УДК 351.863:343.37:004.056.5]+004.942:061ЄС JEL Classification C60, C69, C88

# ЗАКОНОМІРНОСТІ ЗДІЙСНЕННЯ КІБЕРАТАК В КРАЇНАХ ЄС НА ОСНОВІ ВИКОРИСТАННЯ АСОЦІАТИВНИХ ПРАВИЛ[1]

**Кузьменко О.В.,**
*доктор економічних наук, професор,*
*Сумський державний університет,*
*e-mail: o.kuzmenko@uabs.sumdu.edu.ua*
*https://orcid.org/0000-0001-8520-2266*
**Доценко Т.В.,**
*доктор філософії, молодший науковий співробітник*
*Навчально-науковий центр бізнес-аналітики*
*Сумський державний університет*
*E-mail: t.dotscenko@uabs.sumdu.edu.ua*
*http://orcid.org/0000-0001-5713-2205*
**Боженко В.В.,**
*кандидат економічних наук, доцент,*
*Сумський державний університет,*
*e-mail: v.bozhenko@uabs.sumdu.edu.ua*
*https://orcid.org/0000-0002-9435-0065*
**Світлична А.О.,**
*студентка,*
*Сумський державний університет,*
*e-mail: aliona.svitlychna@student.sumdu.edu.ua*

*Перехід до інформатизації суспільства, масштабне поширення електронної комерції та неналежний рівень цифрової грамотності призвів до зростання обсягів кібершахрайств, що вимагає удосконалення існуючих та розробка нових методів та способів захисту об'єктів інформаційної інфраструктури. Метою даного дослідження є визначення закономірностей здійснення кібератак у країнах Європейського Союзу шляхом побудови економіко-математичної моделі, в основі якої лежить використання асоціативних правил. Для дослідження було обрано методи: логічне узагальнення – при формуванні вхідної структури даних здійснення кібератак, яка включає перелік показників кібератак, рік здійснення, країни, які постраждали та країни реципієнти кібератак, тип та категорія шахрайств; методика моделювання Data Mining – Association Rules на основі використання асоціативних правил зв'язку між явищами, які є об'єктом спостережень; візуалізація та графічний дизайн – при побудові мережі асоціативних правил причинно-наслідкових зв'язків між досліджуваними явищами здійснення кібератак. У роботі було визначено, що потужною технологією, що дозволяє виявляти взаємозв'язки та закономірності між пов'язаними подіями або елементами, для обробки баз даних великих розмірів, виступає моделювання на основі асоціативних правил. У ході дослідження було виявлено, що в 77.14% випадків шпіонаж здійснюється зловмисниками з Росії, у 88,24% - з Німеччини, у 93,75% - з Китаю. 84,62% шпіонажу спостерігається у галузі приватного сектору, 82,05% - у державному секторі. При цьому частка спостережень, для яких шпіонаж здійснюється з Росії, складає 43,55%. Частка спостережень, для яких шпіонаж здійснюється як з Німеччини, так і з Китаю, становить 24,19% вибірки. Найбільша частка спостережень (51,61%) відповідає здійсненню кібератак у вигляді шпіонажу у державному секторі, а 35,48% спостережень відповідає галузі приватного сектору. У 76 % випадків шпіонаж здійснюється зловмисниками з Росії. Розроблена методика дозволить оперативно, автоматично обробляти суттєвий обсяг вхідної інформації, виявляти можливий найповніший, найінформативніший набір закономірностей, визначити ризик від кібершахрайств на базі даних досліджуваних європейських країн, для прийняття керівною ланкою ефективних рішень щодо управління таким ризиком, його мінімізації, з найменшими ресурсними затратами, передбачення кіберзагроз, протидії кібератакам у країнах ЄС.*

*Ключові слова: кібератаки, кіберзлочини, країни ЄС, моделювання, асоціативні правила.*
DOI: 10.21272/1817-9215.2021.1-11

## ПОСТАНОВКА ПРОБЛЕМИ

Фінансовий сектор здійснює обслуговування економічних відносин широкого кола учасників: державні та приватні установи та організації, їх працівники та клієнти, інші

[1] Роботу виконано в межах науково-дослідної теми «Data-Mining для протидії кібершахрайствам та легалізації кримінальних доходів в умовах цифровізації фінансового сектору економіки України» (номер державної реєстрації 0121U100467) та держбюджетної науково-дослідної роботи № 0121U109559 «Національна безпека через конвергенцію систем фінансового моніторингу та кібербезпеки: інтелектуальне моделювання механізмів регулювання фінансового ринку».

фінансові посередники тощо. Від усіх цих учасників до фінансових установ потрапляє персональна інформація, комерційні дані, фінансова інформація тощо. Але, враховуючи сучасні технологічні можливості, існують особи та/або угрупування, що прагне скористатися такими ресурсами у незаконних цілях, виникає загроза того, що конфіденціальна інформація може бути зламана та потрапити до злочинців шляхом здійснення кіберзлочинів. А з огляду на стрімке використання цифрових продуктів в умовах пандемії, то проблема кіберзлочинності дедалі загострюється і постає однією з головних загроз репутації, безпеці та економіці нації. Тому, для виявлення, знешкодження, мінімізації та попередження кіберризиків, науково-практичним світовим співтовариством вживаються різноманітні заходи для боротьби з можливими кібератаками. А ефективність вжиття механізмів протидії кібершахрайствам напряму залежить, в першу чергу, від виявлення закономірностей здійснення кібератак з досвіду країн світу.

## АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Питання, пов’язані з кібератаками, досліджуються широким колом вчених. Серед них варто виділити наступні надбання: DIDDOS-підхід для виявлення та ідентифікації розподілених кібератак, що пропонують науковці Рехман С. У., Халік М., Імтіаз С. І., Расул А., Шафік М., Джавед А. Р., Башир А. К. [1]; вплив кібератак на репутацію та зриви в діяльності компанії (Камія С., Кан Дж. -., Кім Дж., Мілідоніс А., Штульц Р. М. [2]; фактичні загрози послідовних кібератак введення неправдивих даних у систему інфраструктури розподілу водних ресурсів (Моазені Ф., Хазай Дж. [3]); забезпечення еластичного багатоваріантного контролю мереж доріг під час кібератак (Меркадер П., Хаддад Дж. [4]); специфіку кібератак у транспортній галузі, (Петрілло А., Пескапе А., Сантіні С. [5] Також варто відмітити наступні аспекти при вивчення питань кіберзлочинів: фактори кіберзлочинності, висвітлені фахівцями Пальмієрі М., Шортленд Н., Мак-Гаррі П. [6]; глобальні тенденції блокування вірусів та кіберзлочинності, описані авторами Говендер І., Ватсон Б. В. В., Амра Дж. [7] взаємозв’язок кіберзлочинності з різними когнітивними процесами, досліджувані у роботі Де Кімпе Л., Уолрейв М., Вердегем П., Понне К. [8].

Вивчення фінансово-економічних процесів у сучасному науковому світі нерозривно пов'язано з використанням новітніх методик моделювання досліджуваних питань. Значний внесок при розробці нових моделей протягом останніх років було здійснено такими дослідниками, як: Лєонов С., Жураковська-Сава Дж., Кузьменко О., Койбічук В. [9] - пропонують використання моделі комплексної оцінки ризиків відмивання грошей на базі гравітаційного та інтелектуального аналізу даних; Лєонов С., Яровенко Г., Бойко А., Доценко Т. [10] - описують застосування різних моделей в системі внутрішнього фінансового моніторингу банківських установ; Кузьменко О., Васильєва Т., Войтович С., Чигрин О., Снєшка В. [11] - розкривають ефективність просторового нелінійного моделювання соціальних та економічних закономірностей при дослідженні covid-19. Наряду з ними, особливої уваги наразі заслуговують трактати, що стосуються вивчення такого виду моделювання, як асоціативні правила. Так, Горбань Х., Кандиба І., Дворецький М., Бойко А. [12] розкривають принципи пошуку різноманітних типів асоціативних правил для багатовимірних даних; Савчук Т. О., Приймак Н. В., Слюсаренко Н. Н., Смоларз А., Смайлова С. та Аміргалієв Ю. [13] описують удосконалений метод пошуку асоціативних правил під час розробки програмного забезпечення; Бова В., Щеглов С., Лещанов Д. [14] досліджують модифікований підхід до проблем оптимізації обробки асоціативних правил на основі генетичного пошуку для неструктурованих даних великого обсягу; Малатерр К., Шартьє Ж., Ларо Ф. [15] описують ефективність застосування тематичних асоціативних правил для характеристики семантичної структури документів; Хачай Т., Міазга Дж. [1] пропонують використання алгоритму вибору глибоких нейронних мереж з асоціативними правилами для вирішення проблем практичних рекомендацій хештегів.

## ПОСТАВКА ЗАВДАННЯ

Метою даного дослідження є визначення закономірностей здійснення кібератак у країнах ЄС шляхом побудови економіко-математичної моделі, в основі якої лежить використання асоціативних правил.

## МЕТОДИ ДОСЛІДЖЕННЯ

Для дослідження закономірностей здійснення кібератак було обрано наступний методичний інструментарій:

– логічне узагальнення – при формуванні вхідної структури даних для аналізу кібератак, яка включає основні їх характеристики: рік здійснення, країни, які постраждали та країни реципієнти кібератак, тип та категорія шахрайств;

– методика моделювання Data Mining – Association Rules на основі використання асоціативних правил зв'язку між явищами, які є об'єктом спостережень. Застосування даного методу дозволяє ідентифікувати та формалізувати закономірності між пов'язаними подіями;

– візуалізація та графічний дизайн – при побудові мережі асоціативних правил причинно-наслідкових зв'язків між досліджуваними явищами.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

На сьогоднішній день при виявленні певних закономірностей фахівцями проводиться обробка баз даних великих розмірів, що потребує розробки певних моделей, здатних опрацьовувати суттєві інформаційні ресурси. А одним з найефективніших вирішень цього питання є використання асоціативних правил та їх пристосування до вивчення досліджуваних питань.

Асоціативні правила – це дуже потужна технологія, що дозволяє виявляти взаємозв'язки між пов'язаними подіями або елементами. Вони описуються у вигляді: $X \to Y, X \cap Y \to \emptyset$. При чому, будь-яке асоціативне правило можна представити двома основними характеристиками [13]:

- підтримка (опора) $supp(X \to Y)$ асоціативного правила $X \to Y$ виступає значенням, що дорівнює відношенню кількості записів $X \cup Y$ в базі даних D, до загальної кількості записів у базі даних;

- довіра $conf(X \to Y)$ до асоціативного правила $X \to Y$ виступає значенням, що дорівнює відношенню її опори $supp(X \to Y)$ до опори $supp(X \to Y)$ набору X.

Асоціативні правила, що виникають при аналізі багатовимірних даних класифікуються за наступними видами:

– міжвимірні асоціаціативні правила, тобто правила між атрибутами різних вимірів (формула 1) [12]:

$$(A_I^x \in D_I) \wedge \ldots \wedge (A_J^y \in D_J) \to A_K^z \in D_K, \quad (1)$$

де I, J, K - певні індекси розмірів, що включені в асоціативне правило, причому I, J, K = 1 ...n; де n - кількість розмірів, $D_I - I^{th}$ - є розмірністю, x, y, z - певні атрибути розмірності, при чому x, y, z = 1 ... $m_i$; $m_i$ - кількість атрибутів $I^{th}$-виміру; $A_I^X$ - певний атрибут $I^{th}$-виміру.

– внутрішньовимірної асоціаціативні правила, тобто правила асоціації в межах одного виміру (формула 2) [12]:

$$(A_I^x \in D_I) \wedge \ldots \wedge (A_I^y \in D_I) \to (A_I^z \in D_I) \wedge \ldots \wedge (A_I^v \in D_I), \quad (2)$$

де I = 1 ...n; де n - кількість розмірів, x, y, z, v - певні атрибути розмірності, при чому x, y, z, v = 1 ... $m_i$; $m_i$ - загальна кількість атрибутів $I^{th}$-виміру.

– гібридні асоціативні правила, тобто можливі залежності між вимірами, при чому певні операнди можуть представляти атрибути одного виміру (формула 3) [13]:

$$(A_I^x \in D_I) \wedge \ldots \wedge (A_J^y \in D_J) \rightarrow (A_J^v \in D_J) \wedge \ldots \wedge (A_K^z \in D_K), \quad (3)$$

Формування асоціативних правил використовується для наступного: виявлення та вивчення вразливих місць у досліджуваних процесах, що дозволить у майбутньому на ранніх етапах мінімізувати, чи, навіть, уникнути додаткових матеріальних витрат; надання можливості керівній ланці визначити необхідну оптимальну кількість потрібних ресурсів та їх ефективний розподіл; автоматичної ідентифікації, виправлення, вирішення проблемних аспектів та вдосконалення досліджуваних процесів.

Розглянемо отримані закономірності здійснення кібератак в країнах ЄС на основі використання асоціативних правил у вигляді наступної послідовності етапів:

1 етап. Формування вхідної структури даних здійснення кібератак на основі застосування методу логічного узагальнення. На даному етапі проводиться збір та систематизація даних щодо характеристик кібератак протягом 2005-2020 рр. (табл. 1).

*Таблиця 1 – Фрагмент вхідної структури даних здійснення кібератак*

| Назва | Дата | Країна-жертва | Країна-ініціатор | Вид кіберзлочину | Сфера галузі |
|---|---|---|---|---|---|
| Атака на Міністерство закордонних справ Австрії | 2020 | Австрія | Росія | шпіотаж | публічна |
| Атака на Польський університет військових досліджень | 2020 | Польща | Росія | дефейс | публічна |
| Атака на Польський університет військових досліджень | 2020 | Польща | Росія | дефейс | військова |
| Атака на центрально європейські аерокосмічні та оборонні компанії | 2020 | ЄС | Північна Корея | шпіотаж | приватна |
| Атака на RedDelta | 2018 | Італія | Китай | шпіотаж | публічна |
| … | … | … | … | … | … |
| Атака на Avast | 2019 | Чехія | Китай | шпіотаж | приватна |
| Атака на аналітичні центри США та Європи | 2019 | ЄС | Росія | шпіотаж | приватна |
| Атака на Міністерство закордонних справ Чехії | 2019 | Чехія | Росія | шпіотаж | публічна |

Таким чином, на основі зібраних даних щодо здійснення кібератак можна констатувати наступне. До країн, які постраждали від кібератак відносяться Австрія, Польща, Італія, Німеччина, Литва, Латвія, Чехія, Норвегія, Франція, Бельгія, Люксембург, Нідерланди, Швейцарія, Болгарія, Турція, Данія, Швеція, Данія, Фінляндія, Угорщина, Іспанія. До країн-ініціаторів здійснення кібератак на території Європейського Союзу віднесено Росію, Китай, Північна Корея, В'єтнам, Ліван, Іран, Казахстан, США. Крім цього, виявлено наступні типи кібератак: шпіонаж, пошкодження або знищення інформації, дефейс, саботаж, доксинг, фінансова крадіжка, відмова в обслуговуванні. Дані кібератаки були здійснені на об'єкти різних сфер: публічний та приватний сектор, військовий сектор, громадянське суспільство.

2 етап. Проведення поглибленого аналізу кібератак на території Європейського Союзу на основі використання асоціативних правил. Для реалізації даного етапу використано програмний продукт STATISTICA 10. Отримані результати представимо у вигляді рисунку 1.

На основі даних, отриманих шляхом побудови асоціативних правил, представлених на рисунку 1, можна зробити наступні висновки: в 77,14% випадків шпіонаж здійснюється зловмисниками з Росії, у 88,24% - з Німеччини, у 93,75% - з Китаю. Встановлено, що 84,62% шпіонажу спостерігається у галузі приватного сектору, 82,05% - у публічній сфері. При цьому частка спостережень, для яких шпіонаж здійснюється з Росії, складає 43,55%. Частка спостережень, для яких шпіонаж здійснюється як з Німеччини, так і з Китаю, становить 24,19% вибірки. У 76% випадків шпіонаж здійснюється зловмисниками з Росії в сфері публічної діяльності. Переходячи до аналізу частоти виявлених випадків здійснення кібератак, що є суттєвим доповненням до наведених вище асоціативних правил (рисунок 2).

| | Summary of association rules (cyber-operations (EC).sta)<br>Min: support = 20,0%, confidence = 10,0%<br>Max. size of an itemset = 10 | | | | | |
|---|---|---|---|---|---|---|
| | Body | ==> | Head | Support(%) | Confidence(%) | Lift |
| 1 | Government | ==> | Russia | 40,32258 | 64,10256 | 1,135531 |
| 2 | Russia | ==> | Government | 40,32258 | 71,42857 | 1,135531 |
| 3 | Government | ==> | Russia, Espionage | 30,64516 | 48,71795 | 1,118708 |
| 4 | Espionage | ==> | Russia, Government | 30,64516 | 36,53846 | 0,906154 |
| 5 | Espionage, Government | ==> | Russia | 30,64516 | 59,37500 | 1,051786 |
| 6 | Russia | ==> | Espionage, Government | 30,64516 | 54,28571 | 1,051786 |
| 7 | Russia, Government | ==> | Espionage | 30,64516 | 76,00000 | 0,906154 |
| 8 | Russia, Espionage | ==> | Government | 30,64516 | 70,37037 | 1,118708 |
| 9 | Espionage | ==> | Russia | 43,54839 | 51,92308 | 0,919780 |
| 10 | Russia | ==> | Espionage | 43,54839 | 77,14286 | 0,919780 |
| 11 | Germany | ==> | Espionage | 24,19355 | 88,23529 | 1,052036 |
| 12 | Espionage | ==> | Germany | 24,19355 | 28,84615 | 1,052036 |
| 13 | China | ==> | Espionage | 24,19355 | 93,75000 | 1,117788 |
| 14 | Espionage | ==> | China | 24,19355 | 28,84615 | 1,117788 |
| 15 | Private sector | ==> | Espionage | 35,48387 | 84,61538 | 1,008876 |
| 16 | Espionage | ==> | Private sector | 35,48387 | 42,30769 | 1,008876 |
| 17 | Government | ==> | Espionage | 51,61290 | 82,05128 | 0,978304 |
| 18 | Espionage | ==> | Government | 51,61290 | 61,53846 | 0,978304 |

*Рисунок 1 – Результати аналізу кібератак на території Європейського Союзу за допомогою асоціативних правил*

Аналіз рисунку 2 дозволяє констатувати, що найбільша частка кіберзлочинів (62,90%) відбувається в державних структурах, наступна за частотою галузь – приватний сектор (41,94%). Найменші частки кіберзлочинів відбуваються у військовій та суспільній сферах і становить 14,52%.

| | Frequent itemsets computed (cyber-operations (EC).sta)<br>Min: support = 10,0%, confidence = 10,0%<br>Max. size of an itemset = 10 | | | |
|---|---|---|---|---|
| | Frequent itemsets | Number of items | Frequency | Support(%) |
| 1 | ( Espionage ) | 1,000000 | 52,00000 | 83,87097 |
| 2 | ( Government ) | 1,000000 | 39,00000 | 62,90323 |
| 3 | ( Military ) | 1,000000 | 9,00000 | 14,51613 |
| 4 | ( EU ) | 1,000000 | 7,00000 | 11,29032 |
| 5 | ( Private sector ) | 1,000000 | 26,00000 | 41,93548 |
| 6 | ( Civil society ) | 1,000000 | 9,00000 | 14,51613 |
| 7 | ( Germany ) | 1,000000 | 17,00000 | 27,41935 |
| 8 | ( France ) | 1,000000 | 7,00000 | 11,29032 |
| 9 | ( Espionage, France ) | 2,000000 | 7,00000 | 11,29032 |
| 10 | ( Espionage, Germany ) | 2,000000 | 15,00000 | 24,19355 |
| 11 | ( Espionage, Private sector, Germany ) | 3,000000 | 7,00000 | 11,29032 |
| 12 | ( Espionage, Government, Germany ) | 3,000000 | 8,00000 | 12,90323 |
| 13 | ( Espionage, Civil society ) | 2,000000 | 7,00000 | 11,29032 |
| 14 | ( Espionage, Private sector ) | 2,000000 | 22,00000 | 35,48387 |
| 15 | ( Espionage, Government, Private sector ) | 3,000000 | 6,00000 | 9,67742 |
| 16 | ( Espionage, EU ) | 2,000000 | 7,00000 | 11,29032 |
| 17 | ( Espionage, Military ) | 2,000000 | 7,00000 | 11,29032 |
| 18 | ( Espionage, Government ) | 2,000000 | 32,00000 | 51,61290 |
| 19 | ( Government, Germany ) | 2,000000 | 9,00000 | 14,51613 |
| 20 | ( Government, Civil society ) | 2,000000 | 6,00000 | 9,67742 |
| 21 | ( Government, Private sector ) | 2,000000 | 7,00000 | 11,29032 |
| 22 | ( Government, Military ) | 2,000000 | 7,00000 | 11,29032 |
| 23 | ( Private sector, Germany ) | 2,000000 | 8,00000 | 12,90323 |

*Рисунок 2 – Частота виявлених випадків здійснення кібератак*

3 етап. Графічне представлення причинно-наслідкових зв'язків між кібератаками на основі застосування методів візуалізації та графічного дизайну. У рамках даного етапу побудовано граф виявлених на другому етапі асоціативних правил, представлений на рисунку 3, який дозволяє отримати візуальне представлення

сутності (вісь Head означає причину, вісь Body – наслідок), ступеня підтвердженості виявлених зв'язків (колір відповідного еліпса), а також частки досліджуваної сукупності, для якої відповідне асоціативне правило характерне (величина еліпсу).

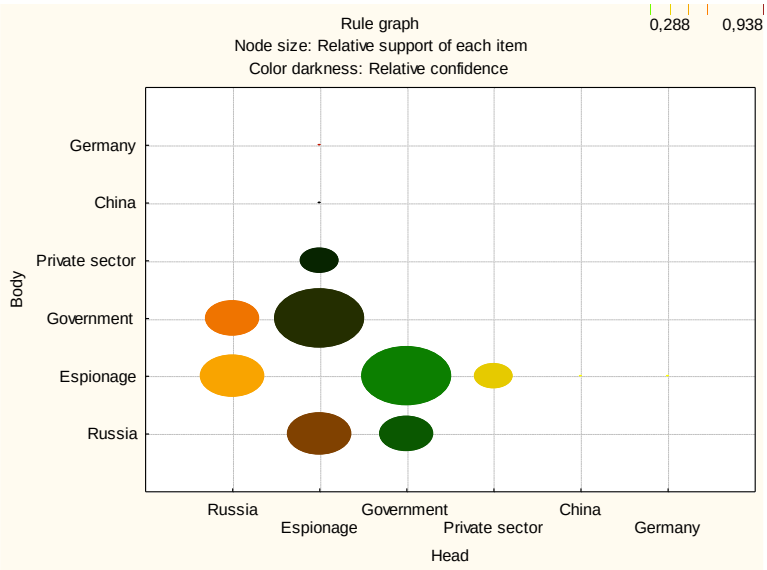


*Рисунок 3 – Граф асоціативних правил*

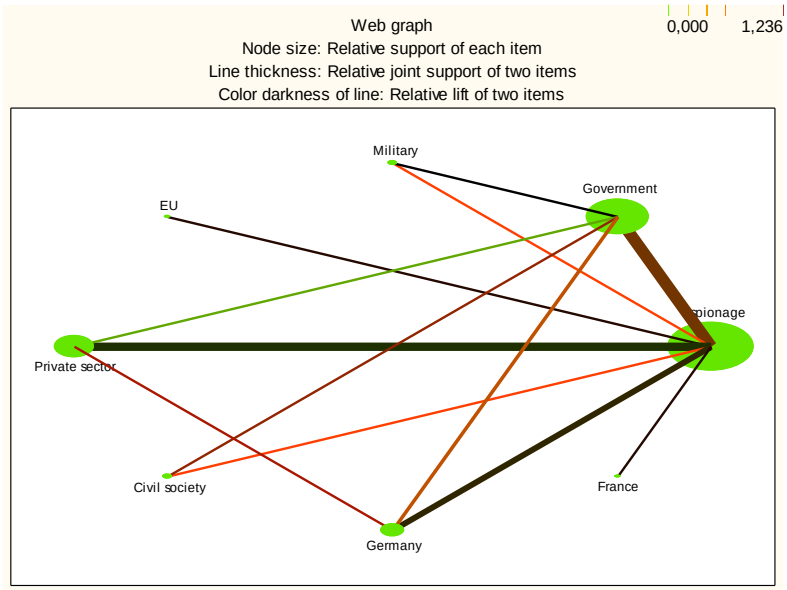


*Рисунок 4 – Веб-граф підтримки виявлених асоціативних правил в розрізі здійснення кібератак в межах країн ЄС*

Переходячи до аналізу рисунку 3 та 4, то найбільшою за частотою виявлених випадків здійснення кібератак (83,87%) є шпіонаж. Серед країн, які стали жертвами кіберзлочинів, необхідно відмітити Німеччину, на частку якої припадає 27,42% випадків, в той час як для Франції даний показник на рівні 11,29% (що відбулось за рахунок шпіонажу). У середньому 11,29% країн ЄС стали постраждали від здійснення кібератак у період з 2005 по 2020 рр.

## ВИСНОВКИ

Зазначимо, що кібератаки, в яких втрачається особиста, комерційна, фінансова інформація, спричиняють вагомі збитки учасників фінансово-економічної системи. А за відсутності новаційних, удосконалених заходів протидії таким кіберзлочинам, масштаби даних протиправних діянь у світі неспинно зростає, і завдає серйозних загроз економічній безпеці країн.

У цій роботі розроблено та описано модель для аналізу закономірностей здійснення кібератак в країнах ЄС на основі використання асоціативних правил. Обрана методологія дозволяє обробляти великі бази даних шляхом формування певних економічних алгоритмів, вирішення яких сприяє пошуку розв'язку поставленого завдання з незначними часовими витратами. Це в подальшому надасть можливість країнам приймати ефективні рішення для передбачення кіберзагроз, протидії кібератакам та забезпечення національної безпеки країн ЄС.

## SUMMARY

***Kuzmenko O., Dotsenko T., Bozhenko V., Svitlychna A.*** **Regularities of cyberatracks in EU countries using association rules**

*The transition to public information, the proliferation of e-commerce and the inadequate level of digital literacy have led to an increase in cyber fraud, which requires the improvement of existing and the development of new methods and ways to protect information infrastructure. The purpose of this study is to determine the patterns of cyberattacks in the European Union by using association rules. Authors have used such methods as: logical generalization – make database of cyberattacks, which includes the year, countries-victims, countries-sponsors, type and category of fraud; Data Mining - Association Rules modeling; visualization and graphic design - when make a network of associative rules of causal relationships between the studied phenomena of cyberattacks. This innovative technology to analyze data allows to identify relationships and patterns between related events or elements. The study found that in 77.14% of cases, espionage is carried out by criminals from Russia, in 88.24% - from Germany, in 93.75% - from China. 84.62% of espionage is observed in the private sector, 82.05% - in the public sector. The share of observations for which espionage is carried out from Russia is 43.55%. The share of observations for which espionage is carried out from both Germany and China is 24.19% of the sample. The largest share of observations (51.61%) corresponds to cyberattacks in the form of espionage in the public sector, and 35.48% of observations correspond to the private sector. In 76% of cases, espionage is carried out by criminals from Russia. The developed technique will allow quickly and automatically process a significant amount of input information, identify the most complete, most informative set of patterns, determine the risk of cyber fraud on the basis of European countries, to make effective decisions to manage such risk, minimize it, with the least resources. anticipation of cyber threats, counteraction to cyber attacks in the EU countries. The obtained results will be of practical value for public authorities and international organizations for the current analysis and adoption of a set of preventive measures to combat cyberthreats.*

*Keywords: cyberattacks, cybercrimes, EU countries, modeling, associative rules.*

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Rehman S.U., Khaliq M., Imtiaz S.I., Rasool A., Shafiq M., Javed A.R., Bashir A.K. DIDDOS: An approach for detection and identification of distributed denial of service (DDoS) cyberattacks using gated recurrent units (GRU). *Future Generation Computer Systems.* 2021. 118. 453-466. URL: doi:10.1016/j.future.2021.01.022.
2. Kamiya S., Kang J., Kim J., Milidonis A., Stulz R.M. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics.* 2021. 139(3). 719-749. URL: doi:10.1016/j.jfineco.2019.05.019.
3. Moazeni F., Khazaei J. Sequential false data injection cyberattacks in water distribution systems targeting storage tanks; a bi-level optimization model. *Sustainable Cities and Society*. 2021. 70. URL: doi:10.1016/j.scs.2021.102895.
4. Mercader P., Haddad J. Resilient multivariable perimeter control of urban road networks under cyberattacks. *Control Engineering Practice*. 2021. 109. URL: doi:10.1016/j.conengprac.2020.104718.
5. Petrillo A., Pescape A., & Santini S. A secure adaptive control for cooperative driving of autonomous connected vehicles in the presence of heterogeneous communication delays and cyberattacks. *IEEE Transactions on Cybernetics.* 2021. 51(3). 1134-1149. URL: doi:10.1109/TCYB.2019.2962601.
6. Palmieri M., Shortland N., McGarry P. Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. *Computers in Human Behaviour.* 2021. 120. URL: doi:10.1016/j.chb.2021.106745.
7. Govender I., Watson B.W.W., Amra J. Global virus lockdown and cybercrime rate trends: A routine activity approach. *Journal of Physics: Conference Series.* 2021. 1828(1). URL: doi:10.1088/1742-6596/1828/1/012107
8. De Kimpe L., Walrave M., Verdegem P., & Ponnet K. What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour and Information Technology.* 2021. URL: doi:10.1080/0144929X.2021.1905066.

9. Lyeonov S., Żurakowska-Sawa J., Kuzmenko O., Koibichuk V. Gravitational and intellectual data analysis to assess the money laundering risk of financial institutions. *Journal of International Studies.* 2020. 13(4). 259-272. URL: doi:10.14254/2071-8330.2020/13-4/18.

10. Leonov S., Yarovenko H., Boiko A., Dotsenko T. Information system for monitoring banking transactions related to money laundering. *CEUR Workshop Proceedings.* 2019. 2422. 297-307.

11. Kuzmenko O., Vasylieva T., Vojtovic S., Chygryn O., Snieška V. Why do regions differ in vulnerability to covid-19? spatial nonlinear modeling of social and economic patterns. *Economics and Sociology*. 2020. *13*(4). 318-340. URL: doi:10.14254/2071-789X.2020/13-4/20.

12. Horban H., Kandyba I., Dvoretskyi M., Boiko A. Principles of searching for a variety of types of associative rules in OLAP-cubes. *CEUR Workshop Proceedings.* 2021. 2845. 181-192.

13. Savchuk T.O., Pryimak N.V., Slyusarenko N.V., Smolarz A., Smailova S., Amirgaliyev Y. Improved method of searching the associative rules while developing the software. *International Journal of Electronics and Telecommunications.* 2020. 66(3). 425-430. URL: doi:10.24425-ijet.2020.131895/715.

14. Bova V., Shcheglov S., & Leshchanov D. Modified approach to problems of associative rules processing based on genetic search. *Proceedings - 2019 International Russian Automation Conference, RusAutoCon 2019*. URL: doi:10.1109/RUSAUTOCON.2019.8867675

15. Malaterre C., Chartier J., Lareau F. The recipes of philosophy of science: Characterizing the semantic structure of corpora by means of topic associative rules. *PLoS ONE, 15. 2020.* URL*:* doi:10.1371/journal.pone.0242353.

16. Hachaj T., Miazga J. Image hashtag recommendations using a voting deep neural network and associative rules mining approach. *Entropy*. 2020. 22(12). 1-13. URL: doi:10.3390/e22121351.

## REFERENCES

1. Rehman, S. U., Khaliq, M., Imtiaz, S. I., Rasool, A., Shafiq, M., Javed, A. R., Bashir, A. K. (2021). DIDDOS: An approach for detection and identification of distributed denial of service (DDoS) cyberattacks using gated recurrent units (GRU). *Future Generation Computer Systems, 118,* 453-466. doi:10.1016/j.future.2021.01.022.

2. Kamiya, S., Kang, J., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics, 139*(3), 719-749. doi:10.1016/j.jfineco.2019.05.019.

3. Moazeni, F., & Khazaei, J. (2021). Sequential false data injection cyberattacks in water distribution systems targeting storage tanks; a bi-level optimization model. *Sustainable Cities and Society, 70* doi:10.1016/j.scs.2021.102895.

4. Mercader P., Haddad J. (2021). Resilient multivariable perimeter control of urban road networks under cyberattacks. *Control Engineering Practice*, 109 doi:10.1016/j.conengprac.2020.104718.

5. Petrillo, A., Pescape, A., & Santini, S. (2021). A secure adaptive control for cooperative driving of autonomous connected vehicles in the presence of heterogeneous communication delays and cyberattacks. *IEEE Transactions on Cybernetics, 51*(3), 1134-1149. doi:10.1109/TCYB.2019.2962601.

6. Palmieri, M., Shortland, N., & McGarry, P. (2021). Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. *Computers in Human Behavior, 120.* doi:10.1016/j.chb.2021.106745.

7. Govender, I., Watson, B. W. W., & Amra, J. (2021). Global virus lockdown and cybercrime rate trends: A routine activity approach. *Journal of Physics: Conference Series, 1828*(1). doi:10.1088/1742-6596/1828/1/012107

8. De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour and Information Technology.* doi:10.1080/0144929X.2021.1905066.

9. Lyeonov, S., Żurakowska-Sawa, J., Kuzmenko, O., & Koibichuk, V. (2020). Gravitational and intellectual data analysis to assess the money laundering risk of financial institutions. *Journal of International Studies, 13*(4), 259-272. doi:10.14254/2071-8330.2020/13-4/18.

10. Leonov, S., Yarovenko, H., Boiko, A., & Dotsenko, T. (2019). Information system for monitoring banking transactions related to money laundering. *CEUR Workshop Proceedings, 2422,* 297-307.

11. Kuzmenko, O., Vasylieva, T., Vojtovič, S., Chygryn, O., & Snieška, V. (2020). Why do regions differ in vulnerability to covid-19? spatial nonlinear modeling of social and economic patterns. *Economics and Sociology, 13*(4), 318-340. doi:10.14254/2071-789X.2020/13-4/20.

12. Horban, H., Kandyba, I., Dvoretskyi, M., & Boiko, A. (2021). Principles of searching for a variety of types of associative rules in OLAP-cubes. *CEUR Workshop Proceedings,* 2845, 181-192.

13. Savchuk, T. O., Pryimak, N. V., Slyusarenko, N. V., Smolarz, A., Smailova, S., & Amirgaliyev, Y. (2020). Improved method of searching the associative rules while developing the software. *International Journal of Electronics and Telecommunications, 66*(3), 425-430. doi:10.24425-ijet.2020.131895/715.

14. Bova, V., Shcheglov, S., & Leshchanov, D. (2019). Modified approach to problems of associative rules processing based on genetic search. *Proceedings - 2019 International Russian Automation Conference, RusAutoCon 2019,* doi:10.1109/RUSAUTOCON.2019.8867675

15. Malaterre, C., Chartier, J., & Lareau, F. (2020). The recipes of philosophy of science: Characterizing the semantic structure of corpora by means of topic associative rules. *PLoS ONE, 15.* doi:10.1371/journal.pone.0242353.

16. Hachaj, T., & Miazga, J. (2020). Image hashtag recommendations using a voting deep neural network and associative rules mining approach. *Entropy, 22*(12), 1-13. doi:10.3390/e22121351.