МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Сумський державний університет

Навчально-науковий інститут бізнесу, економіки та менеджменту

(повна назва інституту/факультету)

Кафедра економічної кібернетики

(повна назва кафедри)

«До захисту допущено»

Завідувач кафедри

Віталія КОЙБІЧУК

(підпис) (Ім'я та ПРІЗВИЩЕ)

_____ 2024р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня бакалавр

(бакалавр / магістр)

зі спеціальності 051 , Економіка ,

(код та назва)

освітньо-професійної

(освітньо-професійної / освітньо-наукової)

програми Економічна кібернетика та бізнес аналітика

(назва програми)

на тему: Економіко-математичне моделювання взаємозв'язків кібербезпеки та безпеки охорони здоров'я країн світу

Здобувача (ки) групи ЕК-01а Савченко Даніїл Дмитрович

(шифр групи) (прізвище, ім'я, по батькові)

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

(підпис) Даніїл САВЧЕНКО

(Ім'я та ПРІЗВИЩЕ здобувача)

Керівник асистент кафедри економічної кібернетики Сумського державного університету, доктор філософії, Тетяна ДОЦЕНКО

(посада, науковий ступінь, вчене звання, Ім'я та ПРІЗВИЩЕ) (підпис)

Консультант[1)] _____

(посада, науковий ступінь, вчене звання Ім'я та ПРІЗВИЩЕ) (підпис)

Суми – 2024

Примітки:

1) Зазначається за наявності

Міністерство освіти і науки України
Сумський державний університет
Навчально-науковий інститут бізнесу, економіки та менеджменту
Кафедра економічної кібернетики

ЗАТВЕРДЖУЮ
Завідувач кафедри
к.е.н., доцент
_____Віталія КОЙБІЧУК
“26” березня 2024 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ НА
ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА
(спеціальність 051 Економіка «Економічна кібернетика та бізнес аналітика»)
студенту 4 курсу, групи ЕК-01а
Савченко Даніїл Дмитрович

1. Тема роботи «Економіко-математичне моделювання взаємозв'язків кібербезпеки та безпеки охорони здоров’я країн світу. Economic and Mathematical Modelling of Interrelationships between Cybersecurity and Healthcare Security in the World» затверджена наказом по університету від 08 травня 2024 року №0486-VI.
2. Термін подання студентом закінченої роботи «24» травня 2024 року
3. Мета кваліфікаційної роботи: розробка структурно-логічної моделі взаємозв'язків кібербезпеки та безпеки охорони здоров’я країн світу.
4. Об’єкт дослідження: взаємозв'язок кібербезпеки та безпеки охорони здоров’я країн світу.
5. Предмет дослідження: математичні методи та моделі оцінювання взаємозв'язків кібербезпеки та безпеки охорони здоров’я країн світу.
6. Кваліфікаційна робота виконується на статистичних даних відкритих інформаційних джерел European Commission, матеріалах законодавчих та нормативних актів, навчальних посібників, наукових публікацій іноземних та вітчизняних дослідників
7. Орієнтовний план кваліфікаційної роботи, терміни подання розділів керівникові та зміст завдань для виконання поставленої мети

Розділ 1. Загальна характеристика об’єкта дослідження та побудова математичної моделі

У розділі 1.

1.1 Аналіз предметної галузі та виявлення найбільш вагомих параметрів об’єкта дослідження.

1.2 Огляд сучасного стану моделювання об’єкта дослідження.

1.3 Постановка задачі моделювання та формування вимог до моделі.

1.4 Розробка математичної моделі.

Розділ 2. Перевірка адекватності моделі та пропозиції по її використанню

У розділі 2.

2.1 Перевірка адекватності побудованої математичної моделі.

2.2 Побудова методики проектувальних розрахунків.
2.3 Розробка програмного застосунку для автоматизації методики розрахунків.
8. Консультації з роботи:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Доценко Т.В., асистент кафедри Економічної кібернетики	01/04/2024	01/04/2024
2	Доценко Т.В., асистент кафедри Економічної кібернетики	05/04/2024	05/04/2024
3			

9. Дата видачі завдання: «01» квітня 2024 року

Керівник кваліфікаційної роботи _____ Т.В. Доценко
(підпис) (ініціали, прізвище)

Завдання до виконання одержав _____ Д.Д. Савченко
(підпис) (ініціали, прізвище)

АНОТАЦІЯ

кваліфікаційної роботи бакалавра на тему

«ЕКОНОМІКО-МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ВЗАЄМОЗВ'ЯЗКІВ КІБЕРБЕЗПЕКИ ТА БЕЗПЕКИ ОХОРОНИ ЗДОРОВ’Я КРАЇН СВІТУ»

Студента Савченко Данііл Дмитрович

(прізвище, ім’я, по батькові)

Зміст кваліфікаційної роботи викладено на 64 сторінках. Список використаних джерел із 41 найменувань, розміщений на 6 сторінках. Робота містить 1 таблицю, 44 рисунків, а також 2 додатки, розміщених на 8 сторінках.

Актуальність теми дослідження. В сучасному цифровому світі, де віртуальна реальність переплітається з реальним життям, питання кібербезпеки та безпеки міцного здоров'я стають дедалі більш актуальними та важливими. Зростання залежності від інформаційних технологій вносить свої виклики і загрози, які впливають на економічний, соціальний та медичний аспекти суспільства. В цьому контексті виникає потреба в розробці комплексних економіко-математичних моделей, спрямованих на аналіз та прогнозування взаємозв'язків між кібербезпекою та безпекою міцного здоров'я країн світу.

Ця робота присвячена вивченню та аналізу таких взаємозв'язків, а також розробці математичних моделей, які допоможуть краще розуміти природу цих явищ та визначати стратегії їхнього управління. Інтеграція кібербезпеки та безпеки міцного здоров'я у загальні моделі дозволить виявити ключові фактори, що впливають на стійкість суспільства в умовах цифрової трансформації та епідеміологічних загроз. У роботі будуть розглянуті основні підходи до економіко-математичного моделювання кібербезпеки та безпеки міцного здоров'я, а також проведений аналіз існуючих та потенційних загроз у цих сферах.

Мета роботи – розробка структурно-логічної моделі взаємозв'язків кібербезпеки та безпеки охорони здоров’я країн світу.

Об’єктом дослідження є взаємозв'язок кібербезпеки та безпеки охорони здоров’я країн світу.

Предметом дослідження є математичні методи та моделі оцінювання взаємозв'язків кібербезпеки та безпеки охорони здоров’я країн світу.

Методи дослідження включають аналіз статистичних даних; теоретичний аналіз літературних джерел з метою вивчення важливих теоретичних понять і напрямів дослідження; бібліометричний аналіз статей бази Scopus по ключовим словам, використовуючи інструментарій VOSViewer; математичне моделювання; використання інструментарію статистичного пакету Statistica для побудови моделі; кластерний аналіз методом k-середніх з метою розподілу країн на однорідні групи; застосування методики Sigma-restricted parameterization - Univariate Tests of Significance - Pareto Chart of t-Values, кореляційного аналізу з метою визначення найвпливовіших факторів; побудова множинної лінійної регресії методом найменших квадратів (OLS-метод); виконання канонічного аналізу на основі канонічних кореляцій з метою виявлення причинно-наслідкового зв’язку між групами факторів.

Інформаційна база дослідження включає наукові статті, звіти організацій, статистичні дані та інші джерела, що стосуються кібербезпеки, охорони здоров’я та економічних аспектів їх взаємодії. Для бібліометричного аналізу використовується ресурсна база платформи Scopus. Статистичні дані зібрано за 2021р. з відкритих інформаційних джерел European Commission.

Наукова новизна одержаних результатів полягає в розробці структурно-логічної економіко-математичної моделі «взаємозв'язків кібербезпеки та безпеки охорони здоров’я країн світу». Для вирішення поставлених завдань використано комплекс загальнонаукових і спеціальних методів дослідження.

Рекомендації щодо використання результатів дослідження. Результати досліджень, проведених у цій роботі, мають потенціал відіграти важливу роль у формуванні політики в галузі кібербезпеки та здоров'я, а також слугувати

основою для подальших наукових досліджень у цій області. Вивчення взаємозв'язків між цими двома сферами може стати кроком до створення більш раціональних та ефективних стратегій кібербезпеки та безпеки охорони здоров'я, що виникають у контексті глобальних викликів сучасності.

Апробація результатів дослідження. Тези: Савченко Д. Д., Доценко Т. В. (2024). Теоретичні аспекти взаємозв'язків кібербезпеки та безпеки охорони здоров’я. Виклики кібербезпеки індустрії фінансових послуг: ІІ наукова онлайн-конференція, Суми, 2 липня 2024 року. Сумський державний університет, 2024.

Ключові слова: канонічний аналіз кібербезпека, безпека охорони здоров’я, кластерний аналіз, кореляційний аналіз, метод найменших квадратів (OLS-метод), Pareto Chart of t-Values, Sigma-restricted parameterization, Univariate Tests of Significance.

Рік виконання кваліфікаційної роботи – 2024 рік.

Рік захисту роботи – 2024 рік.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. В сучасному цифровому світі, де віртуальна реальність переплітається з реальним життям, питання кібербезпеки та безпеки міцного здоров'я стають дедалі більш актуальними та важливими. Зростання залежності від інформаційних технологій вносить свої виклики і загрози, які впливають на економічний, соціальний та медичний аспекти суспільства. В цьому контексті виникає потреба в розробці комплексних економіко-математичних моделей, спрямованих на аналіз та прогнозування взаємозв'язків між кібербезпекою та безпекою міцного здоров'я країн світу.

Ця робота присвячена вивченню та аналізу таких взаємозв'язків, а також розробці математичних моделей, які допоможуть краще розуміти природу цих явищ та визначати стратегії їхнього управління. Інтеграція кібербезпеки та безпеки міцного здоров'я у загальні моделі дозволить виявити ключові фактори, що впливають на стійкість суспільства в умовах цифрової трансформації та епідеміологічних загроз. У роботі будуть розглянуті основні підходи до економіко-математичного моделювання кібербезпеки та безпеки міцного здоров'я, а також проведений аналіз існуючих та потенційних загроз у цих сферах.

Результати досліджень, проведених у цій роботі, мають потенціал відіграти важливу роль у формуванні політики в галузі кібербезпеки та здоров'я, а також слугувати основою для подальших наукових досліджень у цій області. Вивчення взаємозв'язків між цими двома сферами може стати кроком до створення більш раціональних та ефективних стратегій управління ризиками, що виникають у контексті глобальних викликів сучасності.

Предметом дослідження є математичні методи та моделі оцінювання взаємозв'язків кібербезпеки та безпеки охорони здоров’я країн світу.

Об’єктом дослідження є взаємозв'язок кібербезпеки та безпеки охорони здоров’я країн світу.

Мета роботи полягає у розробці структурно-логічної моделі взаємозв'язків кібербезпеки та безпеки охорони здоров’я країн світу.

Основними завданнями дослідження є: охарактеризувати предметну галузь та виявити найбільш вагомі параметри об’єкта дослідження; проаналізувати сучасний стан моделювання об’єкта дослідження; сформувати постановку задачі моделювання та вимог до моделі; розробити математичну модель; перевірити адекватність побудованої математичної моделі; побудувати методику проектувальних розрахунків; розробити програмний застосунок для автоматизації методики розрахунків.

Методи дослідження включають аналіз статистичних даних; теоретичний аналіз літературних джерел з метою вивчення важливих теоретичних понять і напрямів дослідження; бібліометричний аналіз статей бази Scopus по ключовим словам, використовуючи інструментарій VOSViewer; математичне моделювання; використання інструментарію статистичного пакету Statistica для побудови моделі; кластерний аналіз методом k-середніх з метою розподілу країн на однорідні групи; застосування методики Sigma-restricted parameterization - Univariate Tests of Significance - Pareto Chart of t-Values, кореляційного аналізу з метою визначення найвпливовіших факторів; побудова множинної лінійної регресії методом найменших квадратів (OLS-метод); виконання канонічного аналізу на основі канонічних кореляцій з метою виявлення причинно-наслідкового зв’язку між групами факторів; економічний аналіз.

Інформаційна база дослідження включає наукові статті, звіти організацій, статистичні дані та інші джерела, що стосуються кібербезпеки, охорони здоров’я та економічних аспектів їх взаємодії. Для бібліометричного аналізу використовується ресурсна база платформи Scopus. Статистичні дані зібрано за 2021р. з відкритих інформаційних джерел European Commission.

Наукова новизна одержаних результатів полягає в розробці структурно-

логічної економіко-математичної моделі «взаємозв'язків кібербезпеки та безпеки охорони здоров’я країн світу». Для вирішення поставлених завдань використано комплекс загальнонаукових і спеціальних методів дослідження.

Апробація результатів дослідження. Тези: Савченко Д. Д., Доценко Т. В. (2024). Теоретичні аспекти взаємозв'язків кібербезпеки та безпеки охорони здоров’я. Виклики кібербезпеки індустрії фінансових послуг: ІІ наукова онлайн-конференція, Суми, 2 липня 2024 року. Сумський державний університет, 2024.

Рекомендації щодо використання результатів дослідження. Результати досліджень, проведених у цій роботі, мають потенціал відіграти важливу роль у формуванні політики в галузі кібербезпеки та здоров'я, а також слугувати основою для подальших наукових досліджень у цій області. Вивчення взаємозв'язків між цими двома сферами може стати кроком до створення більш раціональних та ефективних стратегій управління ризиками, що виникають у контексті глобальних викликів сучасності.

РОЗДІЛ 1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ОБ'ЄКТА ДОСЛІДЖЕННЯ ТА ПОБУДОВА МАТЕМАТИЧНОЇ МОДЕЛІ

1.1 Аналіз предметної галузі та виявлення найбільш вагомих параметрів об'єкта дослідження

Кібербезпека або cyber security – це заходи, які вживають для захисту даних або пристроїв, підключених до мережі, від несанкціонованого доступу та використання у злочинних цілях. Кібербезпека це те, що забезпечує конфіденційність, цілісність і доступність даних протягом їх всього життєвого циклу [1, 2, 3, 4, 5]. Виклики сучасної кібербезпеки наступні: у цифрову еру кібербезпека є критичною проблемою для людей, корпорацій та урядів; зі збільшенням використання технологій і цифрових пристроїв як ніколи необхідно захищати електронні пристрої, мережі та дані від небажаного доступу, крадіжки та пошкодження; з розвитком технологій дія кібербезпеки щодо захисту організації, співробітників і критично важливих активів від кіберзагроз стикається з кількома проблемами [6, 7, 8, 9].

Для кращого захисту від кіберзагроз необхідно знати типи кібербезпеки. На рисунку 1.1 показано різні типи кібербезпеки:

1. Безпека мережі: це практика захисту комп'ютерної мережі від несанкціонованого доступу або атак. Він включає використання брандмауерів, систем виявлення та запобігання вторгненням, а також віртуальних приватних мереж (VPN). Основна мета – захист інфраструктури мережі, включаючи сервери, маршрутизатори, комутатори та інші мережеві пристрої.

2. Безпека програми: стосується заходів, вжитих для захисту програмного забезпечення від кібератак. Це включає в себе тестування коду, виявлення вразливостей і забезпечення відсутності будь-яких недоліків безпеки в програмі. Може бути реалізована на різних етапах життєвого циклу розробки програмного забезпечення, від планування до розгортання.

3. Інформаційна безпека: передбачає захист цифрової інформації, такої як дані, що зберігаються в базах даних, файлах або інших сховищах. Інформаційна безпека забезпечує конфіденційність, цілісність і доступність даних, захищаючи їх від несанкціонованого доступу, розголошення, зміни або знищення. Він включає різні заходи безпеки, такі як контроль доступу, шифрування та резервне копіювання.

4. Хмарна безпека: стосується захисту даних і систем, розміщених на хмарних платформах, таких як Amazon Web Services (AWS), Microsoft Azure та Google Cloud. Включає в себе поєднання технічних і адміністративних елементів керування, спрямованих на захист даних, що зберігаються в хмарі, а також самої хмарної інфраструктури.

5. Безпека інтернету речей (IoT); відноситься до мережі підключених пристроїв, таких як смартфони, розумні будинки та переносні пристрої. Безпека IoT передбачає безпеку самих пристроїв, а також мережі, яка їх з'єднує. Зі збільшенням кількості пристроїв IoT зростає й ризик кібератак.

6. Управління ідентифікацією та доступом (IAM): це практика керування ідентифікацією користувачів і контролю доступу до ресурсів в організації. IAM включає різні заходи безпеки, такі як автентифікація користувачів, авторизація та контроль доступу [10, 11, 12, 13].

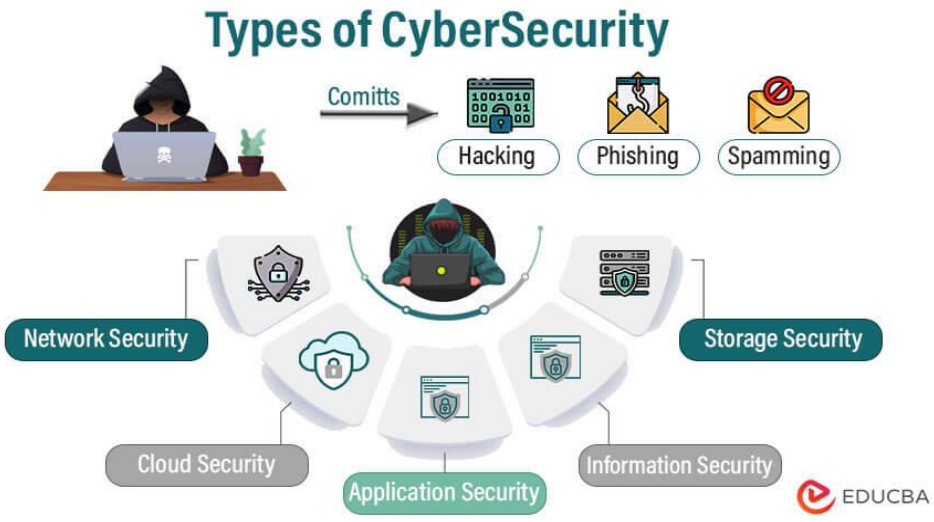


Рисунок 1.1 – Типи кібербезпеки

Джерело: Educba Blog [13].

Охорона здоров'я – це поліпшення здоров'я шляхом профілактики, діагностики, лікування, полегшення або вилікування хвороб, недуг, травм та інших фізичних і психічних розладів у людей. Цей термін включає роботу, пов'язану з наданням первинної, вторинної та третинної медичної допомоги, а також з громадським здоров'ям [14, 15, 16].

Системи охорони здоров'я – це організації, створені для задоволення медичних потреб цільових груп населення. Добре функціонуюча система охорони здоров'я вимагає наявності механізму фінансування, добре підготовленого та адекватно оплачуваного персоналу, достовірної інформації, на якій ґрунтуються рішення та політика, а також добре утримуваних закладів охорони здоров'я для надання якісних медикаментів та технологій [17, 18, 19].

Заклади охорони здоров’я повинні розвивати та популяризувати міцну культуру безпеки охорони здоров’я, яка включає зобов’язання щодо безпеки працівників, надання та адекватний доступ до засобів безпеки та засобів індивідуального захисту, а також широкі зусилля з навчання, які використовують протоколи, що вимагають певних заходів безпеки.

Культура безпеки охорони здоров’я має кілька важливих характеристик:

- Організації повинні взяти на себе зобов’язання надавати ресурси для вирішення проблем безпеки та запроваджувати безпечне обслуговування в будь-який час, демонструючи, що безпека є високим пріоритетом.
- Кожен повинен нести відповідальність за знання безпеки, впровадження та звітування про небезпечні умови з відповідальністю на всіх організаційних рівнях.
- Організації повинні визнавати дії високого ризику, такі як вплив патогенних мікроорганізмів, що передаються через кров та аерозолів, або хімічних речовин на робочому місці.
- Стандарти запобігання травматизму на робочому місці та належне робоче середовище повинні бути встановлені та контролюватися.

- Щоб забезпечити ефективні та стійкі рішення щодо безпечного догляду за пацієнтами, одночасно забезпечуючи безпеку медичних працівників, необхідно шукати внесок у різні дисципліни.
- Працівники охорони здоров'я повинні вірити, що вони можуть повідомляти про помилки або випадкові помилки, не боячись помсти, щоб безпека могла бути покращена за допомогою постійної підтримки та зворотного зв'язку, а не застосування покарань [20, 21, 22, 23].

Існує п'ять категорій небезпек, пов'язаних з роботою системи охорони здоров'я, які необхідно контролювати та запобігати в культурі безпечної та здорової праці (рисунок 1.2):

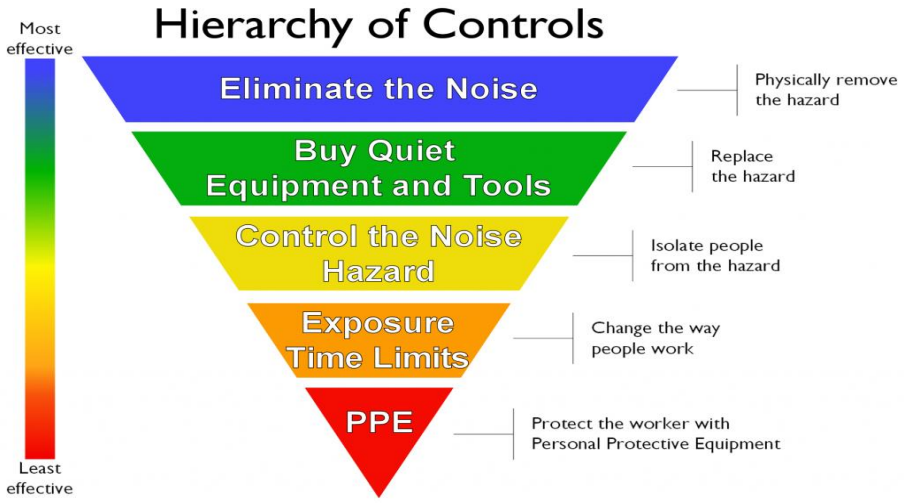


Рисунок 1.2 – Категорії небезпек пов'язаних з роботою системи охорони здоров'я

Джерело: Blogs.cdc.gov [23].

- Біологічні небезпеки – це збудники захворювань, які можуть передаватися від людини до людини різними шляхами і можуть призвести до гострих або хронічних захворювань.
- Хімічні небезпеки – стосуються будь-яких форм хімічних речовин, включаючи ліки, розчини, гази, пари, аерозолі та тверді частки, які є потенційно токсичними або подразливими для системи організму.

- Механічні небезпеки навколишнього середовища – це аспекти робочого місця, які можуть спричинити або посилити нещасні випадки, травми, напруги або дискомфорт.
- Фізичні небезпеки – це агенти на робочому місці, які можуть спричинити пошкодження тканин шляхом передачі енергії від агента людині.
- Психосоціальні небезпеки – це фактори робочого середовища, які можуть спричинити стрес, напругу або міжособистісні проблеми для працівника [24, 25, 26, 27].

Зв'язок між кібербезпекою та безпекою охорони здоров'я можна представити наступною схемою (рисунок 1.3):

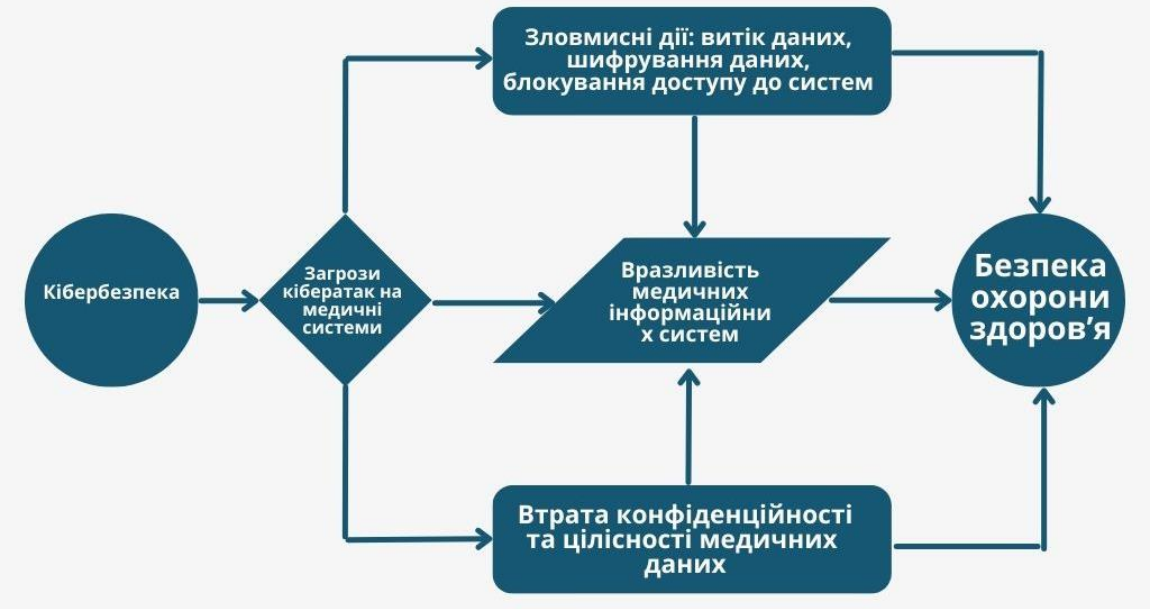


Рисунок 1.3 – Взаємозв'язок між кібербезпекою та безпекою охорони здоров'я

Джерело: сформовано автором

Ця схема демонструє, як загрози кібербезпеки, такі як кібератаки на медичні системи, призводять до вразливостей у медичних інформаційних системах, що в свою чергу може призвести до зловмисних дій, таких як витік даних, шифрування даних або блокування доступу.

У розрізі даної роботи доцільно також проаналізувати загальний перелік ключових слів у відібраних наукових публікаціях. За допомогою програмного забезпечення VOSviewer було сформовано три кластери ключових слів, що зустрічаються найчастіше в наукових працях за період з 2015 р. по 2024 р. (рисунок 1.4). Найбільшим кластером є жовтий, що містить у собі 15 ключових слова (найбільш часто зустрічаються такі слова, як «кібербезпека», «охорона здоров`я», «безпека мережі», «Інтернет речей», «охорона здоров`я»). Це дозволяє узагальнити жовтий кластер як такий, що опосередковує взаємозв'язків кібербезпеки та безпеки міцного здоров'я країн світу. Наступний за обсягом є зелений кластер, що складається з 10 ключових слів. До нього увійшли такі поняття, як «комп'ютерна безпека», «кібератака», «людини», «медичне обчислення », «конфеденційність». Другий за обсягом кластер (9 слів) включає в себе такі поняття як «комп`ютерна злочинність», «злочинність», «ризики для здоров'я». Третій за обсягом кластер (8 слів) включає в себе такі поняття як «кібербезпека», «охорона здоров'я», «галузі охорони здоров'я».

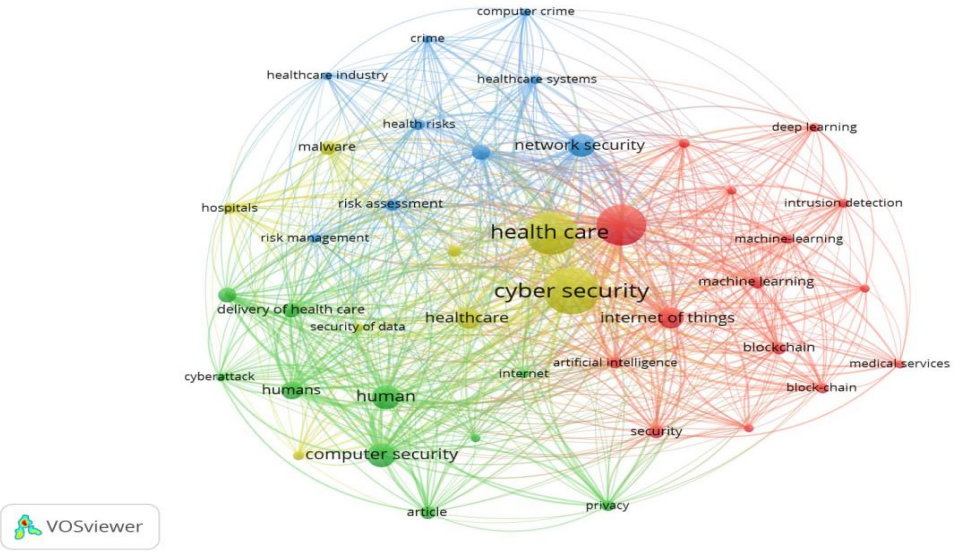


Рисунок 1.4 – Результати бібліометричного аналізу ключових слів, що одночасно трапляються в публікаціях, проіндексованих наукометричною базою Scopus, за запитами «cyber security» та «helth care» за допомогою інструментарію VOSviewer

Джерело: сформовано автором

На рисунку 1.5 представлено хронологію наукових публікації з досліджуваної проблематики протягом 2020-2022 років, що опублікована в наукометричній базі Scopus. З 2020 року найбільш вживаними у наукових роботах поняттями були ті, що пов’язані з управління ризиками та комп’ютерними безпекою (фіолетовий, синій кольори).З 2020-2021 року активно досліджувалася проблема охорони здоров’я, комп’ютерна безпека (синій колір). Починаючи з 2022 р. досліджується блокчейн та машинне навчання.

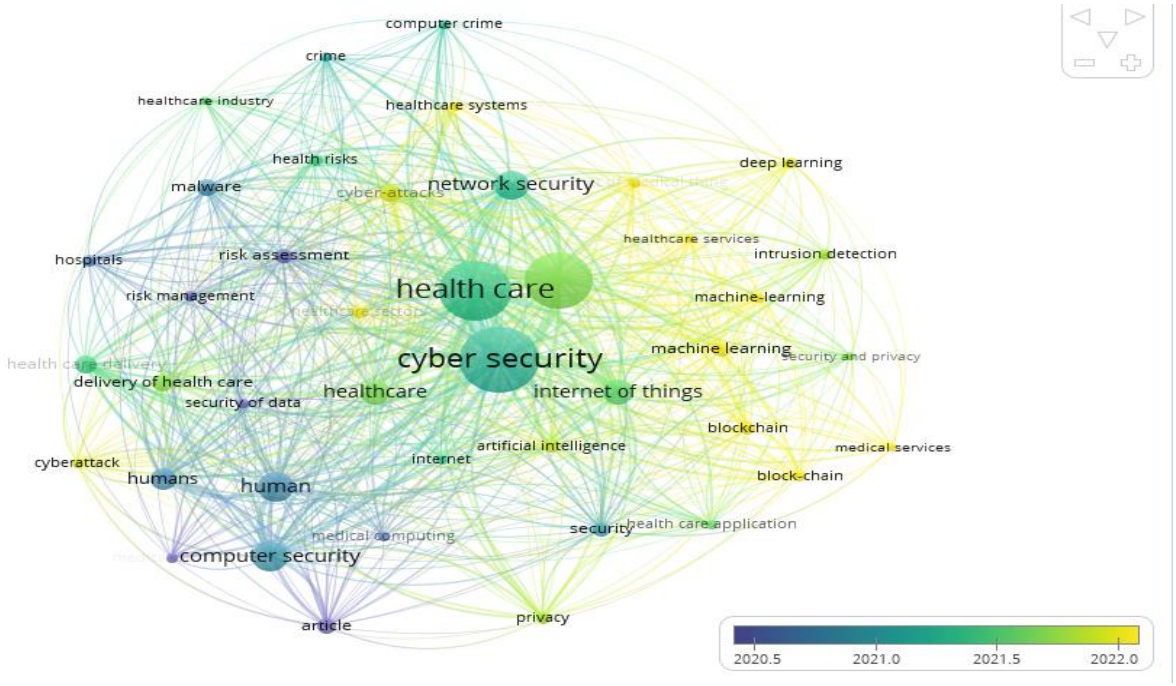


Рисунок 1.5 – Результати бібліометричного аналізу ключових слів, що одночасно трапляються в публікаціях, проіндексованих наукометричною базою Scopus, за запитами «cyber security» та «helth care» за допомогою інструментарію VOSviewer

Джерело: сформовано автором

Отже, проведений бібліометричний аналіз наукових публікацій підтвердив актуальність обраного напрямку дослідження.

1.2. Огляд сучасного стану моделювання об’єкта дослідження

Моделювання – це спосіб дослідження будь-яких явищ, процесів або об'єктів шляхом побудови й аналізу їх моделей. У широкому розумінні моделювання є однією з основних категорій теорії пізнання і мало не єдиним науково обґрунтованим методом наукових досліджень систем і процесів будь-якої природи в багатьох сферах людської діяльності [29].

Форми моделювання різноманітні і залежать від видів структурних моделей та сфери застосування. Виділяють предметне і знакове моделювання. Предметне припускає створення моделей, що відтворюють просторово-тимчасові, функціональні, структурні й інші властивості оригіналу (конкретно-наукові моделі). Знакове полягає в репрезентації параметрів об’єкта за допомогою символів, схем, формул, пропозицій мови (логіко-математичні моделі). Гносеологічний зміст моделювання утворює основу для переносу результатів, одержаних у ході вивчення моделей, на оригінал.

Під управлінським моделюванням розуміється процес побудови і дослідження аналогів реальних явищ, об’єктів, процесів, у яких відображені найважливіші, з погляду мети управління або дослідження, властивості й опущені другорядні, малоістотні. Наприклад, нормативна модель системи управління дає можливість уявити в основних рисах удосконалену систему управління, взаємозалежну за всіма її підсистемами і елементами.

На особливу увагу сьогодні заслуговує імітаційне моделювання, що повторює функції або розвиток соціального явища. Види імітаційних моделей можуть бути різними. Серед них виділяються ігрові (люди виконують ігрові ролі); машинні (комп’ютерні аналоги) і людино-машинні моделі. Останні являють собою діалогові комп’ютерні системи, що імітують реальні соціальні процеси з активним використанням евристичних даних, які одержують у процесі взаємодії з людиною, що є експертом у галузі знання або практики.

У комп’ютерному імітаційному моделюванні (машинне і людино-машинне) об’єкт вивчення і його соціологічна теорія первинні стосовно методів, експертних оцінок і т. д. [29, 30].

Моделювання кіберзагроз – це процес аналізу різноманітних ділових і технічних вимог до системи, визначення потенційних загроз і документування того, наскільки ці загрози роблять систему вразливою. Загроза стосується будь-якого випадку, коли неавторизована сторона отримує доступ до конфіденційної інформації, програм або мережі організації [31].

Процес моделювання кіберзагроз включає 5 ключових кроків (рисунок 1.6):

1. Постановка цілі (конфіденційність для захисту даних від несанкціонованого розголошення; цілісність для запобігання несанкціонованим змінам інформації; можливість надання необхідних послуг навіть під час атаки на систему).

2. Візуалізація (два типи візуалізацій: діаграма потоку даних: вона показує, як дані переміщуються у вашій системі; діаграма процесу: на ній показано, як користувачі взаємодіють і переміщуються в різних варіантах використання).

3. Визначення загрози (проаналізувати діаграми візуалізації, щоб зрозуміти фактичні загрози; з’ясувати різні способи, якими ваші активи можуть бути скомпрометовані, і хто є потенційними зловмисниками).

4. Пом’якшення (обробка гсписоку або бібліотеки загроз, пов’язаних із кожним активом і його операціями, а також список можливих профілів зловмисників; визначення, до якої з загроз вразлива ваша програма).

5. Перевірка (перевірка, чи всі вразливості усунено, чи всі загрози пом'якшені, чи залишкові ризики чітко задокументовані; вирішення наступних кроків для керування виявленими загрозами та вирішення, коли відбудеться наступна ітерація моделювання загроз) [32, 33].

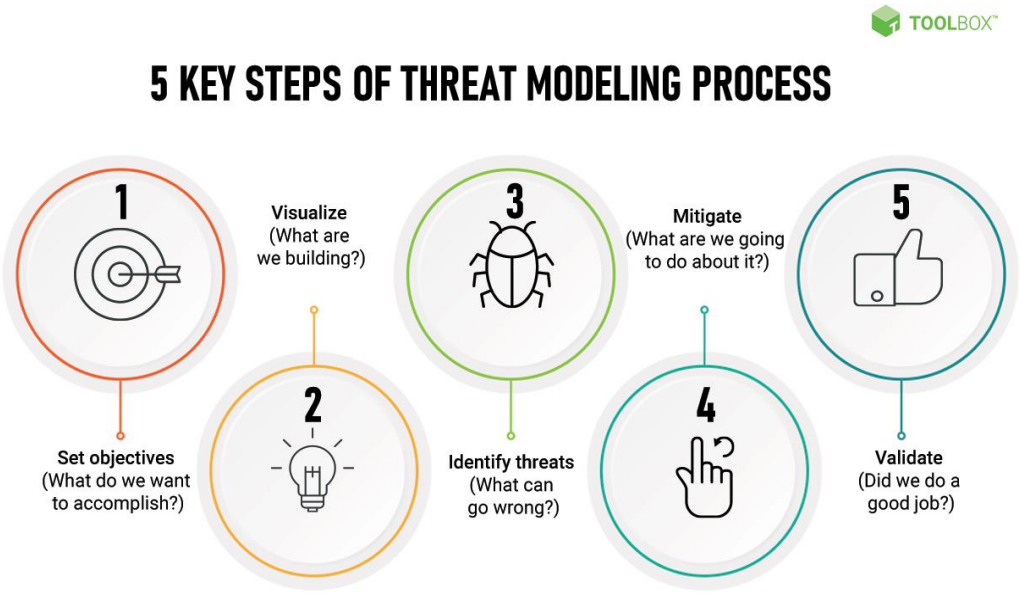


Рисунок 1.6 – Ключові кроки процесу моделювання загроз

Джерело: Spiceworks.com [34].

Наступним виділено три методологій моделювання кіберзагроз:

1. STRIDE (методологія, розроблена корпорацією Майкрософт для моделювання загроз, пропонує мнемоніку для визначення загроз безпеці в шести категоріях: підробка, втручання, відмова, розголошення інформації, відмова в обслуговуванні, підвищення привілеїв).

2. DREAD (спосіб класифікувати й оцінювати ризики безпеки за п’ятьма категоріями: потенційна шкода, відтворюваність, можливість використання, постраждалі користувачі, виявленість).

3. P.A.S.T.A («Процес симуляції атак і аналізу загроз» – семиетапна методологія, орієнтована на ризик; пропонує динамічну ідентифікацію загроз, процес підрахунку та оцінювання; після того, як експерти проведуть детальний аналіз виявлених загроз, розробники можуть розробити стратегію пом’якшення, орієнтовану на ресурси, проаналізувавши програму через погляд, орієнтований на зловмисників) [33, 34].

У найширшому плані можна виділити чотири основні моделі охорони здоров’я (рисунок 1.7):

1. Модель Беверіджа (уряд діє як єдиний платник, усуваючи будь-яку конкуренцію на ринку, щоб зберегти низькі витрати та стандартизувати виплати; будучи єдиним платником, національна служба охорони здоров'я контролює, що можуть робити «внутрішні мережеві» провайдери та які вони можуть стягувати; фінансується за рахунок податків, немає плати з власної кишені пацієнтів або будь-якого розподілу витрат; критичне зауваження - потенційний ризик надмірного використання).

2. Модель Бісмарка (більш децентралізована форма охорони здоров'я; роботодавці та працівники несуть відповідальність за фінансування своєї системи медичного страхування через «лікарняні фонди», створені шляхом відрахувань із заробітної плати; постачальники та лікарні, як правило, є приватними, хоча страхові компанії є державними; уряд контролює ціноутворення; не забезпечує загального медичного страхування; критика - як забезпечити догляд за тими, хто не може працювати або не може дозволити собі платити внески, включаючи старіння населення та дисбаланс між пенсіонерами та працівниками).

3. Національна модель медичного страхування (держава діє як єдиний платник за медичні процедури; провайдери є приватними; моделлю керують приватні постачальники, але виплати надходять від державної програми страхування, у яку платить кожен громадянин; є універсальним страхуванням, яке не приносить прибутку та не відмовляє у виплаті претензій; це дешевше і набагато простіше в навігації; такий баланс між приватним і державним дає лікарням і постачальникам більше свободи; критикою є можливість довгих списків очікування та затримок у лікуванні, які вважаються серйозною проблемою політики охорони здоров'я).

4. Кишенькова модель (пацієнти повинні платити за свої процедури зі своєї кишені; заможні отримують професійну медичну допомогу, а бідні – ні, якщо тільки вони якимось чином не знайдуть достатньо грошей, щоб заплатити за це; охорона здоров'я все ще залежить від доходу) [35, 36, 37, 38].

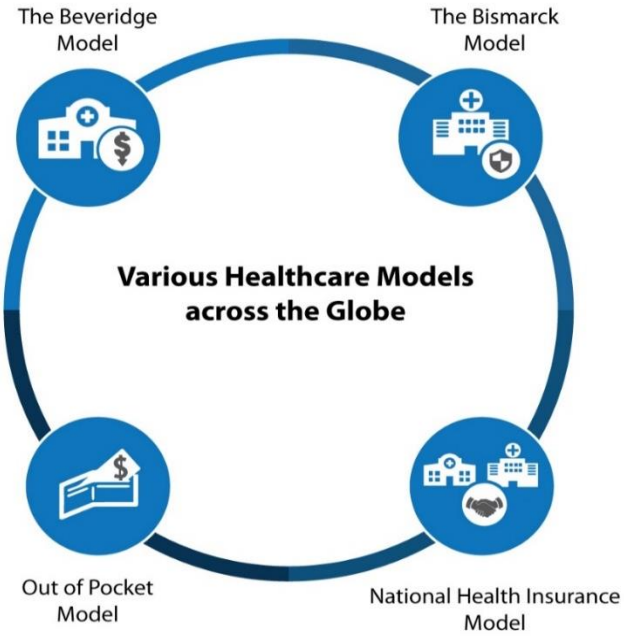


Рисунок 1.7 – Ключові моделі охорони здоров’я

Джерело: telradsol.com [40].

Безпека охорони здоров’я має включати ретельний аналіз сильних і слабких сторін глобальних моделей, щоб вони могли інформувати про нову політику охорони здоров’я та зрештою створити модель, яка працюватиме для всіх [39, 40].

1.3. Постановка задачі моделювання та формування вимог до моделі

Перед початком математичного опису моделі та виконанням розрахунків, необхідно сформувати загальну схему, що відображатиме механізм проведення дослідження взаємозв'язків кібербезпеки та безпеки охорони міцного здоров’я країн світу.

Моделювання взаємозв'язків буде проводитися на макрорівні в розрізі обраних показників, що відображають кібербезпеку та безпеку охорони

міцного здоров’я. Для цього було обрано найбільш вагомі та репрезентативні характеристики об’єкту дослідження.

Часовий період дослідження визначено 2021 рік, використовуючи фактичні дані світових статистичних джерел.

Модель повинна відповідати наступним критеріям:

1. Врахування номінальних обсягів кібербезпеки та безпеки охорони міцного здоров’я.
2. Обчислення реальних показників, що стосуються кібербезпеки та безпеки охорони міцного здоров’я.
3. Можливість порівняння вхідних даних з різних джерел.
4. Узгодженість показників інформаційної бази дослідження.
5. Врахування пріоритетності впливу показників.
6. Урахування існуючих та потенційних взаємозв’язків обраних показників.
7. Надання узагальненої оцінки рівня взаємозв’язків між обраними сферами.

Модель повинна бути достовірною, оперативною та системною, адекватно відображати взаємозв'язок між обраними показниками. Крім того, вона повинна відповідати потребам та рівню керівництва держав, щоб забезпечити її ефективне використання для прийняття важливих рішень.

1.4. Розробка математичної моделі

Перший етап. Формування даних. Перед розробкою математичної моделі необхідно зібрати та підготувати вхідні дані, які відображатимуть стан кібербезпеки та безпеки охорони міцного здоров’я країн світу. Статистичні дані зібрано за 2021р. з відкритих інформаційних джерел European Commission.

Формування даних – це процес збору, обробки та підготовки вхідної інформації для подальшого аналізу та використання. Цей етап включає в себе зібрання різноманітних даних з різних джерел, перевірку їхньої точності та достовірності, а також структурування та підготовку до подальшого використання.

Для розробки математичної моделі взаємозв'язків кібербезпеки та безпеки охорони міцного здоров’я країн світу необхідно підготувати вхідні дані, що включатимуть наступні показники:

- Показники, що характеризують кібербезеку: CS – Глобальний індекс кібербезпеки та його складові, CS1 – Правові заходи у сфері кібербезпеки; CS2 – Технічні заходи для забезпечення кібербезпеки; CS3 – Організаційні заходи, спрямовані на підвищення рівня кібербезпеки; CS4 – Розвиток потенціалу у сфері кібербезпеки; CS5 – Кооперативні заходи з іншими країнами та міжнародними організаціями.
- Показники, що характеризують безпеку у сфері охорони міцного здоров’я: HS – Глобальний індекс безпеки здоров'я та його складові – HS1 – Запобігання виникненню або поширенню патогенних мікроорганізмів; HS2 – Раннє виявлення та повідомлення про епідемії, що мають потенційне міжнародне значення; HS3 – Швидке реагування та пом'якшення наслідків поширення епідемій; HS4 – Достатня та надійна система охорони здоров'я для лікування хворих та захисту медичних працівників; HS5 – Зобов'язання щодо покращення національної спроможності, плани фінансування для усунення прогалин та дотримання глобальних норм; HS6 – Загальне середовище ризику та вразливість країни до біологічних загроз.

Ці дані є основою для подальшого аналізу та розробки математичної моделі, яка дозволить встановити взаємозв'язки між кібербезпекою та безпекою охорони міцного здоров’я та їх вплив на економіку країн світу.

Другий етап. Групування країн світу шляхом кластерного аналізу.

Кластерний аналіз базується на методі k-середніх (k-means clustering) [41] (формула 1.1):

$$\sum_{i=1}^{N} d(a_i, b_j(a_i))^2 \quad (1.1)$$

де d – метрика, a_i – і-ий об'єкт даних, $b_j(a_i)$ – центр кластера, якому на j-ій ітерації приписаний елемент

Цей метод є одним з найпоширеніших і найефективніших алгоритмів кластеризації. Основна ідея полягає в тому, щоб розділити набір даних на k груп або кластерів таким чином, щоб об'єкти в одному кластері були якомога більш схожими між собою, а об'єкти в різних кластерах - якомога більш відмінними один від одного.

Метод k-середніх виконується ітеративно та включає наступні кроки:

- Вибір числа кластерів k, яке бажано визначити заздалегідь або за допомогою евристичних методів.
- Ініціалізація початкових центрів кластерів (центроїдів). Центроїди можуть бути випадковими об'єктами з набору даних або обрані іншим чином.
- Повторення наступних кроків до тих пір, поки центроїди не стабілізуються: прив'язка кожного об'єкта до найближчого центроїда; перерахування центроїдів як середнього значення всіх об'єктів, які до них належать.
- Зупинка алгоритму, коли центроїди більше не змінюються або коли досягнуто задану кількість ітерацій.

Метод k-середніх дозволяє ефективно розділити набір даних на кластери і використовується для групування схожих об'єктів у великих наборах даних. В контексті аналізу взаємозв'язків кібербезпеки та безпеки охорони міцного здоров’я країн світу, кластерний аналіз допоможе виділити групи країн зі схожими характеристиками в цих сферах для подальшого дослідження та моделювання.

Третій етап. Визначення найвпливовіших факторів у кожній групі – Sigma-restricted parameterization – Univariate Tests of Significance – Pareto Chart of t-Values; кореляційний аналіз.

Після групування країн за допомогою кластерного аналізу, наступним етапом є визначення найвпливовіших факторів у кожній з отриманих груп. Для цього можна використовувати методи Sigma-restricted parameterization, Univariate Tests of Significance, та кореляційний аналіз. Крім того, можна побудувати Pareto Chart of t-Values для визначення найзначущіших факторів у кожній групі.

Короткий опис кожного з методів:

Sigma-restricted parameterization: Цей метод дозволяє враховувати вплив кількох змінних одночасно на результат. Він може бути особливо ефективним при аналізі великих об'ємів даних, де є багато потенційно важливих факторів.

Univariate Tests of Significance: Цей метод дозволяє визначити статистичну значущість кожного фактора окремо. Це допомагає зрозуміти, які саме змінні мають найбільший вплив на результат.

Pareto Chart of t-Values: Цей метод дозволяє візуалізувати вплив кожного фактора на результат у вигляді графіка Pareto. Він допомагає ідентифікувати та виділити найбільш важливі фактори серед усіх. Для обчислення t-значень (t-статистики) для кожного коефіцієнта регресії β у множинній лінійній регресії виглядає так (формула 1.2):

$$t = \frac{\hat{\beta}}{AB(\hat{\beta})} \qquad (1.2)$$

де: $\hat{\beta}$ – оцінка коефіцієнта регресії.

$AB(\hat{\beta})$ – стандартна помилка оцінки коефіцієнта регресії.

Кореляційний аналіз: Цей метод дозволяє визначити ступінь взаємозв'язку між різними змінними. Він допомагає виявити, які фактори взаємодіють між собою та як вони впливають на результат.

Використання цих методів допоможе визначити найважливіші фактори, які впливають на кібербезпеку та безпеку охорони міцного здоров’я в різних групах країн, що сприятиме подальшому аналізу та розробці математичної моделі.

Четвертий етап. Побудова множинної лінійної регресії для кожної групи – методу найменших квадратів (OLS-метод).

Після визначення найвпливовіших факторів у кожній групі країн, наступним етапом є побудова множинної лінійної регресії для кожної групи за допомогою методу найменших квадратів (OLS-метод).

Метод найменших квадратів є одним з найпоширеніших і найефективніших методів для побудови лінійної регресії. Онлайн OLS-метод полягає в тому, що він знаходить лінію, яка найкращим чином підганяється до набору даних, шляхом мінімізації суми квадратів відхилень між спостережуваними значеннями залежної змінної і значеннями, передбаченими моделлю.

Модель множинної лінійної регресії має вид:

Припустимо, ми маємо групу залежних змінних Q та k незалежних змінних B_1, B_2,…,B_k. Функція регресії виражається (формулою 1.3):

$$Q = \beta_0 + \beta_1 T_1 + \beta_2 T_2 + \ldots + \beta_k T_k + \varepsilon \qquad (1.3)$$

де: Q – залежна зміна.

B_1, B_2,…,B_k – коефіцієнти регресії, які потрібно оцінити.

ε - помилка моделі.

Побудова множинної лінійної регресії за допомогою методу найменших квадратів дозволить отримати математичну модель, яка описує взаємозв'язки між різними факторами кібербезпеки та безпеки охорони міцного здоров’я країн світу у кожній групі.

П’ятий етап. Виконання кореляційного аналізу для визначення наявності і величини статистичного зв’язку між факторами двох груп.

Після побудови множинної лінійної регресії для кожної групи країн, наступним етапом є виконання кореляційного аналізу для визначення наявності і величини статистичного зв’язку між факторами двох груп.

Кореляційний аналіз дозволяє визначити, наскільки сильно зв'язані між собою різні фактори. Зазвичай для цього використовується коефіцієнт кореляції Пірсона або інші методи виміру кореляції. Значення коефіцієнта кореляції може бути від -1 до +1, де -1 вказує на повний негативний зв'язок, +1 – на повний позитивний зв'язок, а 0 – на відсутність зв'язку. Для обчислення коефіцієнта кореляції Пірсона між двома змінними A і B виглядає так (вормула 1.4):

$$r = \frac{n(\sum_{i=1}^{n} a_i b_i) - (\sum_{i=1}^{n} a_i)(\sum_{i=1}^{n} b_i)}{\sqrt{[n\sum_{i=1}^{n} a_i^2 - (\sum_{i=1}^{n} a_i)^2]\,[n\sum_{i=1}^{n} b_i^2 - (\sum_{i=1}^{n} b_i)^2]}} \qquad (1.4)$$

де: n – кількість спостережень (пар значень A і B).

a_i та b_i – значення A і B відповідно для i-го спостереження

$\sum$ – сума всіх значень від i=1 до n

r – коефіцієнт кореляції.

Виконання кореляційного аналізу допоможе краще зрозуміти взаємозв'язки між факторами двох груп країн та визначити ті, які мають найбільший вплив на кібербезпеку та безпеку охорони міцного здоров’я.

Шостий етап. Проведення канонічний аналізу для виявлення причинно-наслідкового зв’язку між групами факторів

Канонічний аналіз є методом мультиплікативного моделювання, який дозволяє виявити лінійні залежності між двома наборами змінних, які представлені в матричному вигляді. Цей аналіз допомагає виявити, як один набір змінних впливає на інший, тобто визначити причинно-наслідкові зв'язки між групами факторів. Оцінка зв’язку між канонічними змінними E і D описується у вигляді наступної (формули 1.5):

$$\begin{cases} E = p_1 a_1 + p_2 a_2 + \ldots + p_x a_x \\ D = q_1 b_1 + q_2 b_2 + \ldots + q_y b_y \end{cases} \quad (1.5)$$

де pi , $(i = \overline{1,x})$ та qj , $(j = \overline{1,y})$, – відповідні ваги коефіцієнтів, що розраховуються при вирішенні задачі з власними значеннями

Проведення канонічного аналізу допоможе виявити причинно-наслідкові зв'язки між групами факторів у контексті кібербезпеки та безпеки охорони міцного здоров’я країн світу. Це сприятиме глибшому розумінню механізмів взаємодії між цими сферами та може служити основою для подальшого розвитку математичної моделі.

Узагальнюючи приведені у роботі етапи моделі, побудовано узагальнену схему економіко-математичного моделювання (таблиця 1.1).

Таблиця 1.1 – Узагальнена схема економіко-математичного моделювання

Вхідні дані:	Математичні співвідношення:	Вихідні змінні:
Показники, що характеризують кібербезеку (CS, CS1, CS2, CS3, CS4, CS5) Показники, що характеризують безпеку у сфері охорони здоров’я (HS, HS1, HS2, HS3, HS4, HS5, HS6)	$\sum_{i=1}^{N} d(a_i, b_j(a_i))^2$ $t = \frac{\hat{\beta}}{AB(\hat{\beta})}$ $Q = \beta_0 + \beta_1 T_1 + \beta_2 T_2 + \ldots + \beta_k T_k + \varepsilon$ $r = \frac{n(\sum_{i=1}^{n} a_i b_i) - (\sum_{i=1}^{n} a_i)(\sum_{i=1}^{n} b_i)}{\sqrt{[n\sum_{i=1}^{n} a_i^2 - (\sum_{i=1}^{n} a_i)^2]\left[n\sum_{i=1}^{n} b_i^2 - \left(\sum_{i=1}^{n} b_i\right)^2\right]}}$ $\begin{cases} E = p_1 a_1 + p_2 a_2 + \ldots + p_x a_x \\ D = q_1 b_1 + q_2 b_2 + \ldots + q_y b_y \end{cases}$ Керовані змінні: Кількість кластерів	Параметри регресії

Сьомий етап. Побудова регресійної моделі. Побудована буде лінійна регресії для аналізу взаємозв'язків між показниками кібербезпеки (CS) та показниками безпеки охорони здоров'я (HS).

РОЗДІЛ 2. ПЕРЕВІРКА АДЕКВАТНОСТІ МОДЕЛІ ТА ПРОПОЗИЦІЇ ПО ЇЇ ВИКОРИСТАННЮ

2.1 Перевірка адекватності побудованої математичної моделі

Щодо перевірки адекватності моделі на етапі кластерного аналізу зазначимо наступне. Кластеризація країн на основі ітеративного дивізійного методу k-середніх з використанням 13 показників дала можливість перевірити адекватність розбивки 190 країн на групи. Показники включали: 6 – показників, що характеризують кібербезеку, 7 – показників, що характеризують безпеку у сфері охорони міцного здоров'я. Для оцінки доцільності поділу на кластери було проведено дисперсійний аналіз, для обрання оптимальної кількості кластерів (від 3 до 10). Для здійснення оцінки та порівняння кластерів застосовано дисперсійний аналіз щодо обрання 3, 4, 5, 6, 7, 8,9 та 10 кластерів. Показники доцільності поділу на кластери є величини міжгрупових дисперсій, Between SS – повинні бути min, внутрішньогрупових дисперсій, Within SS – повинні max, величина критерію Фішера, F – повинно мати значення більше критичного, ймовірності можливого відхилення нульової гіпотези, p (свідчать про адекватність кластеризації) – повинно прямувати до 0 (для економічних досліджень - менше 0,05) (рисунок 2.1).

	Analysis of Variance (SpreadsheetCS_HS.sta)					
Variable	Between SS	df	Within SS	df	F	signif. p
CS	196453,7	2	35022,9	187	524,467	0,00000
CS1	5852,7	2	2438,8	187	224,373	0,00000
CS2	9375,1	2	2148,0	187	408,081	0,00000
CS3	7946,3	2	2567,6	187	289,364	0,00000
CS4	8761,0	2	2416,0	187	339,048	0,00000
CS5	7487,6	2	2566,7	187	272,757	0,00000
HS	27980,2	2	7262,6	187	360,220	0,00000
HS1	42350,8	2	16891,3	187	234,427	0,00000
HS2	46266,8	2	27107,0	187	159,587	0,00000
HS3	14028,3	2	13522,3	187	96,997	0,00000
HS4	45633,6	2	19093,7	187	223,463	0,00000
HS5	13538,3	2	20155,7	187	62,801	0,00000
HS6	17677,6	2	23902,9	187	69,148	0,00000

Рисунок 2.1 – Аналіз адекватності кластеризації за 2021 рік

Отже, аналіз результатів формувань країн світу, від 3 до 10 кластерів, визначив найбільш адекватним 3-кластерне групування країн, а кластеризація є адекватною, оскільки всі показники є статистично значущі (при чому найкращі рівні для 3 кластерів).

Щодо перевірки адекватності моделі на етапі Sigma-restricted parameterization, регресійного аналізу (потужним інструментом для виявлення причинно-наслідкових зв'язків, прогнозування та прийняття обґрунтованих рішень у різних сферах) (рисунок 2.2). Summary Statistics містить підсумкові статистичні дані. Маємо результат по регресійному аналізу кібербезпеки. Де Multiple R= 1,00 – коефіцієнт множинної кореляції, показує силу лінійного зв'язку між предикторами та залежною змінною; значення 1,00 вказує на ідеальну кореляцію. Multiple R^2= 1,00 – коефіцієнт детермінації, показує, яку частину варіації залежної змінної пояснюють незалежні змінні; значення 1,00 вказує на те, що 100% варіації пояснюються моделлю. Adjusted R^2 = 1,00 – коригований коефіцієнт детермінації, враховує кількість предикторів у моделі; значення 1,00 вказує на те, що модель повністю пояснює варіацію залежної змінної навіть з урахуванням кількості предикторів. F(5,183): 36347,20 – статистика F-тесту для загальної значущості моделі; велике значення вказує на те, що модель є статистично значущою. p: 0,00 – рівень значущості (p-value), значення 0,00 вказує на те, що модель є статистично значущою на дуже високому рівні (зазвичай $p < 0,05$ вважається значущим). Std.Err. of Estimate:1,12 – стандартна помилка оцінки; вказує на середню величину похибки при прогнозуванні значень залежної змінної за допомогою моделі.

	Summary Statistics; DV: CS (Spreadshe
Statistic	Value
Multiple R	1,00
Multiple R?	1,00
Adjusted R?	1,00
F(5,183)	36347,2
p	0,00
Std.Err. of Estimate	1,12

	Summary Statistics; DV: HS (Spreadshe
Statistic	Value
Multiple R	1,00
Multiple R?	1,00
Adjusted R?	1,00
F(6,182)	11625,3
p	0,00
Std.Err. of Estimate	0,71

Рисунок 2.2 – Результати оцінки якості та адекватності регресійної моделі

Маємо результат регресійного аналізу охорони здоров'я: Multiple R= 1,00 – значення 1,00 вказує на ідеальну кореляцію. Multiple R^2= 1,00 – значення 1,00 вказує на те, що 100% варіації пояснюються моделлю. Adjusted R^2 = 1,00 – значення 1,00 вказує на те, що модель повністю пояснює варіацію залежної змінної навіть з урахуванням кількості предикторів. F(6,182): 11625,35 – велике значення вказує на те, що модель є статистично значущою. p: 0,00 – значення 0,00 вказує на те, що модель є статистично значущою на дуже високому рівні (зазвичай $p < 0,05$ вважається значущим). Std.Err. of Estimate:0,71 – стандартна помилка оцінки. Високі значення Multiple R та R^2 (1,00) вказують на те, що модель дуже добре пояснює варіацію залежної змінної. Низьке значення p (0,00) підтверджує, що модель є статистично значущою. Стандартна помилка оцінки Std.Err. of Estimate:0,71 – дає уявлення про точність прогнозів моделі.

Додатковий є аналіз, що містить результати тесту порівняння сум квадратів для всієї моделі та залишкових сум квадратів (Test of SS Whole Model vs. SS Residual) у Statistica для змінної CS та HS (рисунок 2.3). Значення Multiple R, R^2 та Adjusted R^2 дуже високі, що свідчить про те, що модель дуже добре пояснює варіацію залежної змінних (CS) та (HS) . Дуже низьке p-значення та високе значення критерію Фішера (F) підтверджують, що модель є статистично значущою. Низьке значення MS Residual показує, що залишкова варіація, яка не пояснена моделлю, є дуже малою, що додатково підтверджує високу якість моделі.

	Test of SS Whole Model vs. SS Residual (Spreadsheet3.sta)										
Dependnt Variable	Multiple R	Multiple R?	Adjusted R?	SS Model	df Model	MS Model	SS Residual	df Residual	MS Residual	F	p
CS	0,99949	0,99899	0,99896	229174,	5	45834,8	230,768	183	1,26102	36347,2	0,00

	Test of SS Whole Model vs. SS Residual (Spreadsheet3.sta)										
Dependnt Variable	Multiple R	Multiple R?	Adjusted R?	SS Model	df Model	MS Model	SS Residual	df Residual	MS Residual	F	p
HS	0,99869	0,99739	0,99731	35056,3	6	5842,71	91,4703	182	0,50258	11625,3	0,00

Рисунок 2.3 – Порівняння сум квадратів для всієї моделі кібербезпеки та індексу безпеки здоров'я та залишкових сум квадратів (Test of SS Whole Model vs. SS Residual).

Цей аналіз підтверджує, що побудована модель є адекватною, має високу пояснювальну здатність і є статистично значущою для аналізу змінних CS та HS.

Щодо перевірки адекватності моделі на етапі канонічного аналізу зазначимо наступне: R – канонічний коефіцієнт кореляції (показує силу та напрям зв’язку між групами показників, R прагне до 1); Chi2 – критерій адекватності (Chi2 прагне до безкінечності); p – ймовірність відхилення гіпотези (показує, що зв’язок між групами показників не існує, p прагне до 0) (рисунок 2.4).

	Canonical Analysis Summary (Sprea Canonical R: ,78771 Chi?(30)=195,90 p=0,0000	
N=189	Left Set	Right Set
No. of variables	5	6
Variance extracted	100,000%	93,4088%
Total redundancy	54,7373%	39,9887%
Variables: 1	CS1	HS1
2	CS2	HS2
3	CS3	HS3
4	CS4	HS4
5	CS5	HS5
6		HS6

Рисунок 2.4 – Перевірка адекватності канонічного аналізу між групою показників кібербезпеки та безпеки охорони здоров’я

Можемо зробити висновки, що значення 0.78771 вказує на сильний зв'язок між змінними лівого (CS) та правого (HS) наборів. Значення Chi2 = 195.90 при p = 0.0000 свідчить про те, що цей зв'язок є статистично значущим і мало ймовірно виник випадково. Отже, канонічний аналіз є адекватний.

2.2 Побудова методики проектувальних розрахунків

На першому етапі сформовано вхідну базу даних.

Другим етапом зроблено кластерний аналіз. Кластеризація країн на основі методу k-середніх проведено з використанням 13 показників (6 – показників, що характеризують кібербезеку, 7 – показників, що характеризують безпеку у сфері охорони міцного здоров’я) для 190 країн світу. Аналіз результатів формувань країн світу у групи від 3 до 10 кластерів, визначив найбільш доцільним 3-кластерне групування країн (рисунки Б.1 – Б.3). Аналіз кластерів допомагає оцінити, наскільки добре кожна країна вписується у свій кластер і які країни мають найподібніші (або відмінні) характеристики від середніх значень кластеру. Групування країн виконано на підставі показника – евклідові відстані, що відображає, наскільки кожна країна віддалена від середнього значення (центроїда) для цього кластеру.

З рисунку Б.1 Members of Cluster Number 1 and Distances from Respective Cluster видно список країн першого кластеру, а також відстань кожної країни від центроїда цього кластеру. Він містить 55 країн з різних континентів і регіонів, що вказує на те, що ці країни мають подібні характеристики за показниками кібербезпеки та безпеки здоров'я. Це Домініканська Республіка (5.89), Північна Македонія (5.80), Руанда (5.88) – країни мають показники, найближчі до середніх значень кластеру, що може вказувати на стабільний розвиток у сферах кібербезпеки та безпеки здоров'я. Молдова (6.73), Узбекистан (6.76), Парагвай (7.61) та інші мають подібні характеристики до центроїда, але можуть мати певні відхилення у деяких показниках. Монако (11.82), Ліхтенштейн (15.84), Панама (17.67) – мають найбільші відхилення від середніх значень кластеру, вони значно відрізняються за деякими показниками кібербезпеки та безпеки здоров'я, або можуть мати унікальні характеристики, що робить їх менш подібними до інших країн у кластері. Країни першого кластеру мають середній рівень розвитку кібербезпеки та безпеки здоров'я, але існують суттєві варіації між країнами. Країни, які знаходяться далеко від центроїда (з великою відстанню), можуть потребувати індивідуальних стратегій розвитку для підвищення рівня кібербезпеки та безпеки здоров'я до середнього рівня кластеру. Країни з невеликою відстанню від центроїда

можуть служити прикладом для інших країн у кластері, оскільки вони найбільше відповідають середнім значенням і можуть мати стабільні та ефективні політики у сферах кібербезпеки та охорони здоров'я.

Проаналізуємо другий кластер (рисунок Б.2). Більшість країн в кластері є європейськими: країни Західної Європи (Бельгія, Німеччина, Франція), Східної Європи (Польща, Литва, Латвія) та інші які мають високий рівень глобального індексу кібербезпеки та глобального індексу безпеки здоров’я. Країни Азії: Південна Корея (11,80), Китай (9,14), Японія (5,84), Сінгапур (9,53) та інші мають далеку відстань від центроїда, що мають високий рівень глобального індексу та середній рівень глобального індексу безпеки здоров’я. Північна та Південна Америка: відстані до центроїда варіюються. Аргентина (13,17) та США (14,25) мають великі відстані. Спільними рисами для даних країн є те, що вони є лідерами по показнику: глобального індексу безпеки здоров’я за місцем розташування. Австралія та Океанія: Австралія (10,42) та Нова Зеландія (7,69) представляють цей регіон і знаходяться на відносно великій відстані, ці країни мають великий рівень глобального індексу та середній рівень глобального індексу безпеки здоров’я. Отже, другий кластер має країни, які мають високий рівень глобального індекс кібербезпеки та середній рівень глобального індексу безпеки здоров’я.

Проаналізуємо третій кластер (рисунок Б.3). Цей кластер має найбільшу кількість країн. Найбільше країн у кластері представлені африканським континентом, включаючи Східну Африку (Кенія, Танзанія), Західну Африку (Нігерія, Гана), Центральну Африку (Демократична Республіка Конго, Чад) та Південну Африку (Південна Африка, Зімбабве). Відстані варіюються від близьких до центроїда (Ангола, Ботсвана) до середніх (Бенін, Камерун) і великих (Екваторіальна Гвінея). Спільною рисою цих країн є низький рівень глобального індексу кібербезпеки та низький рівень глобального індексу безпеки здоров’я. Азія: представлені країни з середніми та великими відстанями до центроїда:, Бангладеш (7,74), Казахстан (8,86) та інші, мають високий рівень глобального індексу кібербезпеки та середній рівень

глобального індексу безпеки здоров’я. Південна Америка Болівією (7,27), Гайаною (9,24) та Центральна Америка Гаїті (6,84), Гватемала (10,40), що мають середні та великі відстані до центроїда, мають низький рівень глобального індексу кібербезпеки та середній рівень глобального індексу безпеки здоров’я. Отже, третій кластер включає країни з різних континентів і різних рівнів економічного розвитку, що свідчить про певні спільні риси в показниках кібербезпеки та безпеки охорони здоров'я.

Вивчаючи статистичні дані зі стандартизованими середніми значеннями та евклідовими відстанями, ми можемо отримати більш детальне розуміння результатів кластерного аналізу для країн світу, зокрема стосовно двох дослідницьких областей, і визначити ключові характеристики кожної сформованої групи. Так, чим менше значення евклідової відстані від центру групування по кожному кластеру тих країн в даному кластері більш схожі за станом розвитку кібербезпеки та охорони здоров'я (рисунок 2.5 та рисунок 2.6).

	Cluster Means (SpreadsheetCS_HS.s		
Variable	Cluster No. 1	Cluster No. 2	Cluster No. 3
CS	74,4885	89,3240	17,8217
CS1	17,3485	18,9132	6,9960
CS2	14,6667	17,8130	2,2311
CS3	14,1260	16,8508	2,5755
CS4	13,7909	17,6993	2,3018
CS5	14,6854	17,9893	3,8707
HS	39,0836	58,5673	28,6314
HS1	30,5400	51,8142	15,0581
HS2	32,3000	57,5795	19,0895
HS3	35,0418	52,1122	31,3546
HS4	32,8545	56,1122	17,8965
HS5	45,7527	62,4469	42,0348
HS6	57,9909	70,2612	46,6651

Рисунок 2.5 – Середні значення показників характеристики взаємозв’язків обраних сфер в межах 3 виділених кластерів.

Cluster Number	Euclidean Distances between Clusters (SpreadsheetCS_HS.sta) Distances below diagonal Squared distances above diagonal		
	No. 1	No. 2	No. 3
No. 1	0,0000	230,684	366,015
No. 2	15,1883	0,000	979,308
No. 3	19,1315	31,293	0,000

Рисунок 2.6 – Евклідові відстані між 3 виділеними кластерами

Третій етап передбачає визначення релевантних факторів, що визначають стан кібербезпеки та безпеки здоров'я на основі методик Sigma-restricted parameterization та кореляційного аналізу.

Перший кроком третього етапу – виконання Univariate Tests of Significance факторів, що визначають стан кібербезпеки та охорони здоров'я. Вона включає значення сум квадратів (SS), ступенів свободи (Deg. of Freedom), середніх квадратів (MS), статистики F і значень p для кожного з ефектів (рисунок 2.7). Усі показники (CS1-CS5, HS1-HS6) мають p-значення 0.000000, що менше 0.05, це означає, що усі показники статистично значущі на високому рівні довіри. Вони впливають на кластеризацію значною мірою. Значення критерію Фішера дуже високі для всіх показників, що свідчить про високу дисперсію між групами у порівнянні з дисперсією всередині груп. Це підтверджує значущість показників. Середні квадрати для показників (MS) значно більші за середні квадрати помилки (Error MS), що додатково підтверджує, що варіація між групами значно перевищує варіацію всередині груп.

Univariate Tests of Significance for CS (Spreadsh
Sigma-restricted parameterization
Effective hypothesis decomposition

Effect	SS	Degr. of Freedom	MS	F	p
Intercept	0,000	1	0,000	0,000	1,00000
"CS1"	1721,45	1	1721,45	1365,11	0,00000
"CS2"	1396,31	1	1396,31	1107,28	0,00000
"CS3"	1634,14	1	1634,14	1295,87	0,00000
"CS4"	1150,32	1	1150,32	912,21	0,00000
"CS5"	1792,55	1	1792,55	1421,49	0,00000
Error	230,76	183	1,261		

Univariate Tests of Significance for HS (Spreadshee
Sigma-restricted parameterization
Effective hypothesis decomposition

Effect	SS	Degr. of Freedom	MS	F	p
Intercept	0,0797	1	0,0797	0,159	0,69100
"HS1"	373,349	1	373,349	742,85	0,00000
"HS2"	567,623	1	567,623	1129,40	0,00000
"HS3"	331,599	1	331,599	659,78	0,00000
"HS4"	369,364	1	369,364	734,93	0,00000
"HS5"	443,229	1	443,229	881,90	0,00000
"HS6"	545,068	1	545,068	1084,53	0,00000
Error	91,470	182	0,502		

Рисунок 2.7 – Univariate Tests of Significance факторів, що визначають стан кібербезпеки та стан безпеки охорони здоров'я

Наступним побудовано Pareto Chart of t-Values значущості впливу факторів (рисунок 2.8). На рисунку 2.8 показані 5 смуг перетину індикаторів CS1 – CS5 та 6 смуг перетину індикаторів HS1 – HS6. Червона лінія межа критичного рівня допуску за стандартом Фішера (p)) 0,05 і означає їх статистичну значущість. Тобто всі показники показують 100% впливу, тому є релевантними факторами, що визначають кібербезпеки та безпеки охорони

здоров’я, що пропонується використовувати в подальшому дослідженні. Діаграма Парето допомагає ранжувати показники від найвпливовішого до показника з найменш впливового.

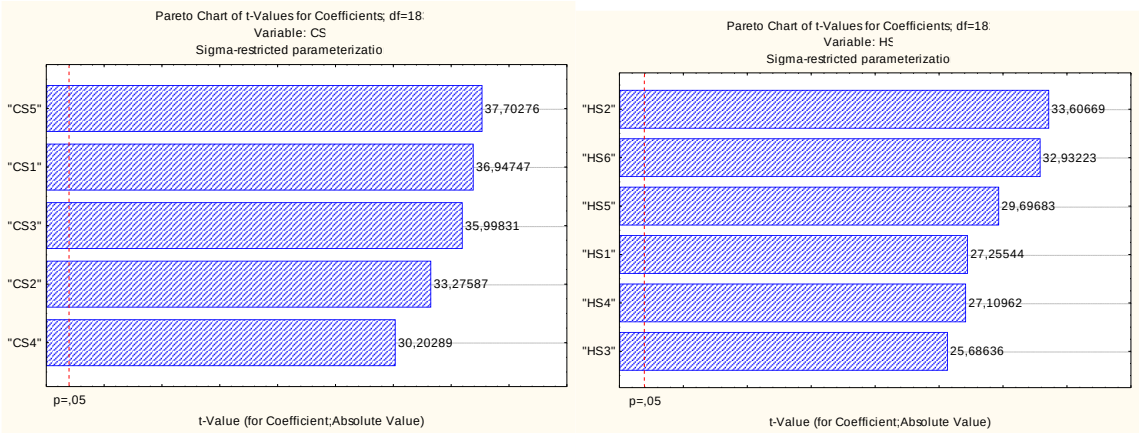


Рисунок 2.8 – Pareto Chart of t-Values значущості впливу факторів, що визначають стан кібербезпеки та стан безпеки охорони здоров’я

Наступний проведено кореляційний аналіз. Побудовано кореляційну матрицю взаємозалежності релевантних факторів, що визначають стан визначають стан кібербезпеки (рисунок 2.9).

Correlations (Spreadsheet3.sta)
Marked correlations are significant at p < ,05
N=189 (Casewise deletion of missing data)

Variable	CS	CS1	CS2	CS3	CS4	CS5
CS	1,00	0,92	0,96	0,95	0,96	0,94
CS1	0,92	1,00	0,84	0,85	0,85	0,82
CS2	0,96	0,84	1,00	0,90	0,91	0,88
CS3	0,95	0,85	0,90	1,00	0,89	0,86
CS4	0,96	0,85	0,91	0,89	1,00	0,90
CS5	0,94	0,82	0,88	0,86	0,90	1,00

Correlations (Spreadsheet3.sta)
Marked correlations are significant at p < ,05
N=189 (Casewise deletion of missing data)

Variable	HS	HS1	HS2	HS3	HS4	HS5	HS6
HS	1,00	0,91	0,88	0,82	0,92	0,74	0,73
HS1	0,91	1,00	0,76	0,64	0,86	0,61	0,64
HS2	0,88	0,76	1,00	0,69	0,77	0,67	0,45
HS3	0,82	0,64	0,69	1,00	0,70	0,54	0,62
HS4	0,92	0,86	0,77	0,70	1,00	0,59	0,63
HS5	0,74	0,61	0,67	0,54	0,59	1,00	0,42
HS6	0,73	0,64	0,45	0,62	0,63	0,42	1,00

Рисунок 2.9 – Кореляційна матриця взаємозалежності релевантних факторів, що визначають стан кібербезпеки та стан безпеки охорони здоров’я

На рисунку 2.9 видно, що розрахункові коефіцієнти кореляції між результативним показником CS та факторними показниками мають наступний зв’язок: сильний зв’язок – коефіцієнт кореляції між CS2 (p=0.84), CS3 (p=0.95), CS4 (p=0.86) та CS5 (p=0.82), CS3 (p=0.80), CS4 (p=0.91) та CS5 (p=0.85) та

CS4 (p=0.90) та CS5 (p=0.90). Всі складові компоненти HS мають значущі кореляції з загальним індексом, що підтверджує їх важливість для загальної оцінки безпеки здоров'я. HS1 та HS4 є найвпливовішими компонентами, що вказує на важливість запобігання та готовності системи охорони здоров'я. HS6 має найслабші кореляції з іншими компонентами, що може вказувати на те, що загальне середовище ризику та вразливість мають специфічні фактори, які не завжди пов'язані з іншими аспектами безпеки здоров'я.

Таким чином, для країн Світу результати проведених перевірок релевантності впливу досліджуваних факторів, що виконано методом Univariate Tests of Significance, побудовою Pareto Chart of t-Values значущості впливу факторів, побудови кореляційної матриці взаємозалежності релевантних факторів, встановлено найвпливовіші фактори: CS1, CS2, CS3, CS4, CS5,HS1,HS2,HS3,HS4,HS5,HS6.

Наступний четвертий етап передбачає визначення сили та напрямку впливу релевантних факторів, що визначають стан кібербезпеки і безпеки охорони здоров’я; побудова множинної лінійної регресії з використанням методу найменших квадратів (OLS-метод).

Першим кроком є визначення інтенсивності впливу, а також напряму впливу відповідних факторів, виявлених для країн світу, для визначення стану кібербезпеки та безпеки охорони здоров’я, для побудови множинної лінійної регресії. Щоб побудувати складну лінійну регресію, ми спочатку використовуємо всі 5 факторів, які визначають ступінь ефективності кібербезпеки країн та всі 6 факторів, які визначають ступінь безпеки охорони здоров’я і впливають на ефективний коефіцієнти CS (рівень кібербезпеки) та HS (безпеки охорони здоров’я). На малюнку 2.10 показаний розрахований показник регресійного аналізу взаємозв'язку між рівнем глобальний індекс кібербезпеки і безпеки охорони здоров’я.

Regression Summary for Dependent Variable: CS (Spreadsheet3.s
R= ,99949690 R?= ,99899406 Adjusted R?= ,99896657
F(5,183)=36347, p<0,0000 Std.Error of estimate: 1,1230

N=189	Beta	Std.Err. of Beta	B	Std.Err. of B	t(183)	p-level
Intercept			-0,00995	0,19900	-0,0500	0,96017
CS1	0,18297	0,00495	0,96526	0,02612	36,9474	0,00000
CS2	0,22225	0,00667	0,99538	0,02991	33,2758	0,00000
CS3	0,22121	0,00614	1,03769	0,02882	35,9983	0,00000
CS4	0,21321	0,00705	0,97067	0,03213	30,2028	0,00000
CS5	0,21502	0,00570	1,03164	0,02736	37,7027	0,00000

Regression Summary for Dependent Variable: HS (Spreadsheet3.s
R= ,99869793 R?= ,99739755 Adjusted R?= ,99731176
F(6,182)=11625, p<0,0000 Std.Error of estimate: ,70893

N=189	Beta	Std.Err. of Beta	B	Std.Err. of B	t(182)	p-level
Intercept			-0,10883	0,27335	-0,3981	0,69100
HS1	0,22101	0,00810	0,17063	0,00626	27,2554	0,00000
HS2	0,24396	0,00725	0,16898	0,00502	33,6066	0,00000
HS3	0,15627	0,00608	0,17667	0,00687	25,6863	0,00000
HS4	0,22419	0,00827	0,16613	0,00612	27,1096	0,00000
HS5	0,15535	0,00523	0,15868	0,00534	29,6968	0,00000
HS6	0,18057	0,00548	0,16608	0,00504	32,9322	0,00000

Рисунок 2.10 – Розрахункові показники регресійного аналізу залежності між глобальний індекс кібербезпеки і безпеки охорони здоров'я.

З рисунку 2.10 видно, що усі фактори, що визначають глобальний індекс кібербезпеки і безпеки охорони здоров'я є статистично значущими. Побудована модель є достатньо адекватною згідно розрахункових показників регресійного аналізу. Згідно показників рисунку 2.10, формулюємо модель лінійної множинної регресійної залежності для кібербезпеки та для безпеки охорони здоров'я (формула 2.1 – 2.2):

$$CS = 0{,}009952 - 0{,}965267 * CS1$$
$$+0{,}995385 * CS2 + 1{,}037696 * CS3 + 0{,}970677 * CS4 + 1{,}031642 * CS5, \quad (2.1)$$
$$HS = 0{,}108832 - 0{,}170634 * HS1$$
$$+0{,}168987 * HS2 + 0{,}176670 * HS3 + 0{,}166137 * HS4 + 0{,}15689 * HS5,$$
$$+0{,}166083 * HS6, \quad (2.2)$$

Отримана модель є адекватною та точною. Усі обрані у модель фактори є статистично значущими, про що свідчать критерії Стьюдента та p-рівні (що є не вище допустимого критичного рівня 0,05). Графік "Normal Probability Plot of Residuals" використовується для перевірки нормальності розподілу залишків (рисунок 2.11).

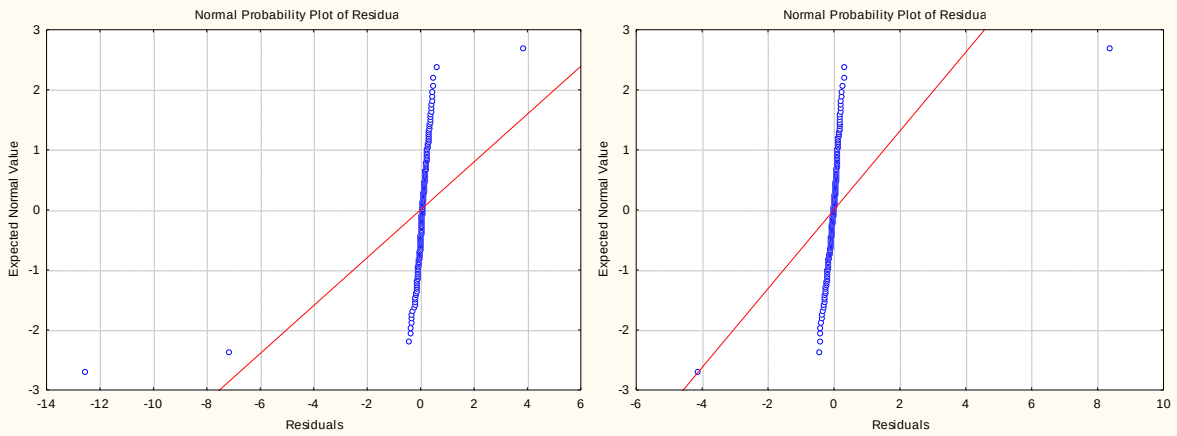


Рисунок 2.11 – Графічне зображення відповідності нормальному закону розподілу залишків лінійної регресійної моделі залежності між рівнем кібербезпеки і безпекою охорони здоров'я.

Наступний п'ятий етап є виконання кореляційного аналізу для визначення наявності і величини статистичного зв'язку між факторами двох груп. Рисунок 2.12 представляє кореляційний аналіз між змінними, що характеризують кібербезпеку (CS) та безпеку у сфері охорони здоров'я (HS).

Correlations (Spreadsheet3.sta)
Marked correlations are significant at p < ,0500
N=189 (Casewise deletion of missing data)

Variable	HS	HS1	HS2	HS3	HS4	HS5	HS6
CS	0,75	0,72	0,67	0,54	0,67	0,49	0,62
CS1	0,68	0,65	0,61	0,48	0,63	0,45	0,56
CS2	0,73	0,72	0,66	0,54	0,67	0,47	0,57
CS3	0,68	0,65	0,62	0,49	0,60	0,45	0,57
CS4	0,73	0,72	0,66	0,53	0,65	0,46	0,61
CS5	0,71	0,68	0,63	0,52	0,63	0,47	0,60

Рисунок 2.12 – Кореляційний аналіз між змінними, що характеризують кібербезпеку (CS) та безпеку у сфері охорони здоров'я (HS)

Загалом спостерігається позитивний зв'язок між заходами кібербезпеки та заходами у сфері охорони здоров'я. Це свідчить про те, що країни, які вкладають ресурси у кібербезпеку, також мають тенденцію до інвестування в безпеку охорони здоров'я. Найсильніші кореляції спостерігаються між загальними індексами (CS та HS), а також між конкретними заходами (CS1 і

HS1, CS2 і HS2). Це вказує на важливість комплексного підходу до забезпечення безпеки в обох сферах. Кореляції між іншими показниками (наприклад, CS3, CS4, CS5) та HS показують помірну позитивну кореляцію, що свідчить про певний взаємозв'язок, але не настільки сильний, як у випадку з першими двома групами показників. Всі кореляції є статистично значущими при $p < 0.05$, що підтверджує наявність реальних зв'язків між змінними.

На шостому етапі виконано канонічний аналіз (рисунок 2.4). Лівий набір змінних (CS1-CS5) повністю пояснює свою спільну дисперсію, тоді як правий набір (HS1-HS6) пояснює 93.4088% своєї. Лівий набір може пояснити 54.7373% дисперсії правого набору це свідчить про те, що показники лівого набору (CS) мають значний вплив і можуть бути хорошими предикторами для показників правого набору (HS)., в той час як правий набір може пояснити 39.9887% дисперсії лівого набору. Це менше, ніж надлишковість лівого набору, що вказує на менший, але все ще суттєвий вплив правого набору змінних (HS) на лівий набір (CS).

Наступний сьомий етап - побудова регресійної моделі. Побудована лінійна регресія для аналізу взаємозв'язків між показниками кібербезпеки (CS) та показниками безпеки охорони здоров'я (HS) (рисунок 2.13).

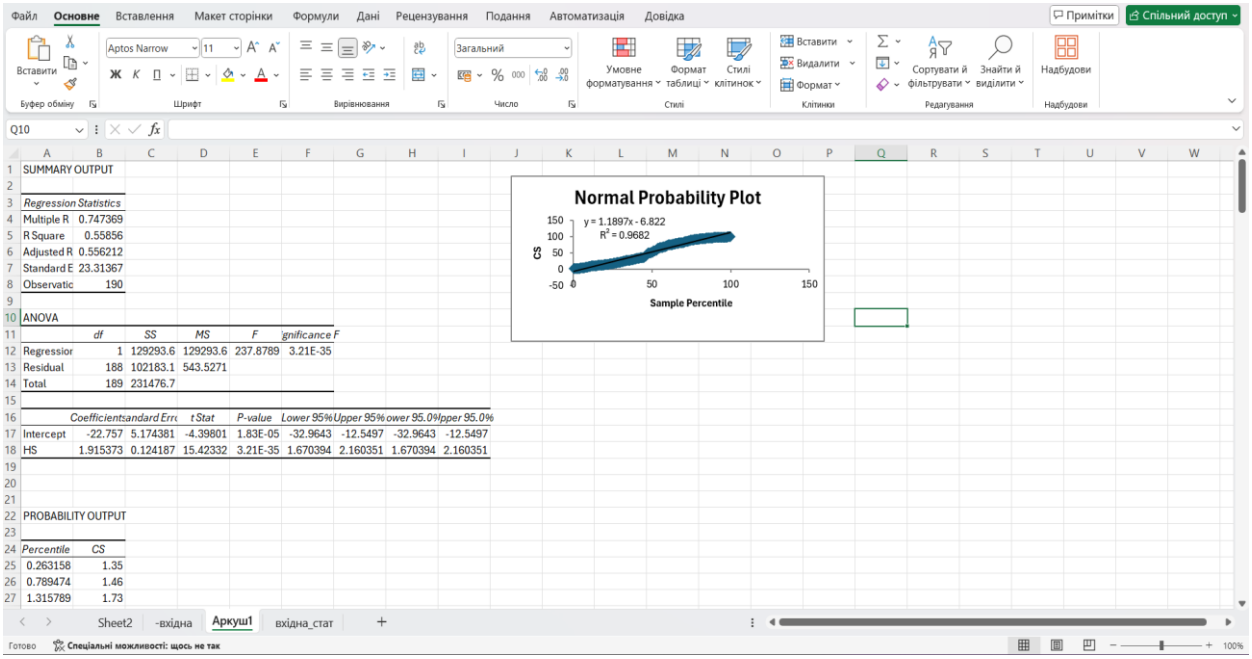


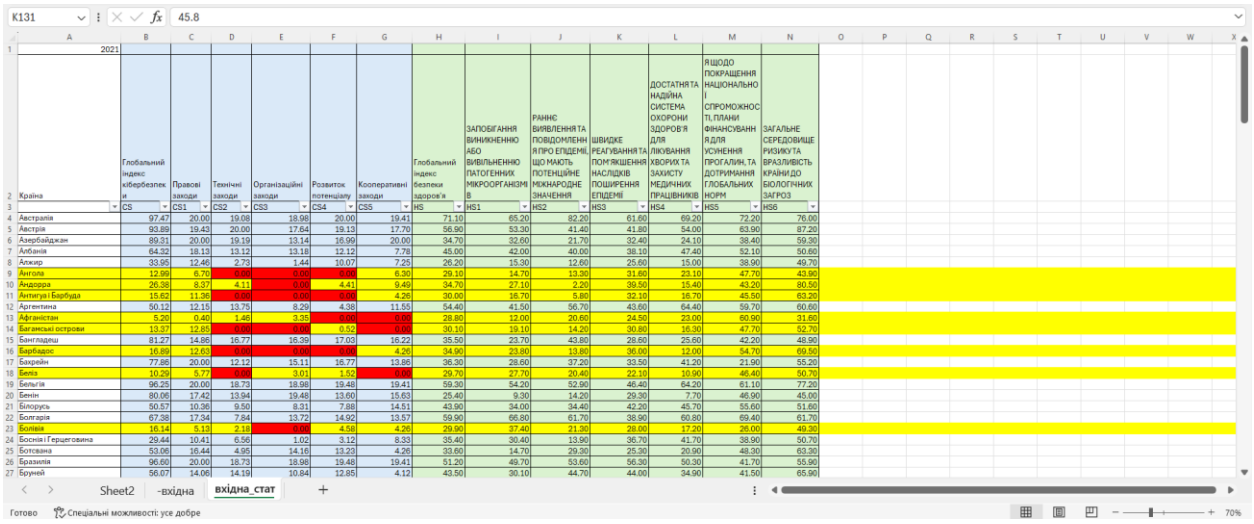
Рисунок 2.13 – Регресійна модель

Модель однофакторної лінійної регресії, де залежною змінною є CS, а незалежною змінною – HS, показує, що існує значущий позитивний зв'язок між показниками кібербезпеки (CS) та безпеки охорони здоров'я (HS). Значення Multiple R варіюється від 0 до 1, де 1 вказує на ідеальну кореляцію, а 0 – на відсутність кореляції. У цьому випадку значення 0.747369 свідчить про високий рівень кореляції між залежною змінною та предиктором (HS). Коефіцієнт детермінації R^2=0.55856 вказує на те, що близько 55.86% варіації залежної змінної пояснюється моделлю. Обидва коефіцієнти (вільний член і коефіцієнт при змінній HS) є статистично значущими.

2.3 Розробка програмного застосунку для автоматизації методики розрахунків

Починаючи роботу, ми використовували інструментарій Microsoft Excel.

Було спрогнозовано дані показників, які були відсутні в інформаційних джерелах (рисунок 2.14).



2021	Глобальний індекс кібербезпеки	Правові заходи	Технічні заходи	Організаційні заходи	Розвиток потенціалу	Кооперативні заходи	Глобальний індекс безпеки здоров'я	ЗАПОБІГАННЯ ВИНИКНЕННЮ АБО ВИВІЛЬНЕННЮ ПАТОГЕННИХ МІКРООРГАНІЗМІВ	РАННЄ ВИЯВЛЕННЯ ТА ПОВІДОМЛЕННЯ ПРО ЕПІДЕМІЇ, ЩО МАЮТЬ ПОТЕНЦІЙНЕ МІЖНАРОДНЕ ЗНАЧЕННЯ	ШВИДКЕ РЕАГУВАННЯ ТА ПОМ'ЯКШЕННЯ НАСЛІДКІВ ПОШИРЕННЯ ЕПІДЕМІЇ	ДОСТАТНЯ ТА НАДІЙНА СИСТЕМА ОХОРОНИ ЗДОРОВ'Я ДЛЯ ЛІКУВАННЯ ХВОРИХ ТА ЗАХИСТУ МЕДИЧНИХ ПРАЦІВНИКІВ	ЯЩОДО ПОКРАЩЕННЯ НАЦІОНАЛЬНОЇ СПРОМОЖНОСТІ, ПЛАНИ ФІНАНСУВАННЯ ДЛЯ УСИНЕННЯ ПРОГАЛИН ТА ДОТРИМАННЯ ГЛОБАЛЬНИХ НОРМ	ЗАГАЛЬНЕ СЕРЕДОВИЩЕ РИЗИКУ ТА ВРАЗЛИВІСТЬ КРАЇНИ ДО БІОЛОГІЧНИХ ЗАГРОЗ
Країна	CS	CS1	CS2	CS3	CS4	CS5	HS	HS1	HS2	HS3	HS4	HS5	HS6
Австралія	97.47	20.00	19.08	18.98	20.00	19.41	71.10	65.20	82.20	61.60	69.20	72.20	76.00
Австрія	93.89	19.43	20.00	17.64	19.13	17.70	56.90	53.30	41.40	41.80	54.00	63.90	87.20
Азербайджан	89.31	20.00	19.19	13.14	16.99	20.00	34.70	32.60	21.70	32.40	24.10	38.40	59.30
Албанія	64.32	18.13	13.12	13.18	12.12	7.78	45.00	42.00	40.00	38.10	47.40	52.10	50.60
Алжир	33.95	12.46	2.73	1.44	10.07	7.25	26.20	15.30	12.60	25.60	15.00	38.90	49.70
Ангола	12.96	6.70	0.00	0.00	0.00	6.30	29.10	14.70	13.30	31.60	23.10	47.70	43.90
Андорра	26.38	8.37	4.11	0.00	4.41	9.49	34.70	27.10	2.20	39.50	15.40	43.20	80.50
Антигуа і Барбуда	15.62	11.36	0.00	0.00	0.00	4.26	30.00	16.70	5.80	32.10	16.70	45.50	63.20
Аргентина	50.12	12.15	13.75	8.29	4.36	11.55	54.40	41.50	56.70	43.60	64.40	59.70	60.60
Афганістан	5.20	0.40	1.48	3.35	0.00	0.00	28.80	12.00	20.60	24.50	23.00	60.90	31.60
Багамські острови	13.37	12.85	0.00	0.00	0.52	0.00	30.10	19.10	14.20	30.80	16.30	47.70	52.70
Бангладеш	81.27	14.86	16.77	16.39	17.03	16.22	35.50	23.70	43.80	28.60	25.60	42.20	48.90
Барбадос	16.89	12.63	0.00	0.00	0.00	4.26	34.90	23.80	13.80	36.00	12.00	54.70	69.50
Бахрейн	77.86	20.00	12.12	15.11	16.77	13.86	36.30	28.60	37.20	33.50	41.20	21.90	55.20
Беліз	10.29	5.77	0.00	3.01	1.52	0.00	29.70	27.70	20.40	22.10	10.90	46.40	50.70
Бельгія	96.25	20.00	18.73	18.98	19.48	19.41	59.30	54.20	52.90	46.40	64.20	61.10	77.20
Бенін	80.06	17.42	13.94	19.48	13.60	15.63	25.40	9.30	14.20	29.30	7.70	46.90	45.00
Білорусь	50.57	10.36	9.50	8.31	7.88	14.51	43.90	34.00	34.40	42.20	45.70	55.60	51.60
Болгарія	67.38	17.34	7.84	13.72	14.92	13.57	59.90	66.80	61.70	38.90	60.80	69.40	61.70
Болівія	16.14	5.13	2.18	0.00	4.58	4.26	29.90	37.40	21.30	28.00	17.20	26.00	49.30
Боснія і Герцеговина	29.44	10.41	6.56	1.02	3.12	8.33	35.40	30.40	13.90	36.70	41.70	38.90	50.70
Ботсвана	53.06	16.44	4.95	14.16	13.23	4.26	33.60	14.70	29.30	25.30	20.90	48.30	63.30
Бразилія	96.60	20.00	18.73	18.98	19.48	19.41	51.20	49.70	53.60	56.30	50.30	41.70	55.90
Бруней	56.07	14.06	14.19	10.84	12.85	4.12	43.50	30.10	44.70	44.00	34.90	41.50	65.90

Рисунок 2.14 – Прогнозування даних за допомогою Microsoft Excel

Для кластерного аналізу використовувалося програмне забезпечення STATISTICA, пакет «Multivariate Exploratory Techniques» – «Cluster Analysis» – k- means clustering (метод к-середніх) – analysis of variance (дисперсійний аналіз) (рисунок 2.15).

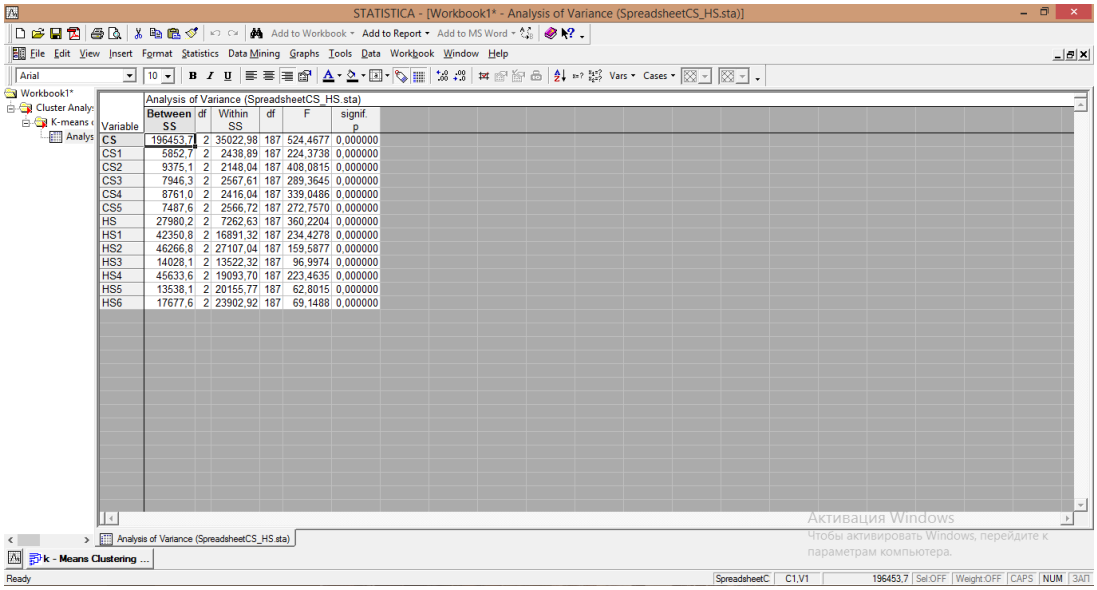


Рисунок 2.15 – Дисперсійний аналізу за допомогою програмного забезпечення STATISTICA

Для кластерного аналізу також використовувалося програмне забезпечення STATISTICA, пакет «Multivariate Exploratory Techniques» – «Cluster Analysis» – k- means clustering (рисунок 2.16, Б.4, Б.5).

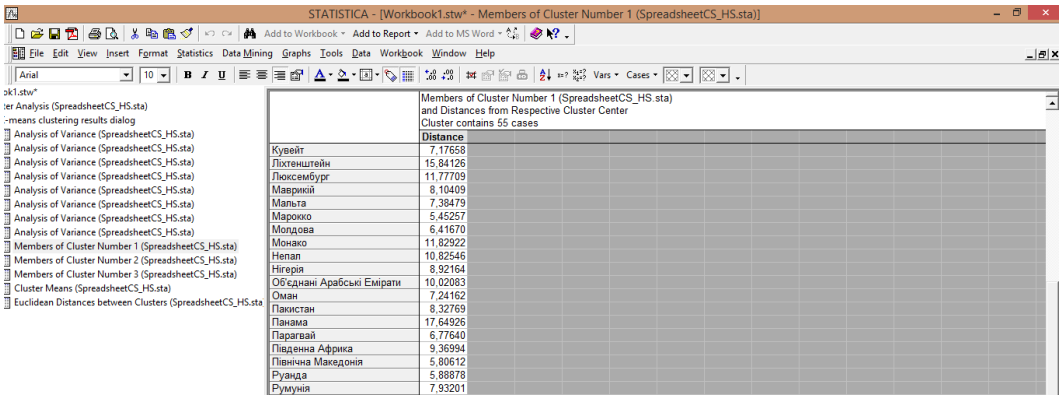


Рисунок 2.16 – Розподіл країн на умовні кластери за допомогою програмного забезпечення STATISTICA

Визначення найвпливовіших факторів виконано в ПЗ STATISTICA шляхом Sigma-restricted parameterization - Univariate Tests of Significance - Pareto Chart of t-Values (рисунок 2.17, Б.6 – Б.8).

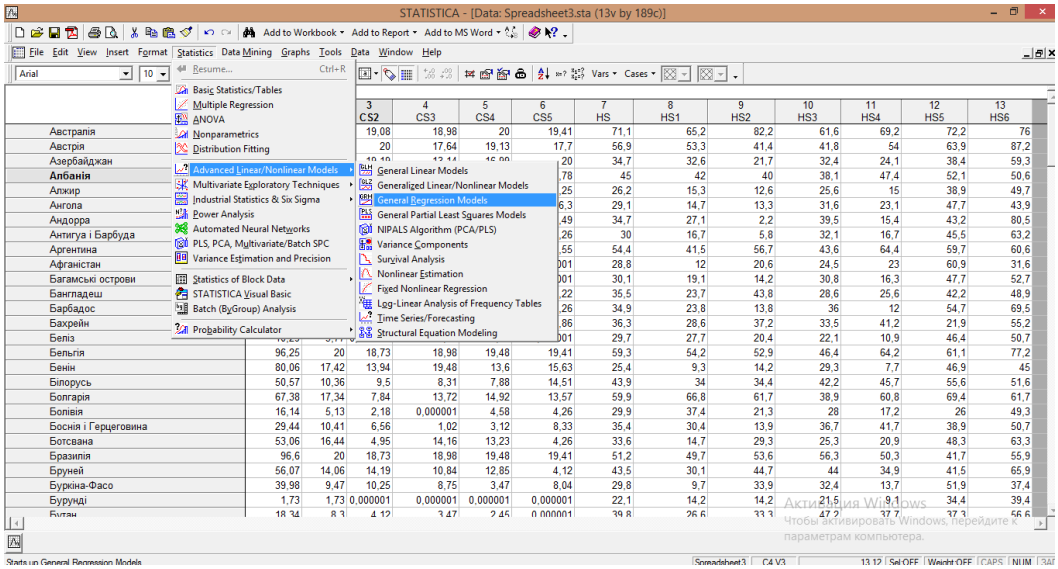


Рисунок 2.17 – Застосування функції «Advanced Linear/Nonlinear Models» – «General Regression Models» у програмному забезпеченні STATISTICA

Проведено кореляційний аналіз між різними змінними у програмному забезпеченні STATISTICA (рисунок 2.18).

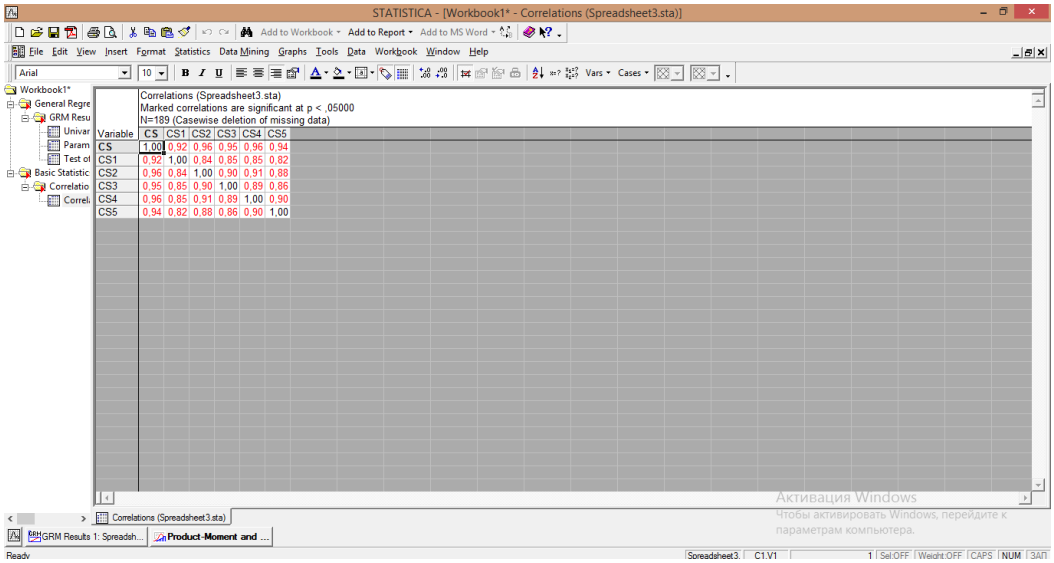


Рисунок 2.18 – Кореляційний аналіз

За допомоги функції – «Multiple Regression» сформовано множинну лінійну регресію для кожної групи кібербезпеки– методу найменших квадратів (OLS-метод) (рисунок 2.19, Б.9, Б.10).

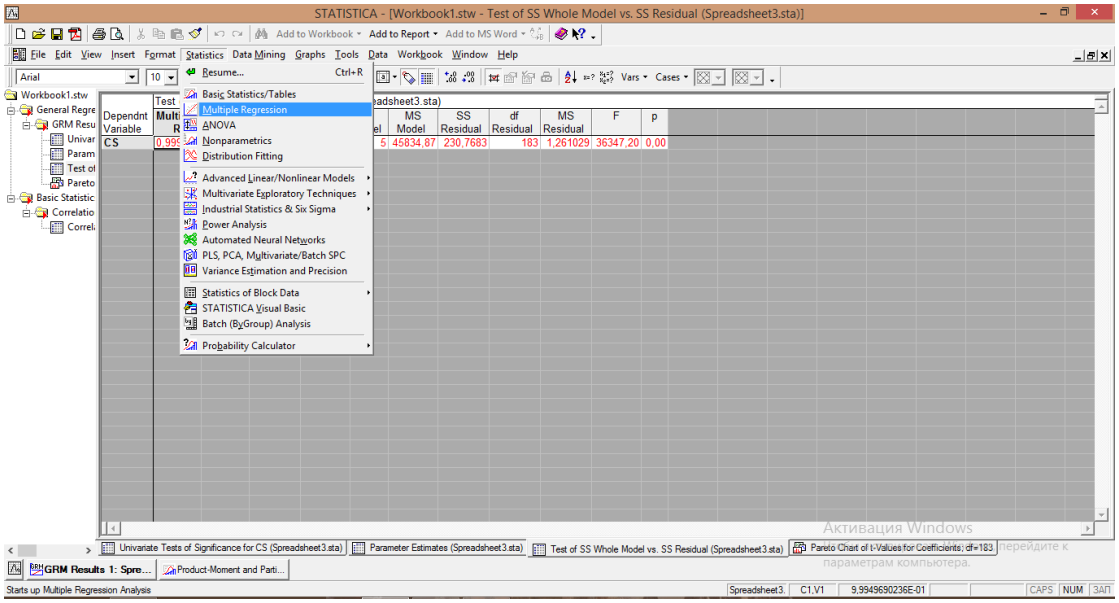


Рисунок 2.19 – Формуємо множинну лінійну регресію для кожної групи кібербезпеки – методу найменших квадратів (OLS-метод)

За допомогою функції «Multiple Regression» побудований графік "Normal Probability Plot of Residuals" (рисунок 2.20).

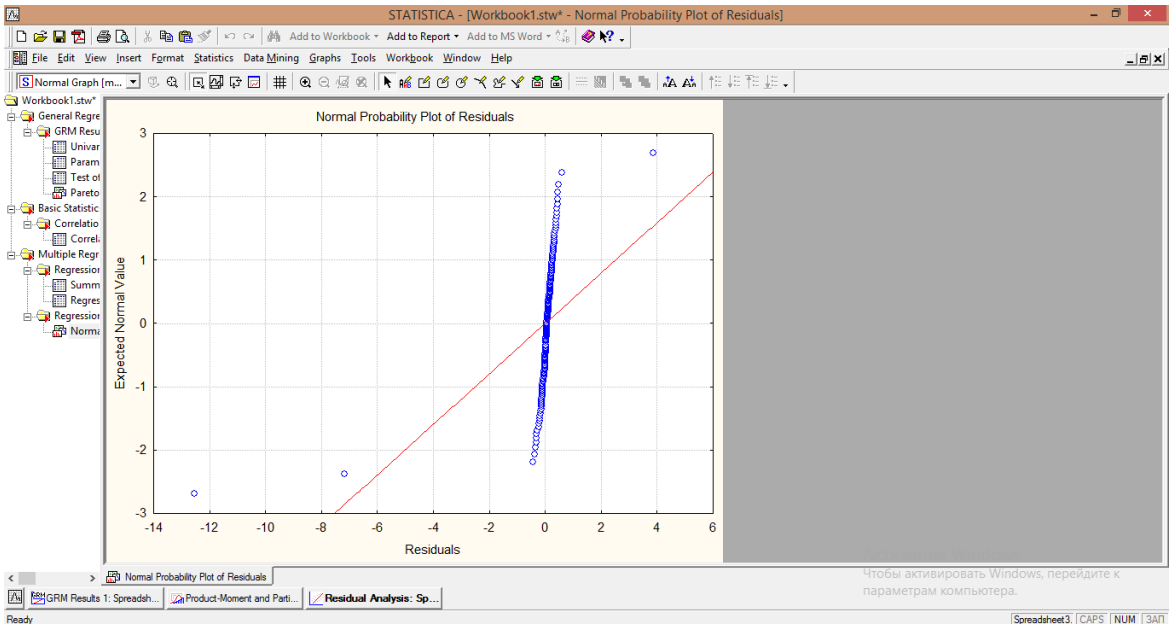


Рисунок 2.20 – Графік "Normal Probability Plot of Residuals"

Проведення кореляційного аналізу було проведено шляхом програмного пакету Statistica, шляхом застосування функції «Correlation matrices» – «Principal Components and Classification Analysis» на основі вхідної вибірки даних (рисунок 2.21, Б.11, Б.12).

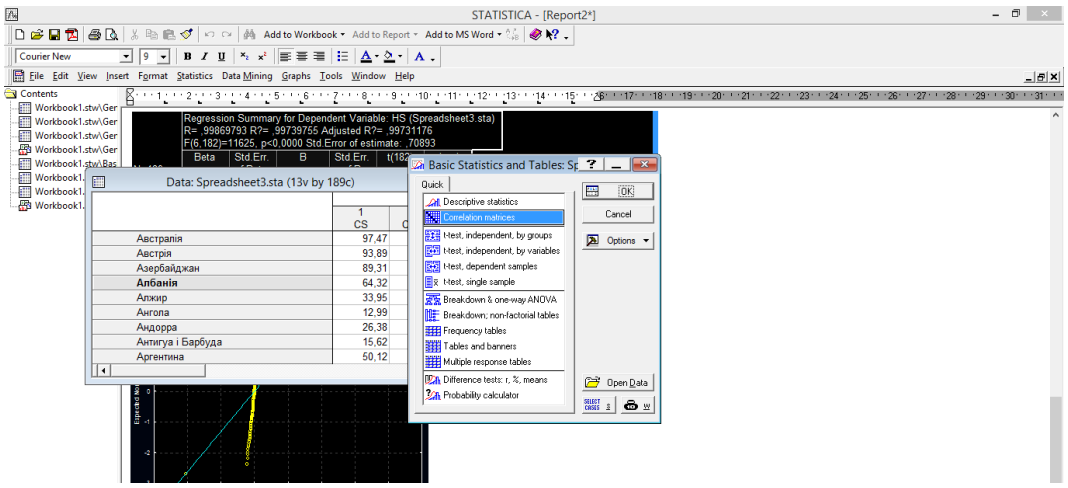


Рисунок 2.21 – Застосування функції «Correlation matrices» у програмному забезпеченні STATISTICA

Канонічний аналіз було проведено за допомогою програмного пакету Statistica 10 та Statistica Portable, шляхом застосування функції «Multivariate Exploratory Techniques» – «Canonical Analysis» на основі вхідної вибірки даних (рисунок 2.22, Б.13, Б.14).

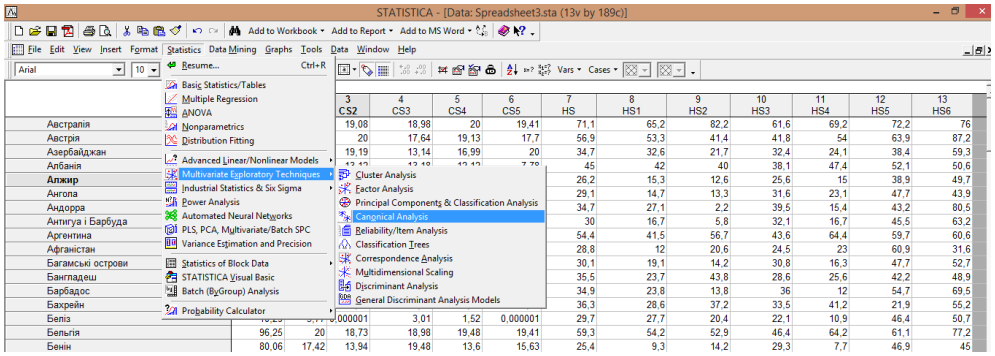


Рисунок 2.22 – Застосування функції функції «Multivariate Exploratory Techniques» – «Canonical Analysis» у програмному забезпеченні STATISTICA

Побудова регресійної моделі за допомогою пакета інструментів Microsoft Excel, за допомогою функції функції вкладці дані «Дані» – «Data Analysis»– «Regression» (рисунок 2.23).

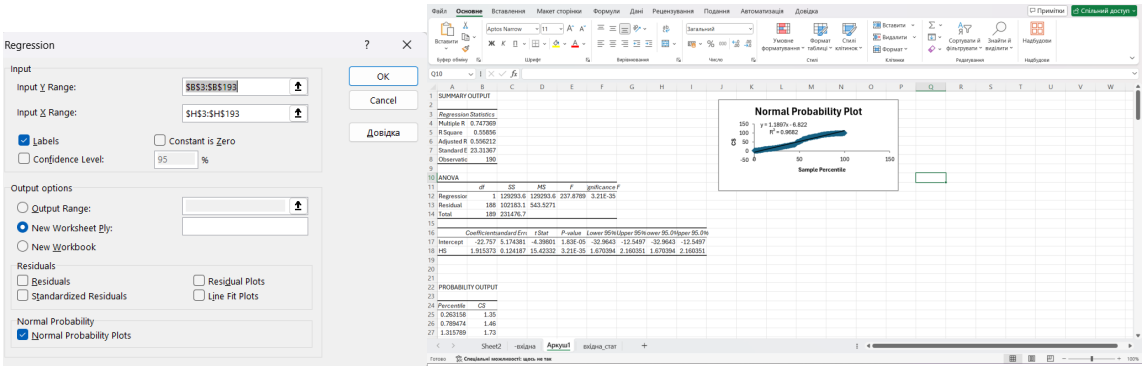


Рисунок 2.23 – Побудова регресійної моделі за допомогою пакета інструментів Microsoft Excel

ВИСНОВКИ

Тема дослідження виявилася надзвичайно актуальною та важливою у сучасному світі, де віртуальна та фізична безпека нарівні здоров'ям населення стають одними з ключових пріоритетів для керівництва країн.

Аналіз предметної галузі та виявлення найбільш вагомих параметрів об’єкта дослідження показав, що кібербезпека та безпека охорони міцного здоров’я є тісно пов’язаними та взаємозалежними сферами. Серед найбільш важливих параметрів були ідентифіковані вразливість медичних інформаційних систем, зловмисні кібератаки на медичні установи, витік та втрата даних пацієнтів, а також порушення конфіденційності та цілісності медичних даних.

Огляд сучасного стану моделювання об’єкта дослідження свідчив про нестачу комплексних математичних моделей, що належним чином ураховують взаємозв'язки між кібербезпекою та безпекою охорони здоров'я. Це підкреслило необхідність розробки нової моделі, яка б враховувала всі аспекти цієї проблеми та забезпечувала більш ефективний аналіз та прийняття стратегічних рішень.

Постановка задачі моделювання та формування вимог до моделі чітко визначили цілі дослідження та встановили критерії ефективності розробленої моделі. Результатом цього став процес розробки математичної моделі, в якому були використані різноманітні методи, такі як кластерний аналіз, регресійний аналіз, кореляційний аналіз та канонічний аналіз. Ці методи дозволили виявити взаємозв'язки між різними факторами та найвагоміші параметри об'єкта дослідження.

Отже, використання економіко-математичного моделювання є перспективним підходом для аналізу взаємозв'язків кібербезпеки та безпеки охорони міцного здоров’я. Розроблена модель може служити основою для прийняття стратегічних рішень у сферах кібербезпеки та охорони здоров'я,

сприяючи підвищенню рівня безпеки та захисту медичних даних та здоров'я населення в цілому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Що таке кібербезпека? Заходи забезпечення кібербезпеки. URL: https://dan-it.com.ua/uk/blog/chto-takoe-kiberbezopasnost-mery-obespechenija-kiberbezopasnosti/ (дата звернення: 1.05.2024).

2. Кібербезпека: Все Що Необхідно Знати Кожному Користувачу Мережі Інтернет. URL: https://www.ukraine-lifehacker.com/kiberbezpeka-vse-shcho-neobkhidno-znaty (дата звернення: 1.05.2024).

3. Alqudhaibi, A., Krishna, A., Jagtap, S. et al. Cybersecurity 4.0: safeguarding trust and production in the digital food industry era. Discov Food, 2024. 4, 2. URL: https://doi.org/10.1007/s44187-023-00071-7 (Last accessed: 12.04.2024).

4. Diaz Ferreyra, N.E., Vidoni, M., Heisel, M. Cybersecurity discussions in Stack Overflow: a developer-centred analysis of engagement and self-disclosure behaviour. Soc. Netw. Anal. Min., 2024. 14, 16. URL: https://doi.org/10.1007/s13278-023-01171-z (Last accessed: 12.04.2024).

5. Faith Fatokun, Zalizah Awang, Suraya Hamid, Johnson O. Fatokun and Azah Norman. Cybersecurity Knowledge Deterioration and the role of Gamification Intervention. Journal of Advanced Research in Applied Sciences and Engineering Technology, 2024. 43, 1. pp.66–94. URL: https://doi.org/10.37934/araset.43.1.6694 (Last accessed: 12.04.2024).

6. Hossain, M.A., Islam, M.S. Enhanced detection of obfuscated malware in memory dumps: a machine learning approach for advanced cybersecurity. Cybersecurity, 2024. 7, 16. URL: https://doi.org/10.1186/s42400-024-00205-z (Last accessed: 12.04.2024).

7. Hossain, M.A., Islam, M.S. Enhanced detection of obfuscated malware in memory dumps: a machine learning approach for advanced cybersecurity. Cybersecurity, 2024. 7, 16. URL: https://doi.org/10.1186/s42400-024-00205-z (Last accessed: 12.04.2024).

8. Що таке кібербезпека? Як стати спеціалістом з кібербезпеки? URL: https://nofluffjobs.com/uk/log/robota-v-it/kiberbezpeka-scho-ce-take-ta-jak-staty-specjalistom-z-kiberbezpeky/ (дата звернення: 1.05.2024).

9. Основні види кібербезпеки в контексті захисту та обробки персональних даних. URL: https://bsoprivacygroup.com/cyber-cecurity/ (дата звернення: 1.05.2024).

10. Типи кібератак. URL: https://experience.dropbox.com/uk-ua/resources/cyber-security (дата звернення: 1.05.2024).

11. Cyber security: State of the art, challenges and future directions. URL: https://www.sciencedirect.com/science/article/pii/S2772918423000188 (Last accessed: 1.05.2024).

12. What are the 6 types of cyber security? URL: https://cypfer.com/resource/what-are-the-6-types-of-cyber-security/ (Last accessed: 1.05.2024).

13. Types of Cyber Security. URL: https://www.educba.com/types-of-cyber-security/ (Last accessed: 1.05.2024).

14. Health care. URL: https://en.wikipedia.org/wiki/Health_care (Last accessed: 1.05.2024).

15. Охорона здоров'я в Україні. URL: https://uk.wikipedia.org/wiki/Охорона_здоров%27я_в_Україні (дата звернення: 1.05.2024).

16. Ahmed, S.T., Mahesh, T., Srividhya, E. Towards blockchain based federated learning in categorizing healthcare monitoring devices on artificial intelligence of medical things investigative framework. BMC Med Imaging, 2024. 24, 105. URL: https://doi.org/10.1186/s12880-024-01279-4 (Last accessed: 21.04.2024).

17. Dotsenko, T., & Kuzmenko, M. Cyber fraud as a threat to the sustainable development of the health care system: a systematic bibliometric analysis. *Sustainable Development of Economy*, 2023. 2(47), pp. 50-57. URL: https://doi.org/10.32782/2308-1988/2023-47-7 (Last accessed: 21.04.2024).

18. Maresova, P., Rezny, L., Bauer, P. Nonpharmacological intervention therapies for dementia: potential break-even intervention price and savings for selected risk factors in the European healthcare system. BMC Public Health, 2024. 24, 1293. URL: https://doi.org/10.1186/s12889-024-18773-7 (Last accessed: 21.04.2024).

19. Meyer, S.B., Brown, P., Calnan, M. Development and validation of the Trust in Multidimensional Healthcare Systems Scale (TIMHSS). Int J Equity Health, 2024. 23, 94. URL: https://doi.org/10.1186/s12939-024-02162-y (Last accessed: 21.04.2024).

20. Souza, P., Haselkorn, T., Baima, J. *et al.* A healthcare claims analysis to identify and characterize patients with suspected X-Linked Myotubular Myopathy (XLMTM) in the Brazilian Healthcare System. Orphanet J Rare Dis, 2024. 19, 188. URL: https://doi.org/10.1186/s13023-024-03144-7 (Last accessed: 21.04.2024).

21. Класифікація основних моделей медичних систем у світі та шлях України. URL: https://ingeniusua.org/articles/klasyfikatsiya-osnovnykh-modeley-medychnykh-system-u-sviti-ta-shlyakh-ukrayiny (дата звернення: 1.05.2024).

22. Методичні вказівки до практичних занять з теми : «Основні моделі систем охорони здоров’я» для самостійної підготовки до практичних занять із дисципліни «Пропедевтика громадського здоров’я» / укладачі: зав. каф., д. м. н., проф. В. А. Сміянов., ст. викл. О.І Сміянова. – Суми: Сумський державний університет, 2020. URL: https://pubhealth.med.sumdu.edu.ua/wp-content/uploads/2021/02/MI-T15-Public-health-propaedeutics.pdf (дата звернення: 1.05.2024).

23. Safety Culture and Health Care. URL: https://blogs.cdc.gov/niosh-science-blog/2020/07/09/hc-safety-culture/ (Last accessed: 1.05.2024).

24. Workplace hazards. URL: https://staysafeapp.com/blog/6-types-of-workplace-hazard/ (Last accessed: 1.05.2024).

25. What are workplace hazards? URL: https://safetyculture.com/topics/workplace-hazards/ (Last accessed: 1.05.2024).

26. Types of Hazards in the Workplace. URL: https://publichealth.tulane.edu/blog/types-of-hazards-in-the-workplace/ (Last accessed: 1.05.2024).

27. Що таке моделювання. URL: https://dimitroova.blogspot.com/p/blog-page_7.html (дата звернення: 1.05.2024).

28. Метод моделювання. URL: https://buklib.net/books/35332/ (дата звернення: 1.05.2024).

29. Iqbal H. Sarker, Helge Janicke, Mohamed Amine Ferrag, Alsharif Abuadbba. Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions towards automation, intelligence and transparent cybersecurity modeling for critical infrastructures. Internet of Things, 2024. URL: https://www.sciencedirect.com/science/article/pii/S2542660524000520 (Last accessed: 17.04.2024).

30. Kumar M, Harsha B, Tesfaye L. 4 AI-driven cybersecurity modeling using quantum computing for mitigation of attacks in IOT-SDN network. Quantum-Safe Cryptography Algorithms and Approaches: Impacts of Quantum Computing on Cybersecurity, 2023. p.37-48. URL: https://doi.org/10.1515/9783110798159-004 (Last accessed: 17.04.2024).

31. Nurul Alieyah Azam, Alya Geogiana Buja, Nor Masri Sahri, Rabiah Ahmad, Nur Fadly Habidin, Shekh Faisal Abdul Latip, Mohamad Yusof Darus, Mohd Shahril Hussin, & Saharudin Saat. A Light Review on Cyber Security Awareness Models for the Elderly. Journal of Advanced Research in Applied Sciences and Engineering Technology, 2024. 44(1). pp. 31–45. URL: https://doi.org/10.37934/araset.44.1.3145 (Last accessed: 17.04.2024).

32. Redhu, R., Narwal, E., Gupta, S. Software implementation of systematic polar encoding based PKC-SPE cryptosystem for quantum cybersecurity. Sci Rep, 2024. 14, 9994. URL: https://doi.org/10.1038/s41598-024-60767-3 (Last accessed: 17.04.2024).

33. Tehrani, M.G., Sultanow, E., Buchanan, W.J. Stabilized quantum-enhanced SIEM architecture and speed-up through Hoeffding tree algorithms enable

quantum cybersecurity analytics in botnet detection. Sci Rep, 2024. 14, 1732. URL: https://doi.org/10.1038/s41598-024-51941-8 (Last accessed: 17.04.2024).

34. What Is Threat Modeling? Definition, Process, Examples, and Best Practices. URL: https://www.spiceworks.com/it-security/network-security/articles/what-is-threat-modeling-definition-process-examples-and-best-practices/ (Last accessed: 1.05.2024).

35. Daniel Asuquo, Kingsley Attai, Okure Obot, Moses Ekpenyong, Christie Akwaowo, Kiirya Arnold, Faith-Michael Uzoka. Febrile disease modeling and diagnosis system for optimizing medical decisions in resource-scarce settings. Clinical eHealth, 2024. 7. pp. 52-76, URL: https://doi.org/10.1016/j.ceh.2024.05.001 (Last accessed: 21.04.2024).

36. Lee, J.T., Crettenden, I., Tran, M. Methods for health workforce projection model: systematic review and recommended good practice reporting guideline. Hum Resour Health, 2024. 22, 25. URL: https://doi.org/10.1186/s12960-024-00895-z (Last accessed: 21.04.2024).

37. Putzier, M., Khakzad, T., Dreischarf, M. Implementation of cloud computing in the German healthcare system. npj Digit. Med., 2024. 7, 12. URL: https://doi.org/10.1038/s41746-024-01000-3 (Last accessed: 21.04.2024).

38. Wei, D., Wong, L.P., He, X. Healthcare utilisation and economic burden of migraines among bank employees in China: a probabilistic modelling study. J Headache Pain, 2024. 25, 60. URL: https://doi.org/10.1186/s10194-024-01763-w (Last accessed: 21.04.2024).

39. Global Healthcare: 4 Major National Models And How They Work. URL: https://www.verawholehealth.com/blog/global-healthcare-4-major-national-models-and-how-they-work (Last accessed: 1.05.2024).

40. Role of Private Enterprises in making Government Healthcare Services Better. URL: https://telradsol.com/role-of-private-enterprises-in-better-healthcare-services/ (Last accessed: 1.05.2024).

41. Vasylieva, T.; Gavurova, B.; Dotsenko, T.; Bilan, S.; Strzelec, M.; Khouri, S. The Behavioral and Social Dimension of the Public Health System of

European Countries: Descriptive, Canonical, and Factor Analysis. Int. J. Environ. Res. Public Health, 2023, 20. 4419. URL: https:// doi.org/10.3390/ijerph20054419 (Last accessed: 21.04.2024).

ДОДАТКИ

ДОДАТОК А

SUMMARY

Savchenko D.D. Economic-Mathematical Modeling of the Interrelationships of Cyber Security and Health Care Security of the Countries of the World. Sumy State University, Sumy, 2024.

In today's digital world, where virtual reality is intertwined with real life, issues of cyber security and health security are becoming more and more relevant and important. The growing dependence on information technologies brings its own challenges and threats that affect the economic, social and medical aspects of society.

The purpose of the work is to study and deepen the theoretical aspects of cyber security and health care security, to identify the main factors and to develop a structural and logical model of the interrelationships of cyber security and health care security in the countries of the world. The work describes the essence and main aspects of the concepts of cyber security and health care security, the current state of modeling of the object under study, the development of a structural and logical scheme of their interrelationships. An economic-mathematical model of the interrelationships of cyber security and health care security of the countries of the world was built, and its adequacy was checked.

Keywords: cyber security, health care security, cluster analysis, Sigma-restricted parameterization, Univariate Tests of Significance, Pareto Chart of t-Values, correlation analysis, least squares method (OLS method), canonical analysis.

АНОТАЦІЯ

Савченко Д.Д. Економіко-математичне моделювання взаємозв'язків кібербезпеки та безпеки охорони здоров’я країн світу. Сумський державний університет, Суми, 2024 рік.

В сучасному цифровому світі, де віртуальна реальність переплітається з реальним життям, питання кібербезпеки та безпеки міцного здоров'я стають дедалі більш актуальними та важливими. Зростання залежності від інформаційних технологій вносить свої виклики і загрози, які впливають на економічний, соціальний та медичний аспекти суспільства.

Метою роботи є вивчення та поглиблення теоретичних аспектів кібербезпеки та безпеки охорони здоров’я, виявлення основних факторів та розробка структурно-логічної моделі взаємозв'язків кібербезпеки та безпеки охорони здоров’я країн світу. В роботі охарактеризовано сутність та основні аспекти понять кібербезпеки та безпеки охорони здоров’я, сучасного стану моделювання досліджуваного об’єкту, розробка структурно-логічної схеми їх взаємозв'язків. Було побудовано економіко-математичну модель взаємозв'язків кібербезпеки та безпеки охорони здоров’я країн світу, перевірена її адекватність.

Ключові слова: канонічний аналіз кібербезпека, безпека охорони здоров’я, кластерний аналіз, кореляційний аналіз, метод найменших квадратів (OLS-метод), Pareto Chart of t-Values, Sigma-restricted parameterization, Univariate Tests of Significance.

ДОДАТОК Б

	Members of Cluster Number 1 and Distances from Respectiv Cluster contains 55 cases
	Distance
Азербайджан	6,5740
Албанія	7,3339
Бангладеш	5,9215
Бахрейн	7,4405
Бенін	11,9709
Білорусь	9,2406
Ботсвана	9,7107
Бруней	7,9038
В'єтнам	9,9884
Гана	5,9892
Домініканська Республіка	5,9838
Еквадор	18,5900
Єгипет	11,1518
Замбія	10,7917
Йорданія	4,8514
Індія	8,7091
Іран (Ісламська Республіка)	7,9234
Ісландія	10,3481
Казахстан	9,9113
Кенія	10,7291
Киргизстан	10,2270
Кіпр	6,6687
Коста-Ріка	4,5098
Кот-д'Івуар	8,2176
Куба	8,9659
Кувейт	7,1765
Ліхтенштейн	15,8412
Люксембург	11,7770
Маврикій	8,1040
Мальта	7,3847
Марокко	5,4525
Молдова	6,4167
Монако	11,8292
Непал	10,8254
Нігерія	8,9216
Об'єднані Арабські Емірати	10,0208
Оман	7,2416
Пакистан	8,3276
Панама	17,6492
Парагвай	6,7764
Південна Африка	9,3699
Північна Македонія	5,8061
Руанда	5,8887
Румунія	7,9320
Саудівська Аравія	9,9424
Сербія	8,2298
Танзанія	10,5008
Туніс	8,9903
Уганда	8,9110
Узбекистан	7,3026
Україна	6,6199
Уругвай	8,7125
Філіппіни	8,0330
Чорногорія	8,5325
Шрі-Ланка	8,3696

Рисунок Б.1 – Склад та характеристика першого кластера країн світу в розрізі станів обраних сфер згідно показника евклідових відстаней

	Members of Cluster Number 2 (S and Distances from Respective C Cluster contains 49 cases
	Distance
Австралія	10,4246
Австрія	7,3130
Аргентина	13,1790
Бельгія	4,2593
Болгарія	9,5355
Бразилія	7,9772
Велика Британія	9,0152
Вірменія	15,9570
Греція	6,1132
Грузія	9,0983
Данія	5,7421
Естонія	6,8576
Ізраїль	10,5894
Індонезія	8,8294
Ірландія	5,4850
Іспанія	5,1780
Італія	6,4788
Канада	9,9309
Катар	9,3705
Китай	9,1447
Колумбія	10,1326
Латвія	6,1938
Литва	5,4662
Малайзія	8,9283
Мексика	6,4217
Нідерланди	5,7268
Німеччина	7,4187
Нова Зеландія	7,6919
Норвегія	7,6244
Перу	13,0222
Південна Корея	7,2577
Польща	5,8918
Португалія	6,1809
Російська Федерація	8,7405
Сінгапур	6,6832
Словаччина	6,7028
Словенія	9,1930
Сполучені штати Америки	14,2623
Таїланд	11,8874
Туреччина	8,0420
Угорщина	5,6930
Фінляндія	9,7714
Франція	7,2575
Хорватія	8,9022
Чехія	8,5064
Чилі	7,5541
Швейцарія	7,1835
Швеція	9,5560
Японія	5,8427

Рисунок Б.2 – Склад та характеристика другого кластера країн світу в розрізі станів обраних сфер згідно показника евклідових відстаней

	Members of Cluster I and Distances from F Cluster contains 86 c
	Distance
Алжир	6,02498
Ангола	3,36255
Андорра	11,79029
Антигуа і Барбуда	6,26056
Афганістан	8,28268
Багамські острови	3,89898
Барбадос	8,46509
Беліз	5,62686
Болівія	7,84338
Боснія і Герцеговина	9,27261
Буркіна-Фасо	9,07055
Бурунді	7,18673
Бутан	9,78855
Вануату	5,23220
Венесуела	7,62064
Габон	5,84314
Гайана	5,04819
Гаїті	7,77417
Гамбія	5,19176
Гватемала	4,59071
Гвінея	5,12036
Гвінея-Бісау	7,37279
Гондурас	5,52293
Гренада	7,17477
Демократична Республіка Конго	6,89603
Джибуті	5,92537
Домініка	5,60820
Екваторіальна Гвінея	10,40686
Еритрея	7,57200
Есватіні	3,96971
Ефіопія	9,08083
Зімбабве	8,70531
Ірак	6,88784
Кабо-Верде	5,97510
Камбоджа	7,53125
Камерун	10,43273
Кірібаті	6,79005
Коморські острови	6,28499
Конго (Республіка)	8,39193
Лаос	6,28427
Лесото	6,37802
Ліберія	9,52982
Ліван	9,51171
Лівія	6,49054
Мавританія	5,35919
Мадагаскар	5,77040
Малаві	7,24699
Малі	6,37456
Мальдіви	6,67928
Маршаллові острови	6,89576
Мозамбік	4,80865
Монголія	10,27943
М'янма	12,07148
Намібія	4,86551
Науру	10,22727
Нігер	6,97749
Нікарагуа	11,19983
Папуа-Нова Гвінея	5,44530
Південний Судан	8,24267
Північна Корея	12,21162
Сальвадор	12,14479
Самоа	8,38544
Сан-Марино	10,93541
Сан-Томе і Принсіпі	4,60289
Сейшельські острови	6,34028
Сенегал	7,81887
Сент-Вінсент і Гренадіни	6,58803
Сент-Кітс і Невіс	7,20758
Сент-Люсія	7,06080
Сирія	10,10682
Соломонові острови	6,84422
Сомалі	10,88768
Судан	8,16878
Суринам	8,22447
Східний Тимор	5,35966
Сьерра-Леоне	6,62279
Таджикистан	4,09459
Того	7,49678
Тонга	6,69358
Тринідад і Тобаго	8,27968
Тувалу	9,53205
Туркменістан	5,94811
Фіджі	8,85013
Центральноафриканська Республіка	9,26618
Чад	9,91985
Ямайка	6,07671

Рисунок Б.3 – Склад та характеристика другого кластера країн світу в розрізі станів обраних сфер згідно показника евклідових відстаней

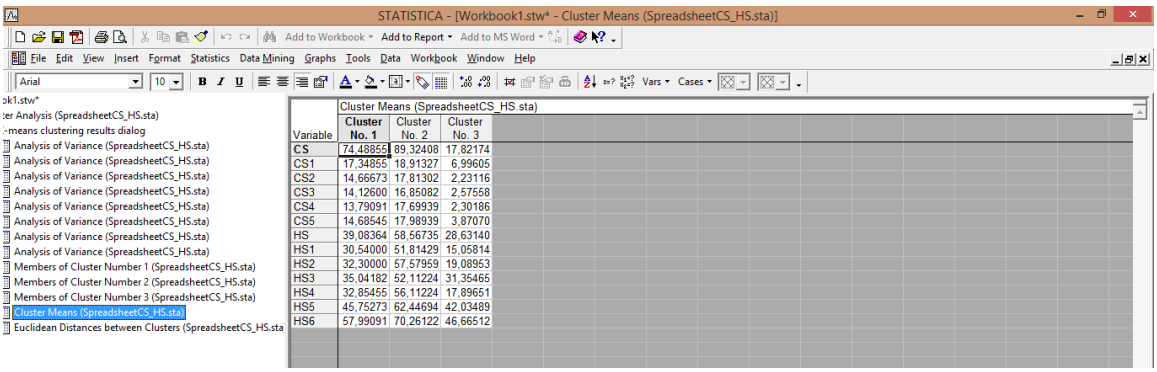


Рисунок Б.4 – Кластерний аналіз методом (середні значення)

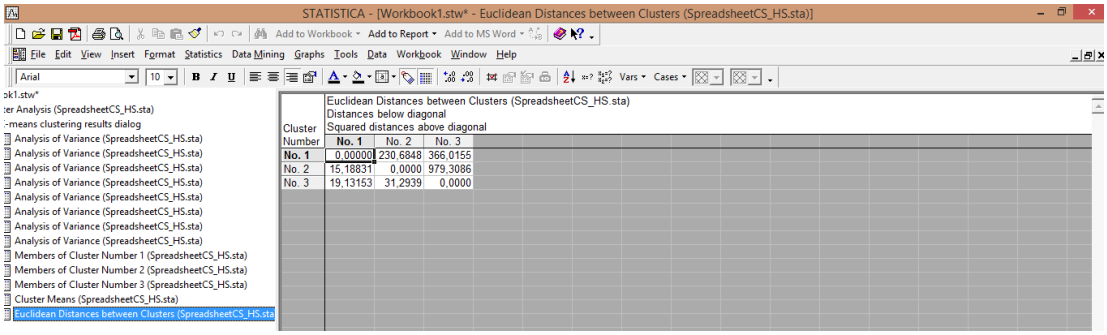


Рисунок Б.5 – Кластерний аналіз – евклідові відстані

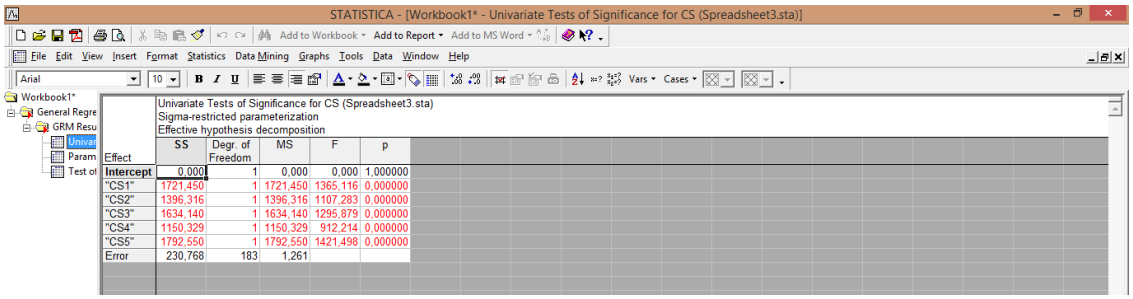


Рисунок Б.6 – Уніваріантні тести на значущість (Univariate Tests of Significance) для змінних

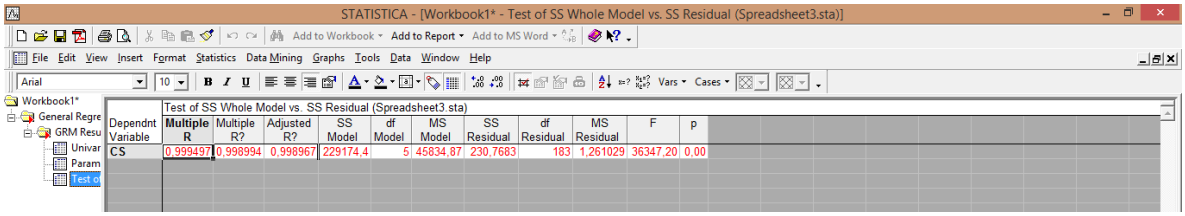


Рисунок Б.7 – Тестування суми квадратів повної моделі (SS Whole Model) проти суми квадратів залишків (SS Residual) для змінних

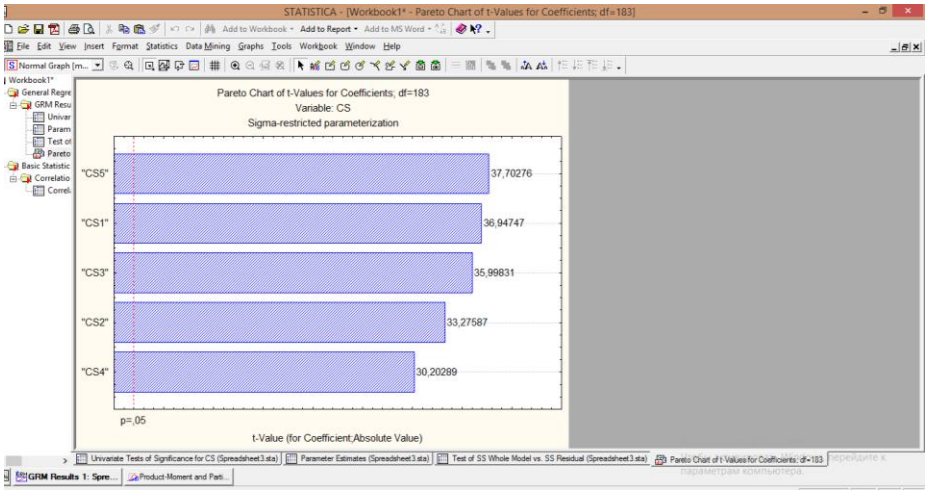


Рисунок Б.8 – Графік значущості впливу факторів, що визначають стан кібербезпеки, побудований за допомогою програмного забезпечення STATISTICA

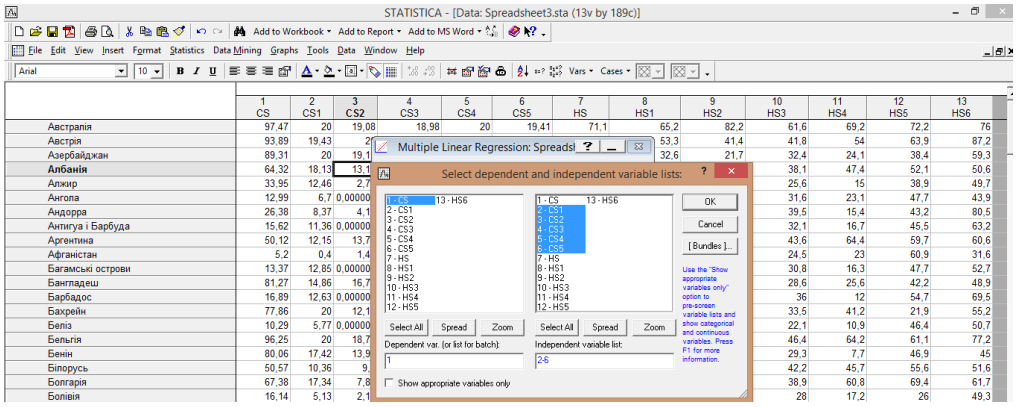


Рисунок Б.9 – Вибір показників першої групи для функції «Multiple Linear Regression» у програмному забезпеченні STATISTICA

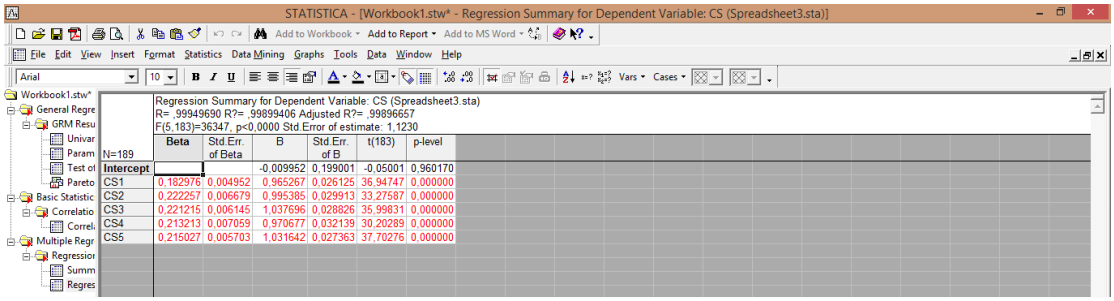


Рисунок Б.10 – Таблиця для представлення результатів регресійного аналізу, виконаного з використанням методу найменших квадратів (OLS)

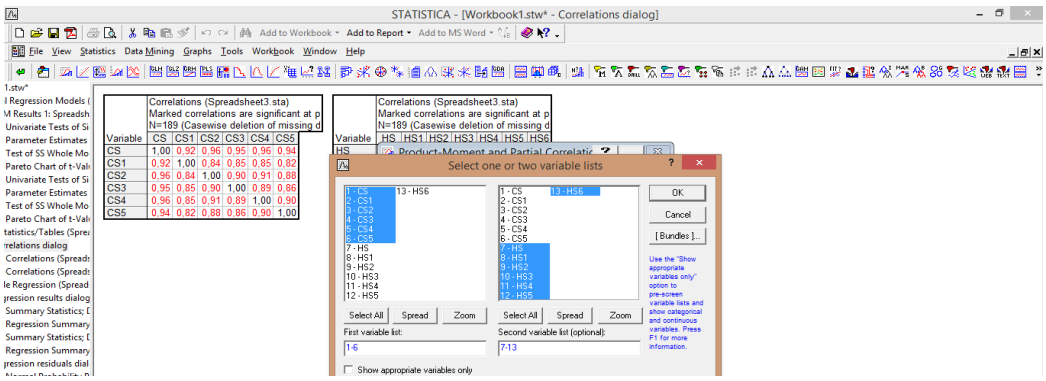


Рисунок Б.11 – Вибір показників груп для функції ««Correlation matrices»» у програмному забезпеченні STATISTICA

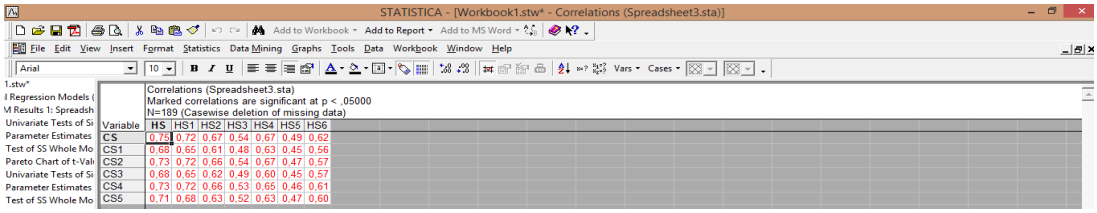


Рисунок Б.12 – Таблиця для представлення кореляційних коефіцієнтів між різними змінними, що включені в аналіз

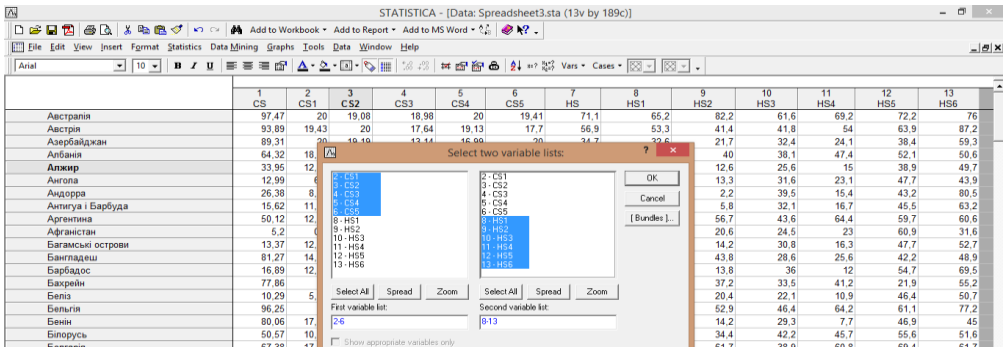


Рисунок Б.13 – Вибір показників груп для функції «Multivariate Exploratory Techniques» – «Canonical Analysis» у програмному забезпеченні STATISTICA

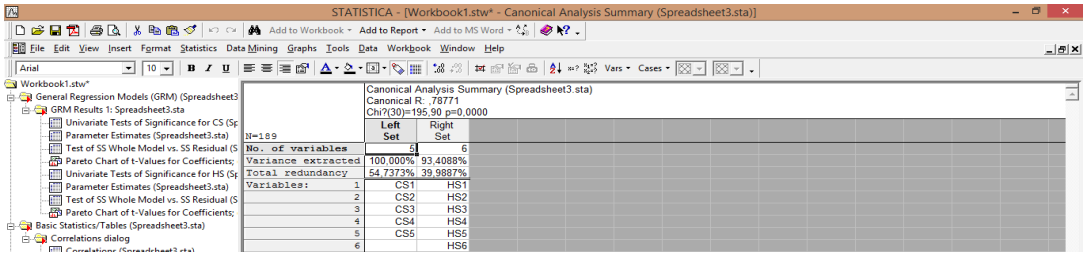


Рисунок Б.14 – Результати канонічного аналізу за допомогою програмного забезпечення STATISTICA