УДК: 37.012.4 : 004.056 : 330.34 JEL Classification: C38, F52, O011

ВПЛИВ РІВНЯ ЕКОНОМІЧНОГО РОЗВИТКУ КРАЇНИ НА ЗАЛЕЖНІСТЬ ВИКОРИСТАННЯ ПЕРСОНАЛЬНИХ ЗАСОБІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА НАСЛІДКІВ КІБЕРЗЛОЧИНІВ

Яровенко Г.М., *к.е.н., доцент, доцент кафедри економічної кібернетики,*
Сумський державний університет, м. Суми, Україна
a.yarovenko@uabs.sumdu.edu.ua

За останнє десятиліття спостерігається зростання обсягів кіберзлочинності у різних сферах життєдіяльності на рівні держави, економічних агентів, окремих індивідів. Тому набувають актуальності питання дослідження процесів формування інформаційної безпеки та виявлення впливів на її ефективність. Метою дослідження є доведення гіпотези про те, що настрої населення, пов'язані із використанням персональних заходів безпеки та формуванням відповідних наслідків інцидентів, відбуваються під впливом рівня економічного розвитку країни. Це здійснювалося за допомогою кластерного аналізу методом k-середніх із використанням аналітичної платформи Deductor Academic на основі даних дослідження, проведеного серед респондентів країн ЄС. Аналіз відповідей показав, що спостерігається тенденція зростання використання онлайн-банкінгу та сервісів електронної комерції; відбувається зростання кількості респондентів, які ставали жертвами кіберзлочинів, особливо соціальної інженерії; знижується тенденція у використанні надійних персональних засобів безпеки. Результати кластерного аналізу, для якого використано дані щодо кількості респондентів-жертв кіберзлочинів та кількості респондентів, які використовують різні засоби персональної безпеки, дозволили сформувати 7 кластерів країн. Аналіз ВВП на душу населення для отриманих кластерів та візуалізація карти країн дозволили підтвердити гіпотезу, але також було визначено, що на залежності використання персональних заходів безпеки та наслідків кіберзлочинів впливають й ментальні особливості країн, сформованих завдяки близькому територіальному розташуванню країн-сусідок, що мають спільні кордони, історичні події, близькі культурні особливості. Отримані результати матимуть практичну значущість для розробки концепції інформаційної безпеки та економічного розвитку держави. Їх можна використати для визначення тих наборів захисту, які відповідають рівню економічного розвитку та доходів населення. Пріоритетними напрямами подальших досліджень є визначення впливів інших факторів на формування інформаційної безпеки країни та формування барицентричної моделі їх вимірів для забезпечення сталого економічного розвитку держави.

Ключові слова: *економічний розвиток, інформаційна безпека, кіберзлочин, кластерний аналіз, персональний захист.*

DOI: 10.21272/1817-9215.2020.1-22

ПОСТАНОВКА ПРОБЛЕМИ

Важливим аспектом організації інформаційної безпеки у країні є ефективне її забезпечення також й на рівні окремого користувача програмних та технічних засобів, що, як наслідок, може впливати на настрої населення у суспільстві. Наприклад, якщо людина стає об'єктом зламування її акаунту у соціальній мережі або її поштової скриньки, то, як правило, це призводить до негативної реакції користувача по відношенню до компаній-власників мережі, провайдерів, тощо. Масовість та систематичність таких дій може викликати зниження кількості користувачів та рівня доходів від розміщення онлайн-реклами, продажу контенту, тощо. Якщо відбувається атака на онлайн-банкінг або застосовується соціальна інженерія, в результаті чого здійснюється витік досить важливої інформації, яка стосується фінансових операцій, рахунків, платіжних карт, то це може призвести до незаконного привласнення коштів з особових рахунків клієнтів. Як наслідок, фінансові установи змушені відшкодовувати втрати своїм клієнтам, або в протилежному випадку вони їх втрачають, що призводить до зменшенню довіри, появи репутаційних ризиків, зростання збитків. Саме тому виникає потреба у дослідженні впливів різних факторів на формування настроїв населення, пов'язаних із застосуванням різних видів заходів персональної інформаційної безпеки, а також із отриманими наслідками в результаті кіберінцидентів. Серед таких факторів – рівень економічного розвитку країни, є найбільш важливим.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проблема, присвячена різним аспектам інформаційної безпеки, є досить актуальною. Вона привертає увагу науковців зі всього світу. Так, аналіз наукових статей в міжнародних журналах, які індексуються у базі даних Scopus, виявив, що однією з перших публікацій, присвячених проблематиці інформаційної безпеки, була стаття 1967 року Дж. Б. Денніса «A position paper on computing and communications» [1]. Автор розглянув напрям розробки положень інформаційної безпеки для розвитку публічних комунікаційних послуг з комутацією повідомлень.

З появою новітніх технологій та із зростанням кібершахрайств збільшилася й кількість публікацій, присвячених теоретичним та практичним питанням інформаційної безпеки на рівні підприємств, банків, держави, окремих індивідів. За даними бази Scopus з 2010 по 2019 роки було опубліковано 15125 наукових праць, присвячених проблематиці інформаційної безпеки [2]. Галузі, в яких здійснювалися дослідження, пов'язані із різними напрямками інформаційної безпеки: комп'ютерні науки (39,8%), інженерія (20,6%), математика (8,1%), соціальні науки (6,5%), прийняття рішення (5,7%), бізнес, менеджмент та бухгалтерський облік (4,5%), фізика та астрономія (3,2%), матеріалознавство (2,1%), енергетика (1,8%), медицина (1,7%), та інш. [2]. Тобто, інформаційна безпека є актуальною передусім для комп'ютерної галузі, оскільки саме ця сфера відповідає за програмну, технічну, методологічну та інформаційну складову захисту інформації, не залежно від сфери діяльності людини.

Аналіз наукових праць за останні 10 років за географічним охопленням показав, що найбільшу увагу до цієї проблеми приділяють вчені Китаю (3684 публікацій), США (1978), Індії (1306), Росії (983), Великобританії (644), Південної Кореї (451), Австралії (445), Тайваню (423), Німеччини (409), тощо [2]. На сьогодні більшість з цих країн є лідерами у розробці потужних програмно-технічних комплексів та систем захисту, тому виправдано, що їх вчені висвітлюють свій практичний досвід у цій сфері. Серед них найвагоміший внесок було зроблено такими закордонними фахівцями, як: Н. Мілославська, А. Ахмад, Р. Фон Солмс, Т. Ахмад, Р. Аміртраджан, М. Варкентін, А. Толстой, С. Фурнелл, Ж.Б.Б. Раяппан, С. Менсфілд-Дейвін, К. Парсонс, А. Маккормак, та інші [2]. Кожним з них було опубліковано 20 і більше публікацій у міжнародних виданнях, які індексуються у базі Scopus, що свідчить про їх значний науковий доробок у дослідження проблематики інформаційної безпеки.

Серед українських вчених можна виділити науковців, які також займаються проблемами інформаційної безпеки. В. Лужецький, А. Кожухівський, О. Войтович приділили увагу теоретичному підґрунтю інформаційної безпеки: основним поняттям, компонентам, заходам та засобам безпеки [3]. На державному рівні проблематику інформаційної безпеки досліджував О. Степко [4]. На рівні суб'єктів господарювання питання інформаційної безпеки розглядали Т. Смачило, М. Кахній [5]. Ю. Дрейс досліджує заходи захисту персональних даних в інформаційних системах [6]. Філоненко С., Мужик І., Німченко Т. розглядали методи мінімізації загроз та розробили систему попередження витоків персональних даних [7].

Не дивлячись на вагомий науковий внесок закордонних та вітчизняних вчених, є ряд питань, які потребують уточнення та дослідження. Сюди слід віднести аспект впливу рівня економічного розвитку країни на залежність використання персональних засобів інформаційної безпеки та наслідків кіберзлочинів.

ПОСТАНОВКА ЗАВДАННЯ

Метою дослідження є доведення гіпотези про те, що поведінка населення, пов'язана із використанням персональних заходів безпеки та формуванням відповідних наслідків інцидентів, формується під впливом рівня економічного розвитку країни.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Проведемо аналіз даних, отриманих в результаті моніторингу громадської думки в країнах – членах Європейського Союзу та країнах кандидатах, що здійснювалося в рамках програми Євробарометр. Для цього було використано дані за 2014 та 2019 роки, представлені на порталі відкритих даних Європейського Союзу [8, 9]. Вибір періоду розрахунків здійснювався виходячи із того, що 2014 рік – це початок проведення дослідження, 2019 рік – останнє проведене опитування на актуальний час.

Спочатку проаналізуємо тенденції використання Інтернет-послуг респондентами, що дозволить сформувати уявлення про їх економічну активність в цифровому середовищі. На рисунку 1 представлена динаміка користувачів онлайн-банкінгу в країнах ЄС за 2014 та 2019 роки.

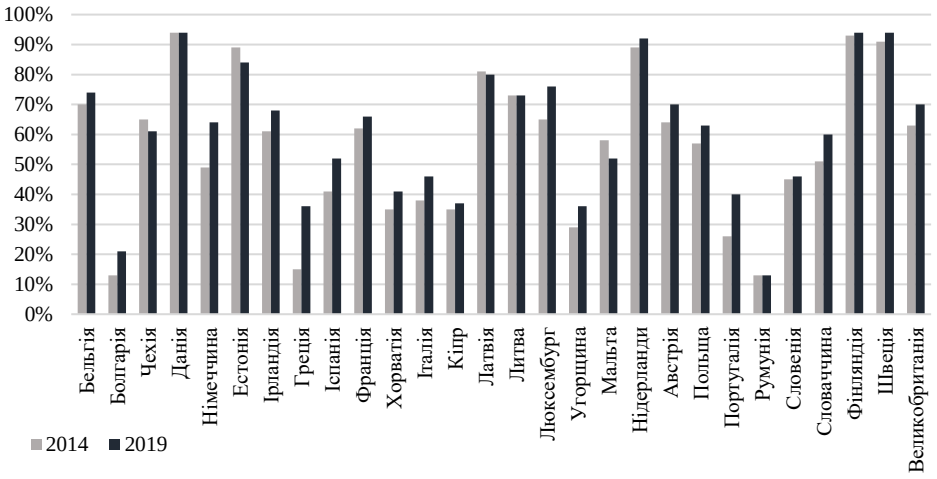

Рисунок 1 – Динаміка користувачів онлайн-банкінгу в країнах ЄС
Джерело: складено автором на основі [8, 9]

Для користувачів більшості європейських країн характерним є зростання операцій із використанням онлайн-банкінгу. Так, це властиво Бельгії (+4%), Болгарії (+8%), Німеччині (+15%), Ірландії (+7%), Греції (+21%), Іспанії (+11%), Франції (+4%), Хорватії (+6%), Італії (+8%), Кіпру (+2%), Люксембургу (+11%), Угорщині (+7%), Нідерландам (+3%), Австрії (+6%), Польщі (+6%), Португалії (+14%), Словенії (+1%), Словаччині (+9%), Фінляндії (+1%), Швеції (+3%), Великобританії (+7%). Рівень використання онлайн-банкінгу за 6 років залишився незмінним або зменшився для користувачів Чехії (-4%), Данії (0%), Естонії (-5%), Латвії (-1%), Литви (0%), Мальти (-6%), Румунії (0%). В цілому спостерігається позитивна тенденція зростання кількості клієнтів комп'ютерних банківських послуг, що в середньому склало близько 5%.

Проаналізуємо інші види комп'ютерних сервісів послуг. Динаміка користувачів, що купують товари та послуги через Інтернет, представлена на рисунку 2. Можна побачити, що перевагу здійсненню операцій купівлі товарів та послуг через засоби Інтернет надають жителі таких країн: Болгарії (+5%), Естонії (+3%), Греції (+6%), Іспанії (+1%), Хорватії (+2%), Італії (+8%), Латвії (+1%), Литви (+5%), Угорщині (+4%), Австрії (+4%), Португалії (+16%), Румунії (+3%), Словенії (+3%), Словаччини (+5%), Фінляндії (+5%), Швеції (+6%). За 6 років кількість операцій купівлі товарів та послуг залишилася незмінною або зменшилася для користувачів Чехії (-4%), Данії (-2%), Німеччині (-1%), Ірландії (-6%), Франції (-10%), Кіпру (-5%), Люксембургу (-5%), Мальти (-18%), Нідерландів (0%), Польщі (-5%), Великобританії (-7%). В середньому для країн ЄС по даному показнику не спостерігаються зміни (0%), що говорить про стабільність настроїв населення в плані здійснення подібних операцій.

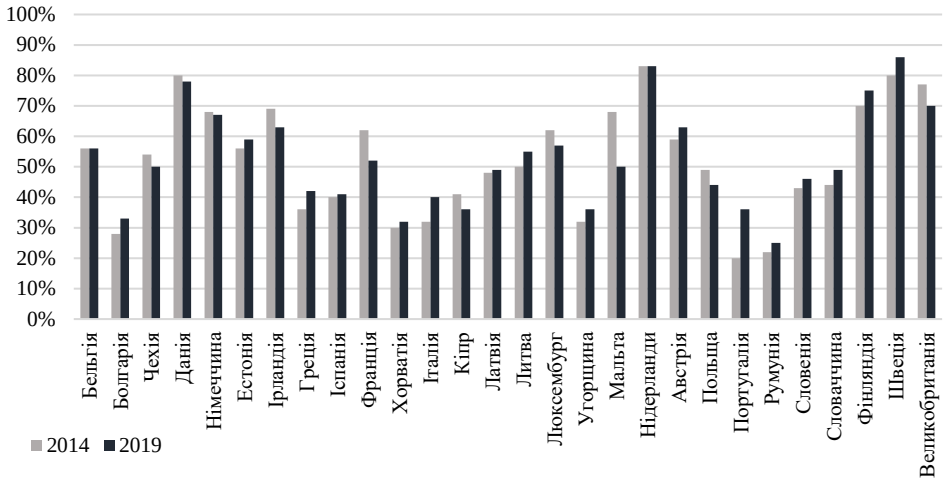

Рисунок 2 – Динаміка користувачів в країнах ЄС, що купують товари та послуги через Інтернет

Джерело: складено автором на основі [8, 9]

Проаналізуємо динаміку користувачів, що продають товари та послуги через Інтернет (рис. 3).

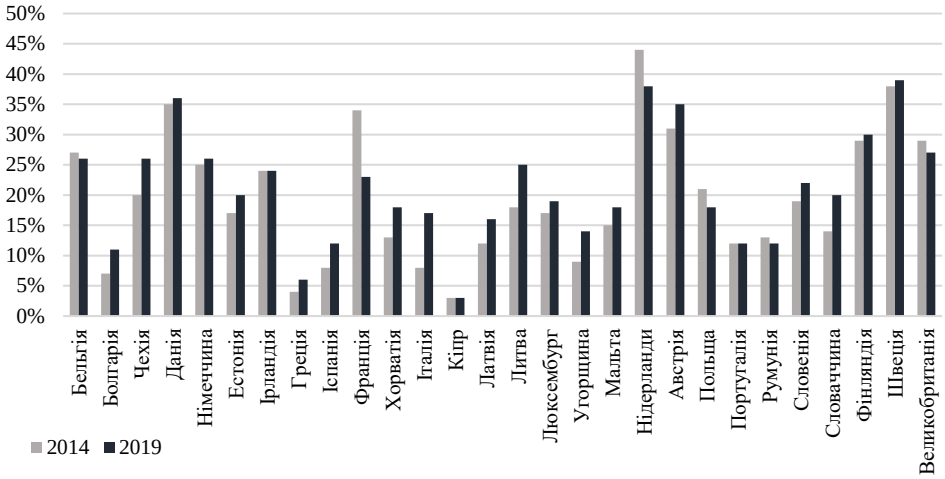

Рисунок 3 – Динаміка користувачів в країнах ЄС, що продають товари та послуги через Інтернет

Джерело: складено автором на основі [8, 9]

Дані рисунку 30 свідчать, що перевагу здійсненню операцій онлайн-продажу товарів та послуг надають жителі таких країн: Болгарії (+4%), Чехії (+6%), Данії (+1%), Німеччині (+1%), Естонії (+3%), Греції (+2%), Іспанії (+4%), Хорватії (+5%), Італії (+9%), Латвії (+4%), Литви (+7%), Люксембургу (+2%), Угорщині (+5%), Мальти (+3%), Австрії (+4%), Словенії (+3%), Словаччини (+6%), Фінляндії (+1%), Швеції (+1%). Кількість операцій продажу товарів та послуг через Інтернет за 6 років залишилася незмінною або зменшилася для користувачів Бельгії (-1%), Ірландії (0%), Франції (-11%), Кіпру (0%), Нідерландів (-6%), Португалії (0%), Румунії (-1%), Польщі (-3%), Великобританії (-2%). В середньому для країн ЄС по даному показнику спостерігається зростання (+2%).

Тобто, не дивлячись на зростання впливу інформаційних загроз на різні види та сфери діяльності людини, спостерігається позитивна тенденція щодо використання населенням комп'ютерних та мобільних технологій, програмних додатків, Інтернету для здійснення операцій фінансово-економічного характеру, що може говорити про зростання довіри до них.

Що стосується заходів безпеки в процесі здійснення онлайн-операцій, найбільш популярними серед респондентів виявилися наступні: використання антивірусних програм, використання тільки власного комп'ютера, не відкриття електронних листів з незнайомих адресів. Динаміка надання ним переваг користувачами з різних країн ЄС представлена на рисунку 4.

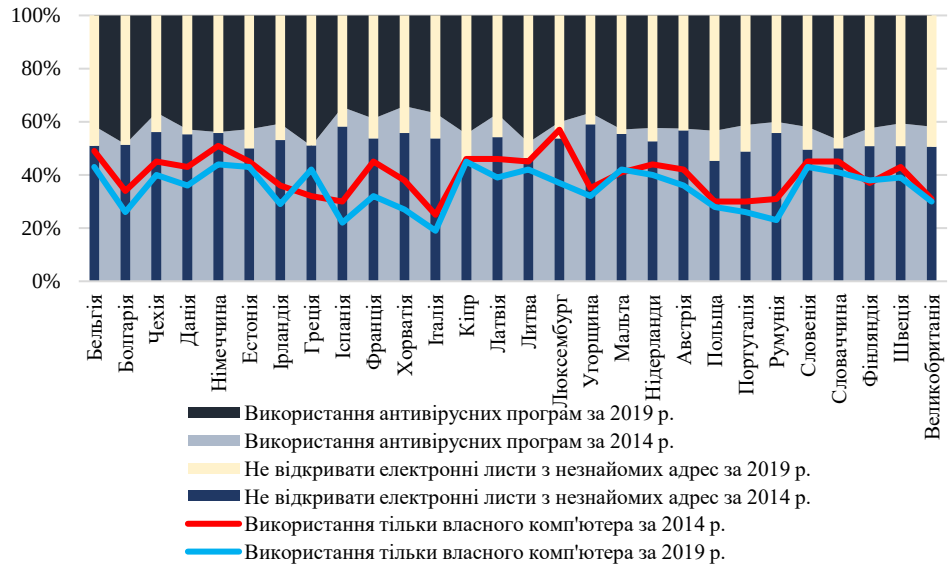

Рисунок 4 – Діаграма трьох найбільш популярних заходів інформаційної безпеки, які використовувало населення країн ЄС у 2014 та 2019 роках
Джерело: складено автором на основі [8, 9]

Так, спостерігається різке зниження використання антивірусних програм у 2019 році у порівнянні із 2014 роком, при чому в середньому це склало -17%. Респонденти з кожної країни знизили рівень їх використання, що у контексті зростання кіберінцидентів, шахрайств та інформаційних витоків, є досить незрозумілим фактом. Можливо це можна пояснити збільшенням вартості такого програмного забезпечення у світлі зростання кіберінцидентів. В середньому на 5% знизилася кількість респондентів, які використовують свій власний комп'ютер та не користуються сторонніми пристроями. Хоча у Греції (+10%), на Мальті (+1%) та у Фінляндії (+1%) цей показник зріс. На 5% зменшилася кількість європейців, які не відкривають підозрілі листи, що говорить або про збільшення довіри до програм, які можуть виявляти та блокувати такі листи, або зменшення обізнаності у питаннях персонального захисту. Хоча респонденти Кіпру (+10%), Литви (+6%), Польщі (+6%), Португалії (+2%), Словенії (+1%), звертають увагу на даний спосіб захисту та не відкривають електронні листи з незнайомих адрес.

Таким чином, за 6 років зменшилася кількість населення, яке активно продовжує захищати свої дані та цифрові пристрої. Тобто можна припустити, що населення намагається вживати певні заходи безпеки, але найбільш дієвим з них надається менша перевага. Це можливо за рахунок впливу рівня доходу населення країни – населення із

вищим доходом можуть дозволити більш дорожчі заходи безпеки, ніж населення країн із нижчим рівнем доходу.

Для виявлення впливів необхідно проаналізувати також й тенденції, які показують рівень зростання чи убування кількості населення, що становилися жертвами кіберзлочинців. В цілому спостерігається зниження кількості жертв інцидентів в середньому на 1% у 2019 році у порівнянні із 2014 роком, що є позитивною тенденцією. Але можна відмітити, що для таких країн, як Угорщина (12%), Австрія (11%), Румунія (11%), Хорватія (10%) та Люксембург (10%), є характерним найбільша кількість жертв даного виду інформаційних загроз. Країнами із найменшим рівнем є: Португалія (1%) та Литва (1%). У випадку, коли респонденти були жертвами соціальної інженерії, ситуація інша, оскільки спостерігається зростання в цілому кількості жертв на 2%. У деяких країнах кількість ошуканого населення досягало 72%, що характерно для Данії. Також високий рівень опитаних, які постраждали від даного виду загроз, з країн: Швеція (60%), Нідерланди (59%), Франція (47%), Німеччина (46%), Ірландія (46%). Найменший рівень постраждалих від соціальної інженерії проявляється серед населення Португалії (5%) та Греції (9%). Якщо аналізувати даний показник у порівнянні із 2014 роком, то практично для усіх країн він зріс, причому у таких країнах, як Фінляндія (+23%), Німеччина (+14%) та Бельгія (+13%), він збільшився досить суттєво. Але спостерігається зменшення кількості ошуканих респондентів Португалії (-15%), Румунії (-8%), Греції (-8%), Мальти (-8%), Литви (-6%), Польщі (-6%), Словаччини (3%), Італії (-2%), Словенії (-2%). Слід відмітити, що ймовірно такий розкид є результатом того, що об'єктами інформаційних загроз є більш економічно активне населення країн із розвинутою економікою. Даний показник склав 38% у 2019 році для населення у віці 25-39 років та 37% для респондентів у віці 40-54 років. Також можна зазначити, що жертвами стали опитувані, що є самозайнятими (41%) або займають керівні позиції (49%). Також 53% з них відносять себе до вище середнього класу та 47% - до вищого класу [9]. Можна зробити припущення, що найбільш привабливими для кіберзлочинців в плані фішингу та соціальної інженерії є фінансово забезпечені особи з найбільш розвинутих країн.

Результати проведеного аналізу надають можливість сформувати гіпотезу про те, що поведінка населення, пов'язана із використанням персональних заходів безпеки та формуванням відповідних наслідків інцидентів, формується під впливом рівня економічного розвитку країни. Для її доведення проведемо кластерний аналіз методом k-середніх, суть якого полягає у розподілі спостережень на певні групи таким чином, щоб кожна з них відповідала певному кластеру з найближчим середнім значенням [10, с. 281]. Тобто при розподілі дані групи формуються з урахуванням їх подібності та мінімізації відстані кожної точки даних у групі із середнім значенням їх центроїда, що називається евклідовою відстанню та визначається за формулою 1 [11]:

$$J = \sum_{j=1}^{k} \sum_{i=1}^{n} \left\| x_i^{(j)} - c_j \right\|^2, \quad (1)$$

де: J – цільова функція центроїда кластера;

c – центроїд кластера;

x – точка даних, з якої починається визначення евклідової відстані;

k – кількість кластерів;

j – скупчення;

n – кількість випадків;

i – випадок.

Алгоритм k-середніх передбачає виконання наступних кроків [12]:

1) випадковим чином ініціалізуються та відбираються k – кластери;

2) ініціалізуються центроїди, для чого відбувається перемішування даних, а потім випадковим чином вибираються k – точки даних для центроїдів;

3) обчислюється евклідова відстань між точками даних та усіма центроїдами за формулою 2, призначається точка найближчому кластеру, обчислюється центроїд всіх точок шляхом визначення середнього значення всіх точок, які належать даному кластеру [13]:

$$c_i = \frac{1}{n}\sum_{j=i}^{n} x_i^{(j)}; \quad (2)$$

4) алгоритм виконується до тих пір, поки центроїди не будуть змінені, тобто присвоєння точок кластерам не буде змінюватися.

У якості вхідних даних оберемо інформацію щодо кількості респондентів-жителів європейських країн, які вживають різні заходи безпеки, та кількості опитаних, що були жертвами інцидентів. Кластеризацію проведемо із використанням аналітичної платформи Deductor Academic [14]. У якості вхідних даних обрано всі заходи персональної безпеки, у якості вихідних – показники, що характеризують постраждалих від інформаційних загроз. В процесі налаштування було враховано:

- розбиття масиву даних на навчальну вибірку (95%) та тестову (5%);
- спосіб розподілу початкових даних – випадково;
- фіксована кількість кластерів, яку було визначено експериментальним шляхом у кількості 7 за найменшою максимальною та середньою похибками кластеризації;
- здійснення кластеризації за максимальною та середньою похибками.

Експеримент відбувався для 2, 3, 4, 5, 6, 7 та 8 кластерів, результати їх середніх значень максимальної та середньої похибок представлені у таблиці 1.

Таблиця 1 – Середні значення похибок

Назва похибки	Кількість кластерів						
	2	3	4	5	6	7	8
Середнє значення максимальної похибки	1,0133	0,9673	0,6011	0,6122	0,6098	0,5454	0,4392
Середнє значення середньої похибки	0,6505	0,6247	0,3944	0,4666	0,4530	0,4123	0,3523

Можна побачити, що із зменшенням кількості кластерів похибки знижуються, але було надано перевагу семикластерній моделі ніж восьмикластерній, тому що остання формує два кластери із одного значення, що вже говорить про зниження якості кластеризації. Також чотирьохкластерна модель має досить непогані значення похибок, але один з її кластерів містить також одне значення, тому вибір зупиняємо на семи кластерах Це підтвердили результати діаграм розсіювання, рівномірний розподіл значень у профілях кластерів, матриця порівнянь.

На рисунку 5 представлений основний візуалізатор кластерної моделі – багатомірна діаграма результатів кластерного аналізу, яка показує кластери країн в залежності від співвідношення персональних заходів безпеки та наслідків інцидентів.

0-й кластер сформували – Чехія, Латвія, Мальта, Словенія та Словаччина; 1-й кластер – Бельгія, Естонія, Франція та Люксембург; 2-й кластер – Греція, Кіпр, Литва; 3-й – Ірландія, Австрія, Великобританія; 4-й – Болгарія, Іспанія, Італія, Польща та Португалія; 5-й – Данія, Німеччина, Нідерланди, Фінляндія, Швеція; 6-й – Хорватія, Угорщина, Румунія.

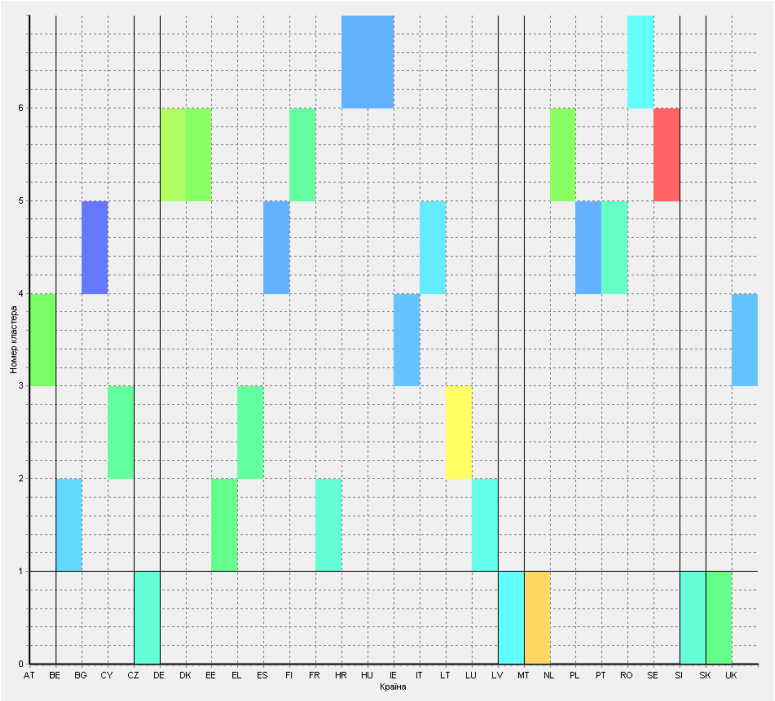

Рисунок 5 – Багатомірна діаграма результатів кластерного аналізу
Джерело: складено автором самостійно

Для кожного кластеру країн зазначимо рівень ВВП на душу населення, узятий за 2019 рік – рік проведення опитування [15], що дозволить підтвердити або спростувати гіпотезу про те, що населення країн, які мають близький рівень економічного розвитку, мають схожі настрої щодо використання засобів інформаційної безпеки, що призводе до схожих відповідних наслідків інформаційних інцидентів.

Використовуючи дані ВВП та результати кластерного аналізу, побудуємо візуалізацію даних (рис. 6). Так, населення країн 6-го кластеру мають приблизно однаковий рівень ВВП на душу населення, який коливається в районі $30140,8 – $34507,1. При цьому можна замітити, що територіально ці країни є близькими сусідами (рис. 6). Для країн 5-го кластеру також є характерним приблизно однаковий рівень економічної активності населення, який перевищує його середнє значення серед аналізованих 28 країн ($47508,47) та знаходиться в діапазоні $51426,0 – $60178,5. На карті 6 чітко видно, що країни даного кластеру знаходяться у територіальній близькості. Країни 4-го кластеру мають досить широкий розкид у значеннях ВВП на душу населення ($24789,6 – $44248,2), хоча можна відмітити, що в середині кластеру Польща та Португалія мають приблизно однаковий рівень економічного розвитку ($34431,2 та $36639,3 відповідно), а також Іспанія та Італія є близькими ($42195,2 та $44248,2). Що стосується географічного розташування, то в межах даного кластеру Іспанія та Португалія є країнами-сусідами (рис. 6).

Населення країн 3-го кластеру також мають різний рівень якості життя населення, але їх значення перевищують середнє для усіх країн, що відносить їх до країн із високим рівнем розвитку. На карті 6 можна побачити, що дві з них мають територіальне сусідство – Великобританія та Ірландія. ВВП на душу населення країн 2-го кластеру знаходиться у межах $30722,2 – $41254,4, але Литва та Кіпр мають дуже близькі значення ($38501,8 та $41254,4 відповідно). Також Греція та Кіпр мають близьке територіальне сусідство (рис. 6).

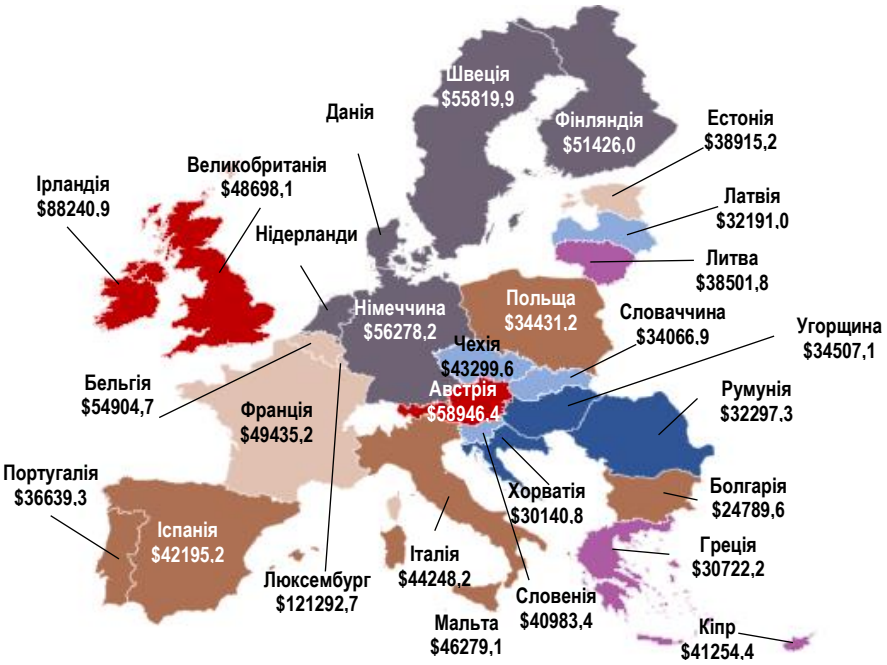

Рисунок 6 – Кластери країн
Джерело: складено автором самостійно

Показник економічного розвитку країн 1-го кластеру має найбільшу розбіжність. Для даної групи характерним є самий високий рівень економічної активності, що відповідає Люксембургу ($121292,7), та самий низький (Естонія – $38915,2). Не дивлячись на таку розбіжність, три країни в середині кластеру є країнами-сусідками із загальними кордонами – Франція, Бельгія та Люксембург (рис. 6). Що стосується 0-го кластеру, то сюди увійшли країни із рівнем ВВП на душу населення нижче середнього рівня, хоча діапазон є досить широкий – $32191,0 – $46279,1. У середині кластеру сформувалося дві групи, які мають близькі значення даного показника – це Латвія, Словаччина та Словенія, Чехія, Мальта. При цьому Словенія, Словаччина та Чехія є країнами-сусідками.

Виходячи з отриманих даних, можна зробити висновок, що настрої населення, пов'язані із використанням персональних заходів безпеки та отриманням відповідних наслідків інформаційних та кіберінцидентів, формуються під впливом рівня економічного розвитку країни та під впливом ментальних особливостей, сформованих завдяки близькому територіальному розташуванню країн-сусідок, що мають спільні кордони, історичні події, близькі культурні особливості (наприклад, Іспанія та Португалія, Великобританія та Ірландія, Греція та Кіпр, Фінляндія, Швеція, Німеччина, Нідерланди та Данія, Франція, Бельгія та Люксембург, Угорщина та Румунія). Тобто для цих країн є спільні риси, які характеризують відношення населення до організації власної інформаційної безпеки та формування самосвідомості та обізнаності щодо можливих наслідків. Сформульована вище гіпотеза є доведеною, але вона повинна також враховувати й вплив ментальних особливостей.

ВИСНОВКИ

Аналіз інформації щодо інцидентів, в результаті яких респонденти ставали жертвами інформаційних та кіберзагроз, дозволив сформувати гіпотезу про те, що населення країн, які мають близький рівень економічного розвитку, мають схожі

настрої щодо використання засобів інформаційної безпеки, що призводить до виникнення схожих наслідків інформаційних інцидентів. Її підтвердження відбувалося за допомогою кластерного аналізу за методом k-means, проведеного на базі аналітичної платформи Deductor Academic. У якості вхідних даних використано дані відповідей щодо заходів персональної безпеки, у якості вихідних – щодо постраждалих від інформаційних загроз. Найбільш ефективною за середнім значенням максимальної та середньої похибок виявилася 7-микластерна модель. Співставлення даних щодо ВВП на душу населення та виділених кластерів дозволили підтвердити та уточнити висунуту гіпотезу, що настрої населення, пов'язані із використанням персональних заходів безпеки та формуванням відповідних наслідків інцидентів, формуються під впливом рівня економічного розвитку країни. Також дана гіпотеза потребує уточнення щодо впливу також й ментальних особливостей країн, сформованих завдяки близькому територіальному розташуванню країн-сусідок, що мають спільні кордони, історичні події, близькі культурні особливості.

В подальших дослідженнях планується екстраполювати отримані результати на український розвиток економіки та заходів інформаційної безпеки, а також тих країн, які мають близький із нею рівень ВВП та територіальне сусідство.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Dennis J.B. A position paper on computing and communications. In *Proceedings of the 1st ACM Symposium on Operating Systems Principles, SOSP*. 1967. P. 6.1-6.10. URL: https://www.scopus.com/record/display.uri?eid=2-s2.0-85060827474&origin=resultslist&zone=contextBox.
2. Analize search results. *Scopus* : website. URL: https://www.scopus.com/term/analyzer.uri?sid=9b8206970e6c1cdd8a0c8783549547da&origin=resultslist&src=s&s=TITLE-ABS-KEY%28%22information+security%22%29&sort=plf-f&sdt=cl&sot=b&sl=37&count=15125&analyzeResults=Analyze+results&cluster=scopubyr%2c%222019%22%2ct%2c%222018%22%2ct%2c%222017%22%2ct%2c%222016%22%2ct%2c%222015%22%2ct%2c%222014%22%2ct%2c%222013%22%2ct%2c%222012%22%2ct%2c%222011%22%2ct%2c%222010%22%2ct&txGid=44b289111640cc0861e0aecc3de12ba6.
3. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки : навчальний посібник. Вінниця : ВНТУ, 2013. 221 с.
4. Степко О.М. Аналіз головних складових інформаційної безпеки держави. *Науковий вісник Інституту міжнародних відносин НАУ. Серія: економіка, право, політологія, туризм*. 2011. №3. С. 90-99.
5. Смачило Т.В., Кахній М.І. Теоретичні засади управління системою інформаційної безпеки підприємства. *Молодий вчений*. 2016. № 12.1(40). С. 969-972.
6. Дрейс Ю.О. Заходи захисту персональних даних в інформаційних (автоматизованих) системах. *Перша всеукраїнська науково-практична конференція* : збірник тез. Одеса: ОНАЗ, 2015. С. 29-32.
7. Філоненко С., Мужик І., Німченко Т. Система попередження витоку персональних даних мережевими каналами. *Безпека інформації*. 2014. Т. 20, № 3. С. 279-285.
8. Special Eurobarometer 404: Cyber security. *EU Open Data Portal* : website. URL: https://data.europa.eu/euodp/en/data/dataset/S1073_79_4_404.
9. Special Eurobarometer 499: Europeans' attitudes towards cyber security. *EU Open Data Portal* : website. URL: https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG.
10. MacQueen J.B. Some methods for classification and analysis of multivariate observations. In *5-th Berkeley Symposium on Mathematical Statistics and Probability*. USA, Berkeley, The University of California, 1967. P. 281-297. URL: http://www.cs.cmu.edu/~bhiksha/courses/mlsp.fall2010/class14/macqueen.pdf.
11. Data Science K-means Clustering – In-depth Tutorial with Example. *DataFlair* : website. URL: https://data-flair.training/blogs/k-means-clustering-tutorial/.
12. Dabbura I. K-means Clustering: Algorithm, Applications, Evaluation Methods, and Drawbacks. *Towards Data Science* : website. URL: https://towardsdatascience.com/k-means-clustering-algorithm-applications-evaluation-methods-and-drawbacks-aa03e644b48a.
13. Fu I., Ravichandran D. K Means Clustering of Sports Images. *Medium* : website. URL: https://medium.com/gumgum-tech/k-means-clustering-of-sports-images-4d2e1d8c4572.
14. Платформа Loginom. *BaseGroup Labs* : веб-сайт. URL: https://basegroup.ru/deductor/download.
15. GDP per capita (current US$). *The World Bank* : website. URL: https://data.worldbank.org/indicator/NY.GDP.PCAP.CD.

REFERENCES

1. Dennis J.B. (1967) A position paper on computing and communications. In *Proceedings of the 1st ACM Symposium on Operating Systems Principles, SOSP*. pp. 6.1-6.10. URL: https://www.scopus.com/record/display.uri?eid=2-s2.0-85060827474&origin=resultslist&zone=contextBox.

2. Analize search results. *Scopus* : website. URL: https://www.scopus.com/term/analyzer.uri?sid=9b8206970e6c1cdd8a0c8783549547da&origin=resultslist&src=s&s=TITLE-ABS-KEY%28%22information+security%22%29&sort=plf-f&sdt=cl&sot=b&sl=37&count=15125&analyzeResults=Analyze+results&cluster=scopubyr%2c%222019%22%2ct%2c%222018%22%2ct%2c%222017%22%2ct%2c%222016%22%2ct%2c%222015%22%2ct%2c%222014%22%2ct%2c%222013%22%2ct%2c%222012%22%2ct%2c%222011%22%2ct%2c%222010%22%2ct&txGid=44b289111640cc0861e0aecc3de12ba6

3. Luzhetskyi V.A., Kozhukhivskyi A.D., Voitovych O.P. (2013) Osnovy informatsiinoi bezpeky : navchalnyi posibnyk [Basics of information security : tutorial]. Vinnytsia.

4. Stepko O.M. (2011) Analiz holovnykh skladovykh informatsiinoi bezpeky derzhavy [Analysis of the main components of information security of the state]. *Naukovyi visnyk Instytutu mizhnarodnykh vidnosyn NAU. Seriia: ekonomika, pravo, politolohiia, turyzm*, no. 3, pp. 90-99.

5. Smachylo T.V., Kakhnii M.I. (2016) Teoretychni zasady upravlinnia systemoiu informatsiinoi bezpeky pidpryiemstva [Theoretical principles of information security system management]. *Molodyi vchenyi*, vol. 12.1(40), pp. 969-972.

6. Dreis Yu.O. (2015) Zakhody zakhystu personalnykh danykh v informatsiinykh (avtomatyzovanykh) systemakh [Measures to protect personal data in information (automated) systems]. Persha vseukrainska naukovo-praktychna konferentsiia : zbirnyk tez. Odesa: ONAZ, pp. 29-32.

7. Filonenko S., Muzhyk I., Nimchenko T. (2014) Systema poperedzhennia vytoku personalnykh danykh merezhevymy kanalamy [System for preventing leakage of personal data through network channels]. *Bezpeka informatsii*, vol. 20, no 3, pp. 279-285.

8. Special Eurobarometer 404: Cyber security. *EU Open Data Portal* : website. URL: https://data.europa.eu/euodp/en/data/dataset/S1073_79_4_404.

9. Special Eurobarometer 499: Europeans' attitudes towards cyber security. *EU Open Data Portal* : website. URL: https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG.

10. MacQueen J.B. (1967) Some methods for classification and analysis of multivariate observations. In *5-th Berkeley Symposium on Mathematical Statistics and Probability*. USA, Berkeley, The University of California, pp. 281-297. URL: http://www.cs.cmu.edu/~bhiksha/courses/mlsp.fall2010/class14/macqueen.pdf.

11. Data Science K-means Clustering – In-depth Tutorial with Example. *DataFlair* : website. URL: https://data-flair.training/blogs/k-means-clustering-tutorial/.

12. Dabbura I. K-means Clustering: Algorithm, Applications, Evaluation Methods, and Drawbacks. *Towards Data Science* : website. URL: https://towardsdatascience.com/k-means-clustering-algorithm-applications-evaluation-methods-and-drawbacks-aa03e644b48a.

13. Fu I., Ravichandran D. K Means Clustering of Sports Images. *Medium* : website. URL: https://medium.com/gumgum-tech/k-means-clustering-of-sports-images-4d2e1d8c4572.

14. Platform Loginom. *BaseGroup Labs* : website. URL: https://basegroup.ru/deductor/download.

15. GDP per capita (current US$). *The World Bank* : website. URL: https://data.worldbank.org/indicator/NY.GDP.PCAP.CD.

SUMMARY

Yarovenko H. **Influence of the country economic development on the dependence of the use of personal information security and the consequences of cybercrime**

Over the past decade, there has been an increase in the volume of cybercrime in various spheres of life at the level of the state, economic agents, and individuals. Therefore, the issues of studying the processes of forming information security and identifying the impact on its effectiveness are becoming topical. The aim of this study is to prove the hypothesis that the behaviour of the population associated with the use of personal security measures and the formation of the corresponding consequences of incidents occurs under the influence of the level of economic development of the country. This was done using k-means cluster analysis via the Deductor Academic analytical platform and based on data from a survey conducted among respondents from EU countries. Analysis of the responses showed that there is a growing trend in the use of online banking and e-commerce services; there is an increase in the number of respondents who have become victims of cybercrimes, especially social engineering; the trend towards the use of reliable personal security equipment is declining. The results of the cluster analysis, for which data on the number of respondents who are victims of cybercrimes and the number of respondents using various personal security tools were used, made it possible to form 7 clusters of countries. Analysis of GDP per capita for the obtained clusters and visualization of the map of countries allowed us to confirm the hypothesis, but it was also determined that the dependence of the use of personal security measures and the consequences of cybercrimes is also influenced by the mental characteristics of countries formed due to the close territorial location of neighboring countries. The results obtained will be of practical importance for the development of the concept of information security and economic development of the state. They can be used to determine which sets of protection are appropriate for the income level of the population. Priority areas for further research are to determine the influence of other factors on the formation of the country's information security and the formation of a barycentric model of their measurements to ensure sustainable economic development of the state.

Keywords*: economic development, information security, cybercrime, cluster analysis, personal protection.*