країнах, використовуючи вразливість в ОС Windows.

Для захисту від ransomware рекомендується регулярно створювати резервні копії даних, встановлювати останні оновлення для операційних систем та програмного забезпечення, використовувати якісне антивірусне програмне забезпечення та навчати працівників розпізнавати фішингові атаки та інші загрози.

Далі варто розглянути такий клас кіберзагроз як Phishing (Фішинг).

Фішинг визначається як кримінальна діяльність, що використовує техніки соціальної інженерії для незаконного отримання конфіденційної інформації, такої як логіни і паролі, обманом користувачів через фальшиві вебсайти або електронні листи.

Фішинг є однією з найорганізованіших форм кіберзлочинності XXI століття. Зловмисники розсилають підроблені електронні листи або створюють фальшиві вебсайти, що імітують легітимні ресурси, щоб обманом змусити користувачів надавати свою конфіденційну інформацію. Це може включати особисті дані, банківську інформацію або логіни до різних сервісів. Фішинг постійно еволюціонує, стаючи дедалі складнішим і важчим для виявлення.

Основні методи фішингу включають:

- Spear-phishing: Цільові атаки на конкретних осіб або організації з використанням персоналізованих повідомлень для підвищення ефективності атак.
- Pharming: Використання шкідливого коду, такого як віруси або трояни, для зміни налаштувань DNS і перенаправлення користувачів на фальшиві вебсайти.
- Social Phishing: Використання інформації з соціальних мереж для створення більш переконливих фішингових атак.

Сучасні фішингові атаки стали настільки витонченими, що можуть імітувати легітимні вебсайти та електронні листи, включаючи логотипи і графічні елементи, що робить їх дуже переконливими. Наприклад, згідно з Forbes, фішингові атаки призводять до втрат у розмірі близько \$500 млн на рік тільки для американських бізнесів.

Рішення для боротьби з фішингом

Для захисту від фішингових атак пропонується трирівневий підхід:

- Запобігання фішингу: Використання чорних списків для блокування фішингових сайтів або фільтрації фішингових електронних листів. Це може бути досягнуто за допомогою технологій машинного навчання, що аналізують URL-адреси та вміст листів для виявлення фішингових ознак.
- Виявлення фішингу: Встановлення індикаторів безпеки у веббраузерах, що попереджають користувачів про потенційно небезпечні сайти. Активні індикатори, такі як поп-апи, значно ефективніші, ніж пасивні.
- Навчання користувачів: Впровадження навчальних програм та ігор, що допомагають користувачам розпізнавати фішингові атаки. Наприклад, система вбудованого навчання може надсилати користувачам фальшиві фішингові електронні листи для навчання в реальних умовах[19].

Третій із найбільш поширених класів кіберзагроз – це Malware (Шкідливе програмне забезпечення)

Malware (шкідливе програмне забезпечення) - це загальний термін для всіх типів шкідливих програм, які використовуються з метою порушення політики безпеки комп'ютерної системи стосовно конфіденційності, цілісності або доступності даних.

Malware включає різні типи шкідливих програм, зокрема віруси, черви, троянські коні, логічні бомби, та інші. Віруси поширюються шляхом вбудовування своїх копій у файли, які передаються на інші комп'ютери. Черви поширюються через мережі без необхідності інфікування файлів. Троянські коні приховані в програмах, які на вигляд мають корисні функції, але насправді виконують шкідливі дії.

Основні методи захисту від malware включають використання антивірусного програмного забезпечення, яке здійснює сканування та виявлення шкідливого коду за допомогою підписів (signature-based detection) та поведінкового аналізу (behavioral

analysis). Підписове виявлення полягає у пошуку відомих шаблонів шкідливого коду, тоді як поведінковий аналіз контролює діяльність програм для виявлення підозрілої поведінки.

Методи шифрування та поліморфізму, які використовуються для маскування шкідливого коду від антивірусних програм. Шифрування приховує код вірусу, використовуючи різні ключі шифрування, тоді як поліморфізм дозволяє вірусу змінювати свою форму, зберігаючи при цьому свою функціональність[19].

Оскільки класифікація кіберзагроз досить велика, наступні класи будуть описані трохи коротше.

Man-in-the-Middle (MitM) атаки. Man-in-the-Middle (MitM) атака є одним з найбільш небезпечних видів кіберзагроз, які можуть суттєво вплинути на безпеку інформаційних систем підприємств. Цей тип атак дозволяє зловмиснику перехоплювати, змінювати і контролювати комунікацію між двома сторонами, які вважають, що спілкуються безпосередньо між собою.

Суть MitM атак

MitM атака включає два основні етапи: перехоплення та дешифрування. Під час перехоплення зловмисник встановлює своє положення в каналі комунікації між двома сторонами, що дозволяє йому перехоплювати всі передані дані. Після цього, зловмисник може дешифрувати ці дані для отримання конфіденційної інформації.

Перехоплення є першим етапом MitM атаки. Зловмисник може використовувати різні методи для перехоплення даних:

- IP spoofing: зловмисник змінює IP-адресу, видаючи себе за інший додаток або користувача.
- ARP spoofing: зловмисник зв'язує свою MAC-адресу з IP-адресою законного користувача в локальній мережі, що дозволяє перехоплювати дані, що надсилаються на цю IP-адресу.
- DNS spoofing: зловмисник змінює записи DNS, перенаправляючи користувачів на свій сайт замість законного.

Дешифрування

Після перехоплення зловмисник повинен дешифрувати захищені дані, щоб отримати доступ до конфіденційної інформації. Це можна зробити різними способами:

- HTTPS spoofing: зловмисник надсилає підроблений сертифікат на браузер жертви, що дозволяє йому перехоплювати та дешифрувати дані.
- SSL hijacking: зловмисник підміняє ключі аутентифікації під час TCP handshake, встановлюючи контроль над сеансом зв'язку.
- SSL stripping: зловмисник знижує рівень захищеного з'єднання HTTPS до незахищеного HTTP, перехоплюючи всі дані, що передаються.

Класична MitM атака

Зловмисник перехоплює дані, створюючи ілюзію прямого зв'язку між двома сторонами, в той час як всі дані проходять через нього.

Man-in-the-Browser (MitB) атака

Зловмисник встановлює шкідливе ПЗ на комп'ютер жертви, яке інтегрується в браузер і перехоплює всі дані, що передаються між жертвою і веб-сайтами.

Захист від MitM атак

Для захисту від MitM атак важливо впроваджувати наступні заходи:

Використання шифрування: Впровадження протоколів шифрування, таких як TLS/SSL, для захисту даних[23].

Denial-of-Service (DoS) та Distributed Denial-of-Service (DDoS) атаки Ці атаки націлені на перевантаження об'єкта атаки величезною кількістю запитів, що призводить до зниження продуктивності або повного припинення надання послуг легітимним користувачам.

Суть DDoS атак

DDoS атаки полягають у використанні множинних скомпрометованих комп'ютерів, які спільно атакують ціль. Ці комп'ютери, також відомі як "зомбі", об'єднуються в ботнет під контролем зловмисника. Атака виконується шляхом надсилання величезної кількості трафіку на цільовий сервер, що призводить до вичерпання його ресурсів.

Основні види DDoS атак:

Flooding атаки: Зловмисники використовують велику кількість запитів для перевантаження мережесих ресурсів. Найпоширенішими є TCP, UDP і ICMP flood атаки.

Атаки на вразливості: Використовують специфічні вразливості в протоколах, таких як HTTP або TCP, для зниження продуктивності сервера.

Принципи дії DDoS атак

DDoS атаки зазвичай виконуються в два етапи:

Впровадження зловмисного ПЗ: Зловмисник впроваджує шкідливе програмне забезпечення на вразливі комп'ютери, перетворюючи їх на зомбі.

Атака на ціль: Зомбі-комп'ютери починають одночасно надсилати запити до цільового сервера, що призводить до перевантаження його ресурсів і зниження продуктивності або повної недоступності сервера.

Вплив DDoS атак

DDoS атаки можуть мати значні фінансові та операційні наслідки для підприємств.

Захист від DDoS атак

Захист від DDoS атак є складним завданням, яке вимагає комплексного підходу:

Попередження атак: Впровадження заходів безпеки, таких як фільтри трафіку і розподіл навантаження.

Виявлення атак: Використання систем моніторингу та аналізу трафіку для виявлення аномалій.

Міграція атак: Використання хмарних сервісів для розподілу навантаження та запобігання перевантаженню серверів[24].

Візуалізація DDoS-атаки – див Рис. 2.1

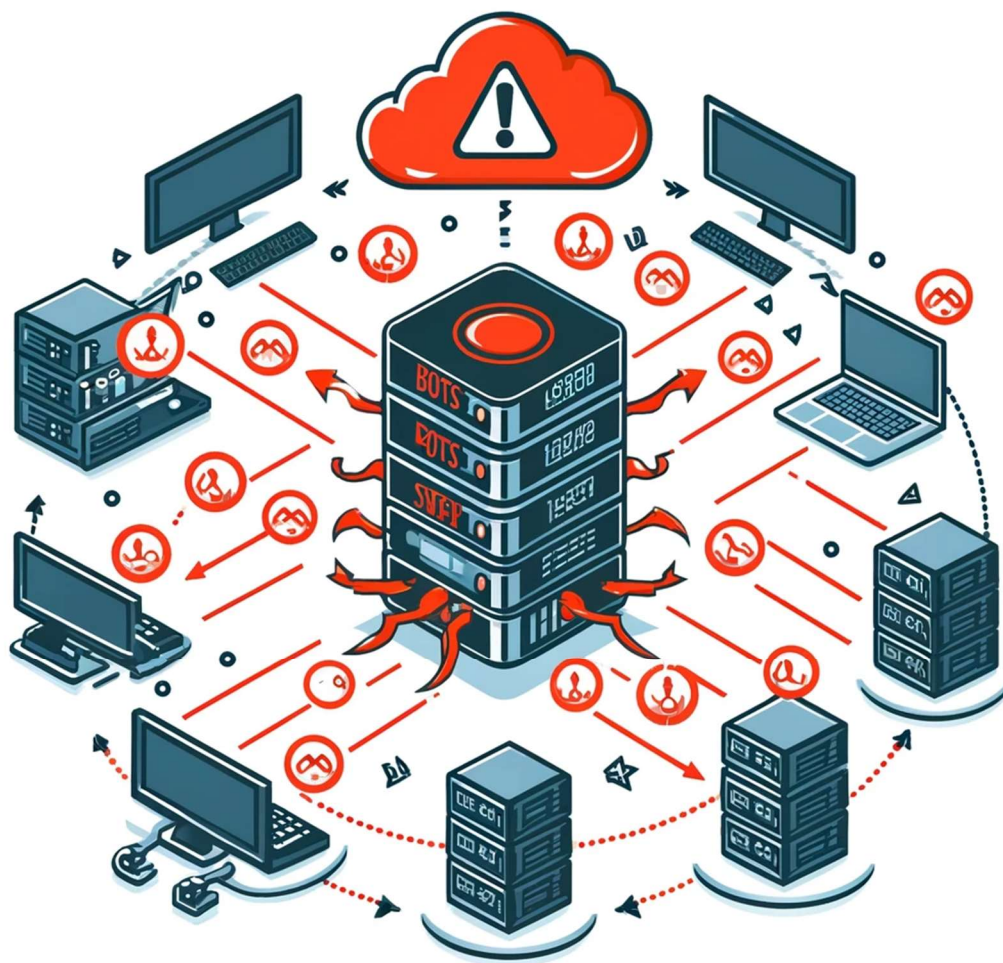


Рис. 2.1 – Логіка роботи DDoS-атаки

Credential Harvesting (Викрадення облікових даних).

Credential harvesting (викрадення облікових даних) є методикою, що використовується зловмисниками для збору імен користувачів та паролів, зазвичай через використання підроблених вебсайтів. Мета цієї техніки полягає в накопиченні якомога більшої кількості комбінацій імен користувачів і паролів, які потім можуть бути продані або використані для компрометації організацій.

Основні методи викрадення облікових даних

- Використання підроблених доменів. Зловмисники створюють фальшиві вебсайти, які виглядають як легітимні, для того, щоб обманом змусити користувачів вводити свої облікові дані. Наприклад, зловмисники можуть створювати домени, що імітують відомі компанії або служби, такі як Office

365. Користувачі, які потрапляють на ці сайти, вводять свої облікові дані, які потім зберігаються зловмисниками.

- Фішингові електронні листи. Зловмисники розсилають фішингові електронні листи, які містять посилання на фальшиві вебсайти. Ці листи можуть виглядати як повідомлення від відомих компаній або служб підтримки. Після натискання на посилання користувачі перенаправляються на фальшиві сайти, де вони вводять свої облікові дані.

Приклад атаки

Технологія Trinity Cyber недавно запобігла спробі викрадення облікових даних в кількох мережах клієнтів. Зловмисники намагалися зібрати дійсні облікові дані Office 365, використовуючи підроблені домени, такі як umcart[.]cloud і viveripa[.]com. Вони надсилали фішингові листи з посиланнями на ці домени, змушуючи користувачів вводити свої дані на підроблених сторінках Office 365. Технологія Trinity Cyber змогла розпізнати та запобігти цій діяльності, видаляючи шкідливий JavaScript код із мережевого трафіку клієнтів[25].

Захист від викрадення облікових даних

- Використання багатофакторної аунтифікації
- Освіта та навчання персоналу
- Використання технологій захисту

Для більш детального ознайомлення із усіма вище наведеними класами– див. [20]

2.3 Оцінка ефективності існуючих заходів безпеки.

В сучасних умовах цифрової трансформації підприємства стикаються з численними кіберзагрозами, які можуть негативно вплинути на їх економічну безпеку. Для мінімізації цих загроз підприємства впроваджують різноманітні заходи кібербезпеки. Однак важливо не лише впроваджувати ці заходи, але й регулярно оцінювати їх ефективність, щоб забезпечити максимальний рівень захисту.

Один із найцікавіших методів оцінювання – це ключові показники ефективності (KPI). KPI є метриками, що дозволяють оцінити ефективність заходів безпеки.

Ключові показники ефективності (KPI) є критично важливими для оцінки ефективності заходів безпеки в будь-якій організації. Правильно розроблені KPI

допомагають відстежувати прогрес у досягненні цілей безпеки, виявляти слабкі місця та приймати обґрунтовані рішення для покращення кібербезпеки.

Основні KPI для оцінки ефективності заходів безпеки

Кількість інцидентів безпеки

Відстеження кількості кіберінцидентів, що сталися за певний період, дозволяє оцінити загальний стан безпеки підприємства. Зменшення кількості інцидентів свідчить про ефективність впроваджених заходів. Інциденти безпеки можуть включати зломи, втрати даних, атаки на мережу та інші форми порушень.

Час реагування на інциденти (MTTR)

Середній час, необхідний для виявлення, аналізу та усунення інциденту, є критично важливим показником. Чим коротший цей час, тим швидше підприємство може відновити нормальну роботу та мінімізувати збитки від інциденту. Показник MTTR допомагає оцінити оперативність роботи команд безпеки та ефективність існуючих процесів реагування.

Рівень усунення вразливостей

Відсоток виявлених вразливостей, які були успішно усунуті за певний період, дозволяє оцінити ефективність управління вразливостями. Високий відсоток усунених вразливостей свідчить про проактивний підхід до кібербезпеки та здатність підприємства запобігати потенційним загрозам.

Кількість виявлених та заблокованих загроз

Цей показник включає кількість шкідливих програм, фішингових атак та інших загроз, які були виявлені та заблоковані за певний період. Висока кількість виявлених та заблокованих загроз може свідчити про ефективність систем виявлення та запобігання загрозам (IDS/IPS), а також антивірусних програм.

Вартість кіберінцидентів

Оцінка прямих та непрямих фінансових втрат від кіберінцидентів допомагає зрозуміти економічний вплив загроз на підприємство. Цей показник може включати витрати на відновлення даних, виплату штрафів, втрату доходів через простої, а також витрати на репутаційні збитки.

Рівень задоволеності користувачів безпекою

Збір відгуків від співробітників щодо їхнього задоволення існуючими заходами безпеки може допомогти виявити проблеми, які не завжди видно з технічної точки зору. Анкети та опитування дозволяють зрозуміти, наскільки працівники обізнані про політики безпеки та наскільки вони довіряють існуючим заходам.

Частота навчання персоналу

Регулярне проведення навчань з кібербезпеки та їх вплив на обізнаність співробітників про поточні загрози є важливим КРІ. Висока частота навчань і позитивні результати опитувань після навчань свідчать про ефективність програм навчання та підвищення загального рівня кібербезпеки на підприємстві.

Використання ключових показників ефективності (КРІ) дозволяє підприємствам систематично оцінювати ефективність своїх заходів безпеки, визначати області для покращення та приймати обґрунтовані рішення щодо захисту від кіберзагроз. Регулярний моніторинг та аналіз КРІ сприяє підвищенню рівня економічної безпеки та стабільності підприємства в умовах цифрової трансформації.

Методика оцінки ризиків

Оцінка ризиків є систематичним процесом управління ризиками, що дозволяє виявляти, аналізувати та мінімізувати ризики, пов'язані з різними загрозами. Цей процес допомагає підприємствам зрозуміти та управляти ризиками, пов'язаними з їх діяльністю, зокрема в умовах кіберзагроз.

Основні етапи оцінки ризиків

Ідентифікація ризиків

Цей етап включає виявлення всіх потенційних загроз, які можуть вплинути на підприємство. Це може бути здійснено шляхом аналізу даних, фізичної оцінки об'єктів, інтерв'ю з працівниками та використання таких методів, як мозковий штурм та бенчмаркінг з іншими компаніями. Типові загрози включають фізичні, хімічні, біологічні, механічні, ергономічні та психо-соціальні ризики.

Аналіз ризиків

Після ідентифікації ризиків, необхідно провести аналіз для визначення того, хто може постраждати та як саме. Це включає оцінку ймовірності виникнення та серйозності наслідків кожного ризику. Аналіз може бути кількісним (з використанням числових значень для вимірювання ризиків) або якісним (залежить від досвіду та думки оцінювачів ризиків).

Оцінка ризиків

Оцінка включає встановлення пріоритетності ризиків для подальших дій. Це може бути здійснено шляхом призначення числових значень для ймовірності та серйозності ризику, що дозволяє створити рейтинг ризиків. На цьому етапі також визначаються поточні заходи контролю та оцінюється їх ефективність.

Впровадження заходів контролю

Після оцінки ризиків необхідно розробити та впровадити заходи контролю для мінімізації ризиків. Заходи контролю можуть включати інженерні рішення, адміністративні заходи, засоби індивідуального захисту та зміни в робочих процесах. Заходи повинні бути спрямовані на усунення або зменшення ризиків до прийняттого рівня.

Моніторинг та перегляд

Оцінка ризиків не є одноразовим процесом. Після впровадження заходів контролю необхідно регулярно проводити моніторинг та перегляд ризиків, особливо після значних змін у процесах або після виникнення інцидентів. Це дозволяє забезпечити актуальність та ефективність заходів безпеки.

Очікування від оцінки ризиків

Процес оцінки ризиків повинен бути систематичним, ретельним, структурованим, повторюваним та консультативним. Результати оцінки мають бути обґрунтованими та піддаватись аудиту. Важливо, щоб оцінка ризиків враховувала всі аспекти робочої діяльності, включаючи організацію роботи, значні загрози та ризики, а також заходи контролю для їх мінімізації[21].

Зворотній зв'язок і навчання персоналу

Залучення персоналу до процесу забезпечення кібербезпеки є критично важливим для ефективного захисту підприємства від кіберзагроз. Регулярне навчання та зворотній зв'язок допомагають підвищити обізнаність співробітників про поточні загрози та методи їх розпізнавання і запобігання.

Навчання співробітників

Регулярні тренінги з кібербезпеки допомагають підвищити обізнаність співробітників про поточні загрози та методи їх розпізнавання і запобігання. Темі тренінгів можуть включати фішинг, використання сильних паролів, розпізнавання соціальної інженерії тощо. Комп'ютеризовані навчальні технології є важливими для проведення практичних тренінгів з кібербезпеки. Вони створюють середовища, які імітують реалістичну IT-інфраструктуру для навчання. Під час тренінгу учасники використовують різні програмні інструменти для виконання атакуючих або захисних дій. Використання цих інструментів генерує дані, які можна використовувати для підтримки навчання.

Анкети та опитування

Проведення анкетування та опитувань серед співробітників для оцінки їхньої обізнаності про кібербезпеку та ефективність проведених навчальних заходів є ключовим елементом зворотнього зв'язку. Результати опитувань можуть допомогти

виявити прогалини в знаннях і визначити необхідність додаткового навчання. Автоматизовані системи зворотнього зв'язку, засновані на даних, зібраних під час навчання, можуть надавати персоналізовані відгуки про виконані дії. Ці відгуки включають аналіз помилок, графіки прогресу, аналіз відповідності та хронологію діяльності.

Автоматизована зворотній зв'язок

Автоматизована зворотній зв'язок є ефективною для підтримки процесу навчання. Наприклад, системи зворотнього зв'язку, які аналізують дані командного рядка, дозволяють надавати учасникам навчання детальний аналіз їхніх дій, виявлення помилок та рекомендації для покращення. Такий підхід дозволяє навчальним закладам та інструкторам краще розуміти потреби студентів і адаптувати навчання до їх потреб.

Залучення співробітників до процесу забезпечення кібербезпеки та надання їм регулярного та автоматизованого зворотнього зв'язку є ключовими елементами ефективного управління кібербезпекою. Це допомагає підвищити обізнаність та підготовленість персоналу, що, в свою чергу, сприяє підвищенню рівня економічної безпеки підприємства в умовах кіберзагроз.

РОЗДІЛ 3

СТРАТЕГІЇ ТА МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ В КІБЕРПРОСТОРІ

3.1 Рекомендацій щодо підвищення рівня економічної безпеки підприємств у кіберпросторі

Попри зростання суспільного резонансу та розкриття масштабних кіберзагроз, бізнес все ще недостатньо фінансує кібербезпеку, що призводить до значних фінансових втрат. Якщо для великих компаній кіберзагрози означають великі збитки, то для середніх та малих підприємств ці загрози можуть поставити під загрозу їхнє існування. Відсутність стратегій розвитку підприємств на випадок кіберзагроз підкреслює необхідність пошуку нових методів захисту інформаційної інфраструктури як основного принципу обліково-аналітичного забезпечення управління економічною безпекою. Тому у цьому підрозділі будуть розглянуті основні рекомендації, спрямовані на підвищення рівня економічної безпеки підприємств в умовах кіберпростору. Рекомендації базуються на аналізі сучасних кіберзагроз проведених в попередніх розділах та методів їх запобігання і включають наступні аспекти:

1. Впровадження багатофакторної аутентифікації (MFA)
2. Освіта та навчання персоналу
3. Використання та розробка сучасних технологій захисту
4. Регулярні аудити та перевірки безпеки
5. Створення груп реагування на інциденти (CSIRT)
6. Використання стандартів та найкращих практик
7. Шифрування даних

Даний список рекомендацій був сформований на основі аналізу джерел в першому розділі, а також враховуючи класифікації кібератак та враховуючи усі наслідки, які вони за собою несуть. Варто розуміти, що лише багатофакторна аутентифікація, яка вимагає від користувачів введення додаткового коду або використання фізичного токена для доступу до системи не дасть остаточного захисту від кібер атак, хоча це значно ускладнить зловмисникам доступ до облікових записів, навіть якщо вони мають правильні логіни і паролі, не дасть повного захисту від кібератак та загроз. Ці заходи можуть працювати поодиночі, але при цьому поєднання цих методик дасть змогу захистити кіберпростір компанії.

Кожна із запропонованих вище рекомендацій спрямована на запобігання якогось типу атак, для прикладу багатофакторна аутентифікація допомагає запобігти

викраденню облікових даних та фішингу, але при цьому ніяк не допомагає проти DDoS-атак. Використання міжнародних стандартів, таких як ISO 27001 та ISO 27005, є важливим кроком для підприємств у забезпеченні ефективного управління кібербезпекою. ISO 27001 встановлює вимоги до системи управління інформаційною безпекою (СУІБ), допомагаючи організаціям створити структуру, яка захищає їхні інформаційні активи. Цей стандарт забезпечує систематичний підхід до управління ризиками, включаючи розробку політик та процедур, оцінку ризиків і впровадження відповідних заходів безпеки.

ISO 27005, як доповнення до ISO 27001, надає детальні рекомендації щодо управління ризиками інформаційної безпеки. Він допомагає організаціям ідентифікувати, аналізувати та мінімізувати ризики, забезпечуючи безпеку їхньої інформації. Використання ISO 27005 дозволяє підприємствам впроваджувати ефективні заходи для зменшення ймовірності кіберінцидентів та їхніх потенційних наслідків.

Найкращі практики, такі як NIST Cybersecurity Framework, також є важливим інструментом для підприємств. Цей фреймворк розроблений Національним інститутом стандартів і технологій США і включає п'ять основних функцій: ідентифікація, захист, виявлення, реагування та відновлення. Він надає рекомендації та інструменти для покращення кібербезпеки, допомагаючи організаціям розуміти контекст своїх інформаційних активів, впроваджувати заходи захисту, виявляти кіберінциденти, ефективно реагувати на них та швидко відновлюватися після атак.

Впровадження цих стандартів і найкращих практик допомагає організаціям створити систематичний підхід до забезпечення кібербезпеки, мінімізуючи ризики та захищаючи інформаційні активи від кіберзагроз. Це дозволяє підприємствам бути більш підготовленими до можливих атак, зменшувати фінансові втрати і забезпечувати безперервність бізнес-процесів[27].

Шифрування даних ж в свою чергу не дасть змогу отримати доступ до даних зловмисникам, навіть, якщо вони зможуть проникнути в систему і витягти якісь важливі для бізнесу моменти. Якщо ж все таки 6 із наведених пунктів не дали результату, завжди повинні бути групи швидкого реагування на інциденти у кіберсвіті.

Формування груп реагування на інциденти з кібербезпеки (CSIRT) дозволяє швидко реагувати на інциденти, зменшуючи їхній вплив на діяльність підприємства. Ці групи повинні мати чітко визначені процедури реагування та постійно тренуватися на випадок виникнення реальних загроз.

CSIRT відповідає за виявлення та моніторинг інцидентів кібербезпеки. Це включає використання інструментів для збору, аналізу та кореляції даних з різних

джерел, таких як системи виявлення вторгнень (IDS), антивірусне програмне забезпечення, лог-файли та інші засоби моніторингу мережі.

Після виявлення інциденту CSIRT проводить оцінку його критичності та впливу на підприємство. Оцінка включає аналіз вразливостей, які були використані, тип атаки та можливі наслідки для організації. Це дозволяє визначити пріоритети для реагування.

CSIRT розробляє та впроваджує заходи для реагування на інциденти. Це може включати ізоляцію уражених систем, знищення шкідливого програмного забезпечення, відновлення систем з резервних копій та впровадження тимчасових або постійних рішень для запобігання повторення інциденту.

Важливою частиною роботи CSIRT є також комунікація з іншими підрозділами підприємства, а також з зовнішніми організаціями, такими як постачальники послуг, регуляторні органи та інші зацікавлені сторони. Це забезпечує координацію дій та обмін інформацією для більш ефективного реагування на інциденти.

Регулярні навчання та тренування для членів CSIRT є необхідними для підтримки їхньої готовності до реагування на реальні загрози. Це включає симуляції інцидентів, аналіз минулих інцидентів та обговорення кращих практик. Навчання дозволяють команді відпрацьовувати процедури реагування та виявляти можливі слабкі місця в процесах.

Формування ефективної CSIRT допомагає підприємству зменшити ризики та втрати від кіберінцидентів, забезпечуючи безперервність бізнесу та захист важливих інформаційних ресурсів[28].

Отже, у підсумку можна сказати, що підприємствам усіх рівнів потрібно приділяти більше уваги фінансування кібербезпеки. Це єдине правильне рішення, яке в майбутньому буде приносити виключно прибуток. Для прикладу можна взяти нещодавній інцидент із телекомунікаційною компанією-оператором «Київстар», яка внаслідок нехтуванням фінансування відділу кібербезпеки та недостатньої уваги до кібератак понесла неймовірні збитки у розмірі «мільярдів гривень» і подальших витрат на відновлення інфраструктури, адже зуйновано близько 40% усієї інфраструктури, та маркетингові кампанії для повернення клієнтської бази. Тому потрібно значно збільшувати фінансування відділів кібербезпеки на усіх рівнях і при цьому завжди зберігати комплексний підхід до кібербезпеки. Інтеграція цих заходів допоможе підприємствам мінімізувати ризики, забезпечити захист інформаційних активів і забезпечити безперервність бізнес-процесів.

Окрім оглянутих в роботі моделей оцінювання рівня економічної безпеки підприємства в кіберпросторі варто звернути увагу саме на математичні моделі прогнозування, такі як регресійні моделі, моделі часових рядів, стохастичні моделі, імітаційні моделі.

Регресійний аналіз дозволяє встановлювати залежності між показниками економічної безпеки та факторами, що на них впливають. Наприклад, можна визначити, як збільшення інвестицій у кібербезпеку впливає на зменшення фінансових втрат від кіберінцидентів.

Моделювання часових рядів дозволяє прогнозувати зміни в рівні економічної безпеки на основі історичних даних. Це може включати прогнозування кількості кіберінцидентів або фінансових втрат у майбутньому.

Стохастичні моделі використовуються для оцінки ризиків і визначення ймовірності настання різних кіберзагроз. Це дозволяє підприємствам розробляти стратегії для мінімізації ризиків і підготовки до можливих інцидентів.

Імітаційні моделі дозволяють тестувати різні сценарії і оцінювати їх вплив на економічну безпеку. Наприклад, можна моделювати вплив різних рівнів інвестицій у кібербезпеку на фінансові результати підприємства.

Математичні моделі є дуже потужним інструментом для аналізу та прогнозування рівня економічної безпеки підприємства. Вони дозволяють оцінювати поточний стан безпеки, виявляти потенційні загрози і розробляти ефективні стратегії для їх мінімізації. Використання таких моделей допомагає підприємствам бути більш підготовленими до кіберзагроз і забезпечувати безперервність бізнес-процесів.

Інтеграційна методика оцінювання економічної безпеки підприємства дозволяє систематизувати процес управління ризиками та забезпечити комплексний підхід до захисту інформаційних ресурсів. Впровадження такої методики сприяє підвищенню рівня безпеки та стабільності підприємства, знижуючи ймовірність фінансових втрат від кіберінцидентів.

Першим кроком є визначення контексту та мети оцінювання економічної безпеки. Це включає ідентифікацію основних активів підприємства, які потребують захисту, а також визначення критичних бізнес-процесів. Важливо врахувати специфіку галузі та регуляторні вимоги. Для ідентифікації та аналізу ризиків можна здійснити за допомогою SWOT-аналізу, методу FMEA (аналізу видів та наслідків відмов) або використання матриці ризиків. Важливо оцінити ймовірність настання ризиків та їх вплив на підприємство. Після цього варто перейти до оцінки вразливостей та загроз які можуть бути використані зловмисниками для здійснення атак. Це включає аналіз технічних, організаційних та людських факторів. Важливо визначити найбільш критичні вразливості та розробити плани їх усунення. А на

основі вже отриманих даних розробляти та впроваджувати заходи контролю та захисту. Це можуть бути технічні заходи (встановлення антивірусного ПЗ, системи виявлення вторгнень), організаційні заходи (розробка політик безпеки, навчання персоналу) та адміністративні заходи (створення груп реагування на інциденти). Впровадження інтеграційної методики оцінювання економічної безпеки дозволяє підприємствам забезпечити комплексний підхід до управління ризиками та захисту інформаційних активів. Використання міжнародних стандартів та найкращих практик, регулярні аудити та навчання персоналу сприяють підвищенню рівня безпеки та стабільності підприємства.

3.2 Огляд можливостей економіко-математичного моделювання та прогнозування рівня економічної безпеки підприємства

У попередньому підрозділі були розглянуті рекомендації, щодо підвищення рівня економічної безпеки в підприємстві, у тому числі і економіко-математичні методи, які дають змогу оцінювати рівень загроз у кіберпросторі. Такі математичні моделі як регресійні є незамінним інструментом для розуміння взаємозв'язків між різними змінними та прогнозування майбутніх показників. Вони допомагають виявити, як певні фактори, такі як витрати на кібербезпеку, впливають на економічну безпеку підприємства. Такий аналіз також корисний для оцінки ефективності різних заходів безпеки. Наприклад, можна порівняти різні сценарії інвестування і побачити, який з них приносить найкращі результати у вигляді зменшення втрат. Це дозволяє не тільки економити ресурси, але й забезпечити максимальний захист від кіберзагроз.

Окрім цього, аналізуючи історичні дані, регресійні моделі допомагають виявити тенденції, які можуть бути корисними для передбачення майбутніх кіберзагроз. Це особливо важливо для підприємств, які хочуть бути на крок попереду потенційних загроз.

Іншими словами, регресійний аналіз не лише дає змогу передбачити, як зміняться фінансові показники в залежності від інвестицій у кібербезпеку, але й допомагає оптимізувати ці витрати, виявити критичні точки та прийняти обґрунтовані рішення для забезпечення максимальної економічної безпеки. Власне саме тому, я і обрав цей метод економіко-математичного прогнозування для демонстрації впливу витрат на кібербезпеку на зменшення фінансових втрат від кіберзагроз.

Першим ділом, потрібно зібрати дані, на основі яких буде проводитись аналіз і прогнозування. За базу до цих даних я використав дані, які отримав під час проходження практики. У наведеній нижче таблиці (див. Табл. 3.1)

X – незалежна змінна, що демонструє річні витрати на кібербезпеку (у тис. грн.).
 Y – незалежна змінна, що демонструє річні збитки від кіберзагроз

Табл. 3.1 – Дані потрібні для регресійного аналізу

Рік	Витрати на кібербезпеку (X) у тис. грн.	Збитки від кіберзагроз (Y) у тис. Грн.
2013	30	50
2014	35	45
2015	40	40
2016	45	35
2017	50	30
2018	55	25
2019	60	20
2020	65	15
2021	70	10
2022	75	5

Таблиця сформована на основі даних отриманих під час проходження переддипломної практики

Для початку потрібно побудувати просту лінійну регресію для визначення залежності між витратами на кібербезпеку (X) та фінансовими збитками від кіберзагроз (Y). Лінійна регресійна модель має наступний вигляд:

$$Y = a + bX$$

Для обчислення параметрів моделі використаємо метод найменших квадратів для знаходження значень параметрів a та b . Процес обчислення виглядає наступним чином :

$$\bar{X} = \frac{1}{n} \sum_{i=1}^n X_i = \frac{30 + 35 + 40 + 45 + 50 + 55 + 60 + 65 + 70 + 75}{10} = 52,5$$

$$\bar{Y} = \frac{1}{n} \sum_{i=1}^n Y_i = \frac{50 + 45 + 40 + 35 + 30 + 25 + 20 + 15 + 10 + 5}{10} = 27,5$$

Коефіцієнт нахилу (b) у регресійному аналізі відіграє ключову роль у розумінні взаємозв'язку між незалежною змінною (предиктором) та залежною змінною (відгуком). Його розрахунок та інтерпретація допомагають відповісти на питання, як зміна незалежної змінної впливає на залежну змінну. Тому перейдемо до розрахунку коефіцієнту нахилу у нашій моделі. Формула коефіцієнту нахилу виглядає наступним чином:

$$b = \frac{\sum_{i=0}^n (X_i - \bar{X})(Y_i - \bar{Y})}{\sum_{i=0}^n (X_i - \bar{X})^2}$$

Через об'ємність розрахунків було вирішено вставити лише кінцевий результат розрахунку коефіцієнту нахилу:

$$b = \frac{-2070}{2064,5} \approx -1$$

Далі потрібно провести розрахунок значення константи a :

$$a = \bar{Y} - b\bar{X}$$

$$a = 27,5 - (-1) * 52,5 = 27,5 + 52,5 = 80$$

Таким чином, наша модель набуде вигляду:

$$Y = 80 - X$$

Із отриманої моделі можна зробити певні висновки, тому перейдемо до інтерпретації наших результатів. Отже, ми отримали значення константи $a = 80$, це означає, що якщо витрати на кібербезпеку дорівнюють нулю ($X=0$), очікувані фінансові втрати від кіберзагроз становитимуть 80 тис. грн.

Коефіцієнт нахилу дорівнює -1 . Це означає, що кожне наше додаткове збільшення витрат на кібербезпеку на 1 тис. грн. зменшує фінансові втрати від кіберзагроз на 1 тис. грн.

Отримавши такі результати, можемо сміливо переходити до прогнозування. Використовуючи нашу модель, ми можемо прогнозувати фінансові втрати від кіберзагроз за різних значень витрат на кібербезпеку. Наприклад, якщо підприємство планує витратити 85 тис. грн. на кібербезпеку в наступному році, очікувані фінансові втрати можна розрахувати так:

$$Y = 80 - 85 = -5 \text{ тис. грн.}$$

Негативний результат означає, що фінансові втрати від кіберзагроз повністю зникають при відповідних витратах.

Окрім розуміння кількості витрат на кібербезпеку, потрібно чітко розуміти куди витрачати ці гроші. В таких ситуаціях в нагоді стає теорія ігор – ще один розділ економіко-математичного моделювання, яке допомагає визначатись із стратегією.

Розглянемо такий сценрій: Підприємство розглядає можливість інвестування у різні заходи кібербезпеки для захисту від потенційних атак. Його мета — знайти оптимальну стратегію, яка мінімізує фінансові втрати від кіберзагроз.

Гравці, та їх можливі стратегії:

Гравці:

- Підприємство: Вирішує, які заходи кібербезпеки впровадити.
- Кіберзлочинець: Вирішує, чи здійснювати атаку на підприємство.

Стратегії підприємства мають такий вигляд:

- S1: Інвестувати в VPN.
- S2: Інвестувати в системи виявлення та запобігання вторгнень (IDS/IPS).
- S3: Інвестувати в обидва заходи.

Стратегії кіберзлочинців:

- A1: Здійснити атаку.
- A2: Не здійснювати атаку.

Складемо матрицю виплат (див. Табл. 3.2):

Матриця виплат показує виграші або втрати для кожного гравця в залежності від обраної комбінації стратегій.

Табл. 3.2 – Матриця виплат

	Атака(A1)	Відсутність атаки(A2)
VPN	(-10;-50)	(-5;0)
IDS/IPS	(-15;-40)	(-5;0)
Обидва заходи	(-20;-30)	(-10;0)

Пояснення виплат – перший елемент у дужках це втрати підприємства, другі – втрати кіберзлочинця, відповідно.

Аналіз рівноваги Неша

Рівновага Неша — це ситуація, коли жоден з гравців не може покращити свій виграш, змінивши стратегію, якщо інші гравці не змінюють свої стратегії.

Аналіз для кіберзлочинця:

- 1) Якщо підприємство обирає S1 (міжмережеві екрани):
 - а) Якщо кіберзлочинець обирає A1 (атака): втрати кіберзлочинця = -50.

- b) Якщо кіберзлочинець обирає A2 (відсутність атаки): втрати кіберзлочинця = 0.
- c) Краща стратегія: A2 (відсутність атаки), бо $0 > -50$.**
- 2) Якщо підприємство обирає S2 (IDS/IPS):
 - a) Якщо кіберзлочинець обирає A1 (атака): втрати кіберзлочинця = -40.
 - b) Якщо кіберзлочинець обирає A2 (відсутність атаки): втрати кіберзлочинця = 0.
 - c) Краща стратегія: A2 (відсутність атаки), бо $0 > -40$.**
- 3) Якщо підприємство обирає S3 (обидва заходи):
 - a) Якщо кіберзлочинець обирає A1 (атака): втрати кіберзлочинця = -30.
 - b) Якщо кіберзлочинець обирає A2 (відсутність атаки): втрати кіберзлочинця = 0.
 - c) Краща стратегія: A2 (відсутність атаки), бо $0 > -30$.**

Аналіз для підприємства:

- 1) Якщо кіберзлочинець обирає A1 (атака):
 - a) Якщо підприємство обирає S1: втрати = -10.
 - b) Якщо підприємство обирає S2: втрати = -15.
 - c) Якщо підприємство обирає S3: втрати = -20.
 - d) Краща стратегія: S1 (міжмережеві екрани), бо $-10 > -15 > -20$.**
- 2) Якщо кіберзлочинець обирає A2 (відсутність атаки):
 - a) Якщо підприємство обирає S1: втрати = -5.
 - b) Якщо підприємство обирає S2: втрати = -5.
 - c) Якщо підприємство обирає S3: втрати = -10.
 - d) Краща стратегія: S1 або S2 (міжмережеві екрани або IDS/IPS), бо $-5 = -5 > -10$.**

Згідно з аналізом, кіберзлочинець завжди обере стратегію не здійснювати атаку (A2), оскільки вона мінімізує його втрати. У відповідь підприємство повинно обрати стратегію S1 або S2, оскільки обидві ці стратегії мінімізують його втрати у випадку відсутності атаки. Таким чином, використання теорії ігор дозволяє підприємству визначити оптимальні стратегії кіберзахисту, враховуючи можливі дії кіберзлочинців. Це допомагає зменшити фінансові втрати та підвищити рівень економічної безпеки.

Об'єднання регресійного аналізу та теорії ігор дозволяє створити комплексну стратегію управління кібербезпекою, яка враховує як історичні дані, так і стратегічну взаємодію між підприємством та кіберзлочинцями. Нижче наведено, як ці методи можуть бути поєднані на основі розглянутих прикладів. Для об'єднання цих методів ми можемо використовувати результати регресійного аналізу для оцінки впливу різних стратегій інвестування в кібербезпеку на фінансові втрати, а також визначити оптимальні стратегії, враховуючи ймовірні дії кіберзлочинців.

1) Прогнозування витрат та втрат:

- a) Використовуємо регресійну модель для прогнозування фінансових втрат від кіберзагроз при різних рівнях інвестицій у кібербезпеку.

- b) Наприклад, якщо підприємство планує інвестувати 50 тисяч доларів у кібербезпеку, очікувані фінансові втрати будуть:

$$Y = 80 - 50 = 30 \text{ тис. доларів.}$$

2) Оцінка стратегій на основі теорії ігор:

- a) Враховуючи прогнозовані втрати, визначаємо оптимальні стратегії для підприємства та кіберзлочинців.
- b) За допомогою матриці виплат оцінюємо, яка стратегія буде найменш витратною для підприємства та найбільш збитковою для кіберзлочинця.

Поєднуємо результати аналізу, щоб визначити оптимальну стратегію. Наприклад, якщо регресійний аналіз показує, що інвестиції в обидва заходи кібербезпеки значно зменшують втрати, а теорія ігор вказує, що кіберзлочинці найімовірніше оберуть не атакувати в такому випадку, то підприємство повинно інвестувати в обидва заходи.

Поєднання регресійного аналізу та теорії ігор дозволяє підприємству приймати більш обґрунтовані рішення щодо інвестицій у кібербезпеку. Регресійний аналіз надає кількісні дані про вплив інвестицій на фінансові втрати, тоді як теорія ігор дозволяє врахувати стратегічну поведінку кіберзлочинців і визначити оптимальні стратегії захисту. Використання цих методів у комплексі забезпечує всебічний підхід до управління економічною безпекою підприємства в умовах зростаючих кіберзагроз. Ці методи дозволяють не лише прогнозувати можливі втрати, але й розробляти ефективні стратегії захисту, що є важливим для збереження стабільності та розвитку сучасних підприємств в умовах зростаючих кіберзагроз.

ВИСНОВКИ

У даній кваліфікаційній бакалаврській роботі проведено комплексний аналіз оцінювання рівня економічної безпеки підприємства у кіберпросторі в умовах цифрової трансформації. Результати дослідження дозволили визначити основні методи та підходи до оцінювання економічної безпеки, а також ідентифікувати основні кіберзагрози, які можуть впливати на стабільність та розвиток підприємств.

До основних результатів дослідження можна віднести класифікацію та аналіз кіберзагроз, розробку рекомендацій щодо підвищення рівня економічної безпеки, впровадження інтеграційної методики оцінювання економічної безпеки, аналіз економіко-математичних моделей, оцінка ефективності заходів безпеки, підвищення стійкості підприємства.

- У ході дослідження були ідентифіковані основні кіберзагрози, що впливають на економічну безпеку підприємств, такі як ransomware, phishing, DDoS атаки та викрадення облікових даних. Ці загрози становлять серйозну небезпеку для фінансової стабільності та безперервності бізнес-процесів.
- На основі аналізу сучасних кіберзагроз були розроблені рекомендації щодо підвищення рівня економічної безпеки підприємств, які включають впровадження багатофакторної аутентифікації, регулярні навчання персоналу, використання сучасних технологій захисту, проведення регулярних аудитів безпеки, створення груп реагування на інциденти (CSIRT) та використання міжнародних стандартів і найкращих практик.
- Була запропонована інтеграційна методика оцінювання економічної безпеки, яка дозволяє систематизувати процес управління ризиками та забезпечити комплексний підхід до захисту інформаційних ресурсів. Використання міжнародних стандартів, таких як ISO 27001 та ISO 27005, а також NIST Cybersecurity Framework допомагає підприємствам створити структуру для ефективного управління кібербезпекою.
- Використання економіко-математичних моделей дозволяє прогнозувати рівень економічної безпеки підприємства, оцінювати вплив кіберзагроз та розробляти стратегії для їх мінімізації. Моделі регресійного аналізу, моделювання часових рядів, стохастичні та імітаційні моделі допомагають підприємствам бути більш підготовленими до можливих атак.
- Запропоновані методи оцінки ефективності заходів кібербезпеки включають використання ключових показників ефективності (KPI), аналіз витрат та вигод, порівняння показників до і після впровадження

заходів, що дозволяє підприємствам оцінити успішність своїх дій та зробити необхідні коригування.

- Впровадження запропонованих заходів кібербезпеки сприяє підвищенню стійкості підприємства, зниженню фінансових втрат від кіберінцидентів, покращенню фінансових показників та відновленню довіри клієнтів і партнерів.

Отже, результати проведеного дослідження підтверджують важливість комплексного підходу до забезпечення економічної безпеки підприємств у кіберпросторі. Використання сучасних методів оцінювання, впровадження передових технологій захисту та регулярне навчання персоналу дозволяють підприємствам ефективно протидіяти кіберзагрозам та забезпечувати стабільний розвиток у сучасних умовах цифрової трансформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Economic Security of the Enterprise Within the Conditions of Digital Transformation by Yuliia Samoilenko, Igor Britchenko, Iaroslava Levchenko, Peter Lošonczy, Oleksandr Bilichenko, Olena Bodnar. *Economic Affairs*, Vol. 67, No. 04, pp. 619-629, September 2022
2. Шилю Жанна. Методика оцінювання рівня економічної безпеки підприємства. *International Science Journal of Management, Economics & Finance*. Vol. 1, No. 4, 2022, pp. 17-25. doi: 10.46299/j.isjmef.20220104.03
3. К. С. Зайченко, Н. І. Діма Економічна безпека підприємства: Сутність та роль
4. Управління системою фінансової безпеки підприємства: автореф. дис... канд. екон. наук: 21.04.02 [Електронний ресурс] / Ю.Г. Кім; Вищ. навч. закл. "Ун-т економіки та права "КРОК". - К., 2009. - 21 с. - укр. - Режим доступу: http://irbis-nbuv.gov.ua/cgi-bin/irbis_all/cgiirbis_64.exe.
5. Штангрет А.М. Економічна безпека підприємства в умовах антикризового управління: концептуальне визначення та механізм забезпечення / А.М. Штангрет, Я.В. Котляревський, М.М. Караїм. – Л: УАД, 2012. – 288с.
6. Milka, A., Artyukh-Pasiuta, O., & Kononenko, Z. (2023). METHODOLOGICAL APPROACHES TO ASSESSING THE LEVEL OF ECONOMIC SECURITY OF THE ENTERPRISE. *Economics, Finance and Management Review*, (4), 20–30 <https://public.scnchub.com/efmr/index.php/efmr/article/view/264/200>
7. Nataliia Levkvovets ENSURING ECONOMIC SECURITY OF THE ENTERPRISE <https://doi.org/10.30525/978-9934-26-220-3-31>
8. K.A. Bollen Indicator: Methodology
9. John B. Guerard Regression Analysis and Forecasting Models
10. Гаркуша С.В. Навчально-методичний посібник для самостійного вивчення дисципліни «Інтелектуальні інформаційні технології»
11. Б. Є. Грабовецький, Економічний аналіз. Навчальний посібник. Видавництво ВНТУ
12. Стендер С. В., Фротер О. С., Снітко Ю. М.: Цифрова інтеграція та кіберзахист економіки України: правові аспекти та інноваційні стратегії. Економіка і фінанси. 2023. No2(34). С. 45-60.
13. Краус К., Краус Н., Штепа О. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. *Innovation and Sustainability*. 2022. No 3. С. 26–37. DOI: <https://doi.org/10.31649/ins.2022.3.26.37>
14. Сидоренко О.В. Математичні методи обробки в психології. - СПб, Мова, 2001. - 349 с
15. Математичні та статистичні методи аналізу соціологічної інформації : Практикум / Л. Ф. Панченко; КПІ ім. І.Сікорського, 2018. – 289 с.

16. Saqib S, Sarah A.S., Manal S. Al-Ghamdi , Hayfa Al-Muhaisen and Abdullah M. Almuhaideb., A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. MDPI, Sensor.
17. Maurya, A. K., Kumar, N., Agrawal, A., & Khan, R. A. (2018). Ransomware Evolution, Target and Safety Measures. *International Journal of Computer Sciences and Engineering*, 6(1), 80-85. DOI: 10.26438/ijcse/v6i1.8085
18. Kumar, S. A. P. (2018). Phishing – challenges and solutions. *Computer Fraud & Security*, January 2018, 15-19. DOI: 10.1016/S1361-3723(18)30007-1.
19. Sharp, R. (2007). An Introduction to Malware. DTU Orbit.
20. Cyber threat categories and definitions. URL: <https://umbrella.cisco.com/trends-threats/cyber-threat-categories-and-definitions>
21. Developing Meaningful Key Performance Indicators. September 2014.
22. Švábenský, V., Vykopal, J., Čeleda, P., & Dovjak, J. (2023). Automated feedback for participants of hands-on cybersecurity training. *Education and Information Technologies*. DOI: 10.1007/s10639-023-12265-8.
23. Mallik, Avijit. "Man-in-the-Middle Attack: Understanding in Simple Words." *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, Volume 2, Nomor 2, Oktober 2018, 109-134.
24. Sachdeva, M., Singh, G., Saluja, K. K., & Singh, K. (2010). DDoS Incidents and their Impact: A Review. *The International Arab Journal of Information Technology*, 7(1), 14-19.
25. Credential Harvesting Summary (2022). Trinity Cyber.
26. "Methodology for risk management related to cyber-security of Unmanned Aircraft Systems." ETFA 2019 - 24th IEEE International Conference on Emerging Technologies and Factory Automation, IEEE Industrial Electronics Society (IES).
27. ISO/IEC 27005:2018. Information technology — Security techniques — Information security risk management. URL: <https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027005-2018.pdf>.
28. FIRST CSIRT Services Framework v2.1.0 bugfix1. URL: https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0_bugfix1.pdf.

Ім'я користувача:
Комп'ютерної математики та інформаційної безпеки... 1016335443

ID перевірки:

Дата перевірки:
08.06.2024 16:49:54 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
08.06.2024 16:50:15 EEST

ID користувача:
100005746

Назва документа: Диплом_Кобяков

Кількість сторінок: 42

Кількість слів: 9990 Кількість символів: 79432 Розмір файлу: 145.56 KB

ID файлу: 1016136077

5.06%

Схожість

Найбільша схожість: 0.51% з джерелом з Бібліотеки (ID файлу: 1000017055)

3.44% Джерелаз Інтернету

257

Сторінка 44

3.46% Джерелаз Бібліотеки

352

Сторінка 46

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0% Вилучень

Немає вилучених джерел