МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ В УМОВАХ ВІЙНИ ТА ГЛОБАЛЬНИХ ВИКЛИКІВ XXI СТОЛІТТЯ: СИНЕРГІЯ НАУКОВИХ, ОСВІТНІХ ТА ТЕХНОЛОГІЧНИХ РІШЕНЬ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

19 травня 2023 року

У двох томах

Том 1

Видавництво
«Юридика»
2023

УДК 005.332.2(4):316.42(477)"364""20"(062.552)
Є24

Рекомендовано до друку Вченою радою
Національного університету «Одеська юридична академія»
(протокол № 3 від 16.06.2023 р.)

За загальною редакцією **С. В. Ківалова.**

Відповідальний за випуск **М. Р. Аракелян.**
Матеріали видано в авторській редакції.

Є24 **Європейські** орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 19 травня 2023 р.) / за загальною редакцією С. В. Ківалова. – Одеса : Видавництво «Юридика», 2023. – Т. 1. – 790 с.

ISBN 978-617-8263-39-3

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень». У першому томі збірника містяться наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині в умовах повномасштабного військового вторгнення у сферах філософських основ, загальної теорії та історичних досліджень держави і права, актуальних проблем світових соціально-політичних процесів, соціології та психології. Висвітлено питання загроз національній безпеці в їхньому конституційному вимірі, у рамках міжнародного та європейського права, трудового права та права соціального забезпечення, земельного, аграрного та екологічного права, пов'язані з функціонуванням економіки та підприємництва в умовах європейського вибору України. Розглянуто проблеми інформатизації та цифровізації суспільства, захисту інформації та кібербезпеки в умовах військового вторгнення, питання методики викладання іноземних мов, теорії та практики перекладу, проблеми лінгвістики та журналістики.

Збірник розраховано на наукових та науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)"364""20"(062.552)

ISBN 978-617-8263-37-9 (у 2 т.)
ISBN 978-617-8263-39-3 (т. 1)

СЕКЦІЯ 13
КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

СЕКЦІЯ 13

КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

Керівник секції: *завідувач кафедри кібербезпеки, доктор економічних наук, професор С. А. Горбаченко*

Секретар секції: *лаборант кафедри кібербезпеки Є. Р. Кулешова*

ГОРБАЧЕНКО СТАНІСЛАВ АНАТОЛІЙОВИЧ

Національний університет «Одеська юридична академія», завідувач кафедри кібербезпеки, доктор економічних наук, професор

ІНФОРМАЦІЙНО-ГЕОМЕТРИЧНІ ПІДХОДИ В МЕНЕДЖМЕНТІ КІБЕРБЕЗПЕКИ

Сучасні підприємства та організації в переважній більшості мають досить складну ІТ-інфраструктуру. Зокрема, одним з наслідків пандемії COVID-19 стало майже обов'язкове (навіть для представників малого та середнього бізнесу) поєднання локальних і хмарних сервісів, щоб співробітники могли входити в систему з офісу або з дому. Така складність та залежність бізнесу від ІТ складової створює й підґрунтя для нових векторів атак кіберзлочинців і сприяє збільшенню ризику порушення безпеки даних. В результаті лише протягом 2021 року кількість кібератак зросла на 50 %, досягнувши історичного піку в 4 кварталі, коли компанії зазнавали в середньому 900 атак на тиждень [1].

На рівні суб'єктів підприємництва теж прийшло розуміння того факту, що кібербезпека є глобальним бізнес-ризиком. Так, на прохання назвати свої найбільші побоювання, 44 % бізнес-лідерів вказали на інциденти з кібербезпекою, це більше, ніж тих, хто назвав пандемію (22 %) або рецесію (11 %) [2]. Тому менеджмент намагається проводити систематичну оцінку активів з огляду на їхню вразливість у кіберсередовищі та розмір потенційних збитків. Насамперед, оцінюються можливі репутаційні втрати, а також збитки від крадіжки фінансової інформації, персональних даних працівників та клієнтів, блокування роботи серверів тощо.

Відповідно, підприємства та організації (насамперед ті, що відносяться до критичної інфраструктури), які зазнавали невпинних атак, зрозуміли, що можуть захистити свої дані, лише інвестуючи в комплексну систему управління кібербезпекою. Якщо конкретизувати основні завдання підприємств при побудові вказаної системи, ними виступають виявлення потенційних загроз кібербезпеки підприємств

і вразливостей, попередження кіберінцидентів, а також нейтралізація або мінімізація загроз інформаційної безпеки підприємства [3]. Вирішення поставлених завдань передбачає не тільки технологічні рішення, а й наявність певної управлінської складової.

В цьому сенсі менеджмент кібербезпеки – це процес планування, розробки, впровадження та керування заходами, які спрямовані на захист комп'ютерних систем, мереж і даних від наявних та потенційних кіберзагроз.

На рівні операційних завдань мета менеджменту кібербезпеки полягає у забезпеченні конфіденційності, цілісності та доступності (в тому числі й контексті зручності) інформації, що зберігається та обробляється в комп'ютерних системах. Задля цього він має спрямовуватися саме на запобігання ризикам, а не на ліквідацію негативного впливу. А в стратегічному значенні менеджмент кібербезпеки повинен стати фундаментом відповідної організаційної культури, в центрі якої знаходяться питання безпеки.

З функціонального погляду менеджмент кібербезпеки має включати методи моніторингу кіберзагроз, методи підвищення ефективності кіберзахисту всіх аспектів діяльності суб'єкта підприємництва, методи розроблення й оцінки індикаторів кібербезпеки, методи забезпечення управлінського впливу на організацію кіберзахисту, методи управління соціальною складовою системи кібербезпеки тощо.

Перспективним напрямком наукових досліджень в сфері менеджменту кібербезпеки, який поки що не набув належного поширення, доречно виділити інформаційну геометрію [4]. Інформаційна геометрія дозволяє об'єднати нові фундаментальні дослідження, які використовують геометричний і топологічний аналіз, для розробки нових методів в прийняті оптимальних рішень, описуючи складні бази даних і зображень, щоб зробити системи «розумнішими» щодо їх прогностичної природи і більш стійкими до помилкової класифікації.

Поєднання диференціальної геометрії з інформацією Фішера є способом вимірювання та дослідження кількості багатовимірної інформації, яку спостережувана випадкова величина X несе про невідомий параметр θ розподілу, який моделює X. Таким чином дисперсія, або очікуване значення спостережуваної інформації також будуть опрацьовуватися для використання в машинному прийнятті рішень в цілому, зосереджуючись на мультиагентних командах.

Враховуючи можливість досліджувати багатовимірні потоки інформації, також можливе застосування методів інформаційної геометрії з метою оптимізації геометричного простору прийняття рішень, наприклад в оцінки працездатності людини, відповідальної за кібербезпеку в багатозадачних середовищах та потребуючих виконання відповідних заходів в стислий термін [5].

Таким чином, багатокритеріальний геометричний аналіз рішень, адаптування методів процесу аналітичної ієрархії (MAI) можна використовувати для організації управлінських задач та генерації максимально ефективних рішень в сфері менеджменту кібербезпеки. Адже саме вони утворюють геометричний простір рішень, доступний до подальшого аналізу.

Список використаних джерел:

1. Дослідження Check Point: кібератаки зросли на 50 % у порівнянні з минулим роком. URL: https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/
2. Барометр ризиків Allianz. 2022. URL: https:// www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html
3. Краус К. М., Краус Н. М., Штепа О. В. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. URL: https://elibrary.kubg.edu.ua/id/eprint/42325/1/Kraus_Tsyfrova_transformatsiia_kiberbezpeky_2022.pdf
4. Shun-ichi Amari. Information Geometry and Its Applications. Applied Mathematical Sciences, Springer, 2016.
5. Hesham Fouad, Ira S. Moskowitz, Derek Brock, Michael. Scott Integrating Expert Human Decision-Making in Artificial Intelligence Applications, Chapter 13, Human-Machine Shared Contexts, Elsevier, pp. 257–275, June 2020. URL: https://www.sciencedirect.com/science/article/abs/pii/B9780128205433000134?via%3Dihub

Ключові слова: менеджмент, кібербезпека, інформаційна геометрія.
Key words: management, cyber security, information geometry.

ВАСИЛЕНКО МИКОЛА ДМИТРОВИЧ

Національний університет «Одеська юридична академія», професор кафедри кібербезпеки, доктор юридичних наук, професор

СЛАТВІНСЬКА ВАЛЕРІЯ МИКОЛАЇВНА

Національний університет «Одеська юридична академія», асистент кафедри кібербезпеки

ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ КІБЕРРОЗВІДКИ

Забезпечення кіберзахисту та кіберрозвідки є важливими аспектами в сфері кібербезпеки. Кіберзахист включає в себе заходи з захисту комп'ютерних мереж, програмного забезпечення та даних від несанкціонованого доступу, витоку інформації, вірусів та інших загроз.

Зокрема, в контексті кібероперацій, на думку Горінова П. В. та Драпушко Р. Г.: «Кіберпростір є новим каналом. Він призначений для створення і поширення різноманітної інформації, яка стала новим двигуном економічного зростання, новою платформою для соціального управління, новим способом міжнародного співробітництва і цілою новою сферою національного суверенітету» [1, с. 267].

Забезпечення кіберзахисту може бути досягнуте за допомогою різних методів, таких як захист мережі за допомогою брандмауера, використання антивірусного програмного забезпечення, регулярні оновлення програмного забезпечення та оперативної системи, використання складних паролів та двофакторної автентифікації, резервне копіювання даних та ін.