МЕТОДИКА ФОРМУВАННЯ КІБЕРБЕЗПЕКОВОЇ КОМПЕТЕНТНОСТІ СТУДЕНТІВ ПРИРОДНИЧО-МАТЕМАТИЧНОЇ ТА ЦИФРОВОЇ ГАЛУЗЕЙ

METHODS OF FORMING CYBER SECURITY COMPETENCE OF STUDENTS OF NATURAL, MATHEMATICAL AND DIGITAL FIELDS

УДК 378
DOI https://doi.org/10.32782/2663-6085/2024/68.2.8

Садовий М.І.,
докт. пед. наук, професор,
професор кафедри математики
та цифрових технологій
Центральноукраїнського державного
університету імені Володимира
Винниченка

Трифонова О.М.,
докт. пед. наук, професор,
в.о. зав. кафедри математики
та цифрових технологій
Центральноукраїнського державного
університету імені Володимира
Винниченка

Стаття присвячена проблемі методики формування кібербезпекової компетентності студентів природничої, математичної та цифрової галузей. Здійснено аналіз джерельної бази. Розглянуто поняття кібер як поняття, під яким розуміється все, що пов'язане з цифровими технологіями, інформаційною безпекою, мережами й електронними системами. У нашому випадку мова йде про взаємовідношення інформації та кібернетики. Крім цього, поняття «кібер» позначає все, що стосується віртуального або електронного простору: «кіберсередовище» або «кіберпростір». На основі дослідження наукових, методологічних, психолого-педагогічних джерел, практичних здобутків ми сформували систему понять визначеної тематики. До них віднесли кібер- середовище, простір, загрози, атаки, інциденти, захист, безпеки. Сталий розвиток сучасного суспільства передбачає стрімкий розвиток інформаційних технологій та глобалізацію, а відповідно виникає складне завдання забезпечення кібербезпеки на глобальному рівні. Це в свою чергу викликає необхідність своєчасно враховувати глобальні виклики та бачення перспектив із реалізації засад кібербезпеки, насамперед в освітньому процесі широких верств населення. Здійснено аналіз поняття кібернетичні системи розглядаються незалежно від їх об'єктивних джерел абстрактно. До них відносяться автоматизовані регуляторні пристрої, ЕОМ, людський мозок, суспільство та ін. Як будь-яка система вона має множину об'єктів, що зв'язані між собою і сприймають, запам'ятовують та переробляють і обмінюються інформацією. На основі аналізу кіберпонять, праць дослідників розглянуто застосування їх до освітнього процесу. Створена модель методики формування кібербезпекової компетентності, що передбачає виокремлення засад кібербезпеки в освітній та науковій діяльності та схематична модель методики формування кібербезпекової компетентності.

Ключові слова: *кібернетика, кібербепека, кіберзахист, методика навчання, освітній процес, кібербезпекова компетентність.*

The article is devoted to the problem of methods of formation of cybersecurity competence of students of natural, mathematical and digital fields. An analysis of the source database was carried out. The concept of cyber is considered as a concept that includes everything related to digital technologies, information security, networks and electronic systems. In our case, we are talking about the relationship between information and cybernetics. In addition, the term «cyber» can refer to anything related to virtual or electronic space, such as «cyber environment» or «cyberspace». On the basis of the study of scientific, methodological, psychological and pedagogical sources, practical achievements, we formed a system of concepts of a certain topic. These included cyber: environment, space, threats, attacks, incidents, protection, security. The sustainable development of modern society involves the rapid development of information technologies and globalization, and accordingly, the difficult task of ensuring cyber security at the global level arises. This, in turn, calls for a timely analysis and consideration of global challenges and vision of prospects for the implementation of cyber security principles, primarily in the educational process of broad segments of the population. The analysis of the concept of cybernetic systems is considered independently of their objective sources in the abstract. These include automated regulatory devices, computers, the human brain, society, and others. Like any system, it has a set of objects (elements) that are interconnected and perceive, remember and process and exchange information. On the basis of the analysis of the concepts of cyber concepts, the works of researchers considered the possibilities of their application to the educational process. A schematic model of the methodology for the formation of the cyber security competence was created, which provides for the identification of the principles of cyber security in educational and scientific activities, and a schematic model of the methodology for the formation of the cyber security competence.

Key words: *cybernetics, cyber security, cyber protection, teaching method, educational process, cyber security competence.*

Постановка проблеми. Законом України «Про основні засади забезпечення кібербезпеки України» (2017) увагу українського суспільства акцентовано на захист життєво важливої сторони суспільного життя людей, яка полягає у результатах взаємодії великих і різносторонніх потоків інформації у кіберпросторі, кіберсередовищі. Для забезпечення аналізу визначеної проблеми доцільно виділити основні поняття кібергалузі та сутність взаємодії потоків інформації.

У загальному підході поняття «кібер (cyber)» походить від грецького слова «kybernan» в перекладі означає «керувати» або «управляти» – префікс, що показує відношення чогось до кібернетики та пов'язаних із нею явищ. Змістова сутність поняття «кібер» пов'язана з інформаційними потоками, інтернетом, комп'ютерами, інформаційними технологіями, електронним середовищем, цифровізацією та ін. Тобто нині під цим поняттям розуміється все, що пов'язане з цифровими технологіями, інформаційною безпекою, мережами та електронними системами. У нашому випадку мова йде про взаємовідношення інформації та кібернетики. Крім цього, поняття «кібер» може позначати все, що стосується віртуального або електронного простору, такого як «кіберсередовище»

або «кіберпростір». Дана проблема в методиці навчання мало досліджена, що й складає проблему.

Аналіз останніх досліджень і публікацій. У 1834 р. під кібернетикою розуміли науку про загальні (фундаментальні) принципи керування в комплексі складними (множинними) системами різноманітної природи походження: технічними, фізичними, біологічними, соціальними та ін. [2; 17]. А.М. Ампер назвав кібернетику наукою про управління суспільством.

Норберт Вінер опублікував у 1948 р. книгу «Кібернетика, або керування й зв'язок у тварині й людині», де вперше узагальнив закономірності, що ставляться до систем керування різних систем.

Започаткував кібернетику в нашій державі С.О. Лебедєв зі створення другої в світі ЕОМ (1950), роботи якого продовжив В.М. Глушков і створив обчислювальний центр АН України (1957), який переріс в Інститут кібернетики НАНУ (1962), де відділ біокібернетики відкрив академік М.М. Амосов, а лабораторію математичних методів у біології та медицині професор Ю.Г. Антомонов [3; 11]. Таким чином, у 1962 р. було започатковано новий напрямок кібернетики – біокібернетику.

У подальшому теоретичні та практичні проблеми кібернетики, їх розвиток розглядали видатні українські вчені П.І. Андон, В.М. Глушков, В.Ф. Губарев, В.С. Дейнека, Ю.М. Єрмольєв, О.Г. Івахненко, І.М. Коваленко, В.С. Королюк, С.О. Лебедєв, І.І. Ляшко, А.О. Морозов, В.Н. Редько, І.В. Сергієнко, В.І. Скурихін та ін. [3]. У результаті було виокремлено методологічні принципи кібернетики: системний аналіз, функціональний і системний підходи до дослідження складних систем. Як наслідок виникли технічна, медична, біологічна, економічна кібернетики та ін. галузі.

Прикладні питання кібернетики вивчали М.М. Амосов, А.В. Анісімов, І.Д. Войтович, М.З. Згуровський, Ю.Г. Кривонос, О.А. Летичевський, О.В. Палагін, О.І. Провотар, В.В. Скопецький, К.Л. Ющенко та ін. [3].

Методику навчання кібернетики розробляли Е.О. Балашов, П.П. Мулеса, В.В. Лаговський, М.М. Семков та ін. [5; 8; 9; 16]. До основних методів кібернетики вони віднесли метод математичного моделювання систем і процесів керування; метод оптимізації систем керування.

Таким чином, вказані вчені та практики заклали основи науки кібернетики, створили відповідні підручники та посібники, проте залишилася не завершена проблема методики навчання кібернетики, а відповідно й методики навчання кібергалузей, що нагальним завданням підготовки фахівців природничо-математичної та цифрової галузей.

У Центральноукраїнському державному університеті ім.В. Винниченка (ЦДУ) перший персональний комп'ютер був поставлений у 307 ауд. викладачем Б.А. Трейгером. Перший комп'ютерний клас «Ямаха» було надано Міністерством освіти і науки України. Його змонтували влітку 1986 р. у семиповерховому приміщенні (608 ауд.) завідувач лабораторії спеціального фізичного практикуму П.В. Сірик і завідувач лабораторії радіотехніки А.І. Ковальчук, доцент І.П. Ганжела. Вони й запустили в дію комп'ютерний клас. Це був початок комп'ютеризації спеціальностей фізико-математичного факультету (декан М.І. Садовий).

Мета дослідження полягає в узагальненні понять науки кібернетики, кібергалузей і на цій основі створення засад методики навчання кібер у поєднанні з інформаційними потоками та цифровими технологіями.

Завданням дослідження є визначити основні поняття галузей пов'язаних із кібер і створити на цій основі їх систему; визначити засади методики навчання кібергалузей та шляхи розвитку методики навчання конкретних галузей кібер.

Виклад основного матеріалу. На основі дослідження наукових, методологічних, психолого-педагогічних джерел, практичних здобутків ми сформували систему понять визначеної тематики. До них віднесли кібер- середовище, простір, загрози, атаки, інциденти, захист, безпеки тощо.

Об'єкти *кіберзахисту* (КЗ) – комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; об'єкти критичної інформаційної інфраструктури; комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу [7].

На державному рівні до *кіберпростору* в основному відносять інформаційний простір, енергетику, науково-дослідні установи, інфраструктуру, логістику, військові об'єкти, центри прийняття рішень, бази даних органів влади, державні реєстри та медіа, електронні комунікації, ІТ-галузі. КЗ в інформаційному просторі є захистом національних інтересів та економічної стійкості [4].

Цифрове комунікаційне середовище функціонує за/у мережі комп'ютерних систем і включає користувачів, мережі, пристрої, все програмне забезпечення, цифрові процеси, інформацію в режимі зберігання або транзиту, програми, служби та системи, які можуть бути безпосередньо або опосередковано підключені до мереж [1; 6].

КЗ є процесом і розглядається: як цифрова безпека, практика захисту цифрової інформації, пристроїв і активів (особистих відомостей, облікових

записів, файлів, фотографій, грошей та ін.) [1; 6].

КЗ інформаційних ресурсів, які складаються з окремих документів і масивів документів у бібліотеках, архівах, фондах, банках даних та інших інформаційних системах, що необхідні для забезпечення інформаційних потреб споживачів у визначеній сфері діяльності [10; 18].

Поняття критичної інфраструктуру розуміється як система, яка має важливе значення для підтримки життєво важливих соціальних функцій суспільства, вони підлягають під КЗ [2; 10].

Кібератаки – несанкціонований доступ до ресурсів електромагнітного та іншого випромінювання вплив на електронні інформаційні ресурси й комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби й обладнання з метою порушення штатного режиму роботи, перехоплення, блокування, спотворення, конфеденційності, знищення, порушення цілісності інформації власника. Актуальним є наростання в світі інтенсивності інформаційно-психологічних операцій та ін.

Кіберзагрози розглядаються як потенційно можливі кібератаки зі своєю специфікою. Це хакерські атаки, віруси, фішинг та ін. подібні дії, що несуть потенційні загрози до втрати конфіденційної інформації, руйнації економічних систем, загроз для фізичної безпеки громадян тощо.

Гібридні загрози – це вибухова суміш, в якої немає зрозумілої формули, це поєднання інформації, її сприйняття, інтерпретації та впливу на ухвалення рішення, скоординовані та синхронізовані дії, які можуть проявлятися різними способами та у багатьох секторах [9].

Кіберінцедент відрізняється від кібератаки, насамперед ненавмисністю впливів через природні катаклізми, аварії, помилки операторів та ін. Зокрема, мали місце помилки оператора в Київстар, які мали певний вплив на інформаційний зв'язок.

Сталий розвиток [14] сучасного суспільства передбачає стрімкий розвиток інформаційних технологій та глобалізацію, а відповідно виникає складне завдання забезпечення кібербезпеки (КБ) на глобальному рівні. Це в свою чергу викликає необхідність своєчасно аналізувати та враховувати глобальні виклики та бачення перспектив з реалізації засад КБ, насамперед в освітньому процесі широких верств населення.

Поняття «кібер» походить від поняття кібернетики. Системи, які піддаються управлінню у принципі, є об'єктами вивчення кібернетики.

Кібернетика запроваджує такі поняття, як кібернетичний підхід, кібернетична система.

Кібернетичні системи розглядаються незалежно від їх об'єктивних джерел абстрактно. До них відносять автоматизовані регуляторні пристрої, ЕОМ, людський мозок, суспільство та ін. Як будь-яка система вона має множину об'єктів (елементів), що зв'язані між собою і сприймають, запам'ятовують, переробляють і обмінюють інформацію.

У цілому кібернетика розглядає фундаментальні принципи формування й аналізу систем управління та автоматизації розумової праці. ЕОМ є її технічними засобами, а розвиток кібернетики пов'язаний з еволюцією електронної обчислювальної техніки. Інструментами синтезу рішень є математичний аналіз, лінійна алгебра, геометрії опуклих множин, теорія ймовірностей й математичної статистики, програмування, економетрика, інформатика та інші [18].

Особливо велика роль кібернетики в інженерній психології та психології професійно-технічного освіти.

Таким чином, кібернетика є наукою про управління складними динамічними системами. Вона вивчає загальні принципи управління та зв'язку, системи від самонавідних ракет-снарядів і швидкодіючих обчислювальних машин до складного живого організму. Управління забезпечує переведення керованої системи з одного стану в інше за допомогою цільово-спрямованого впливу керуючого [5; 6].

На основі аналізу понять кіберпонять, праць дослідників [6; 15] ми розглянули можливості застосування їх до освітнього процесу, що передбачає виокремлення засад КБ в освітній і науковій діяльності:

– в комп'ютерній діяльності ліцензійне програмне забезпечення є запорукою безпеки за умови систематичного оновлення;

– запровадження системи постійної звірки різними перевіреними на практиці антивірусними програмами цифрового наповнення, що дає надійність збереження інформації без спотворень та вірусів;

– створення надійного алгоритму обмеження доступу до життєважливих персональних даних: кодів, логінів, паролів, об'єктивних даних особистостей та ін.;

– запровадження науково обґрунтованих закодованих правил двофакторної аутентифікації створення паролів, які передбачають складне поєднання цифр, літер, символів, своєрідних знаків тощо і дасть змогу захиститися від інформаційних вірусів, маніпуляцій та дезінформації;

– уміння працювати з спливаючими вікнами, вкладками, посиланнями та формування навичок їх блокування і жорсткого обмеження доступу користувачів до комп'ютерної мережі неперевірених носіїв інформації;

– створити технологію підвищення імунітету до інформаційних загроз визначення критичного для користувача накопичення інформації і на цій

основі здійснення ревізії і резервного копіювання важливої інформації.

Визначені засади слугують підставою для окреслення шляхів створення методики навчання кібергалузей та недопущення кіберзагроз.

Методика формування КБ компетентності в кібергалузях і недопущення кіберзагроз передбачає володіння студентами предметними компетентностями та знаннями про КЗ [17]. Це нагальна потреба часу для кожної особистості, бо цього вимагає діджиталізоване суспільство. Закон України «Про основні засади забезпечення кібербезпеки України» зобов'язує громадян захищати життєві інтереси свої та суспільства, держави в ході використання кіберпростору. Це стосується вимог сталого розвитку до інформаційного суспільства та цифрового комунікативного середовища. Фахівці цифрових технологій забезпечені компетентностями своєчасного виявлення й нейтралізація потенційних кіберзагроз у кіберпросторі.

Методика формування КБ компетентності студентів включає в себе широкий спектр підходів та інструментів для навчання студентів з питань безпеки в інтернеті та захисту інформації (рис. 1).

До показників визначеної методики відносяться метод кейс-орієнтованого оцінювання цифровими компонентами КЗ, логістики програмування, аналіз критеріїв оцінювання, аналіз гібридного інструментарію. Критерії вимог до якості КБ розглядається через узагальнення традиційних вимог та їх декомпозиції. Рівні вразливості інформаційної КБ цифрових компонентів – через оцінку критичності наслідків втручання [16].

Компоненти КБ компетентності включають вміння протидіяти гібридним загрозам у неочікуваних, непрогнозованих ситуаціях.

Інноваційна методика «гібридного навчання» КЗ включає штучний інтелект, змагальні моделі навчання; моделювання інтелектуальної технології гібридних загроз [9].

Аналіз приведеної моделі приводить до висновку, що методика формування КБ компетентності через навчання, освіту, загальну обізнаність студентів відіграє методологічну основу ключової протидії гібридним загрозам. Така методологія забезпечує формування навичок прийняття студентами рішень, насамперед у розпізнаванні гібридних загроз, визначення їх мети, прогнозування наслідків власних дій при гібридних впливах і захисту свого робочого та соціального простору.

Принципи, методи та засади навчання КБ включають основні концепції КБ (конфіденційність, цілісність, доступність, ідентифікація, аутентифікація та ін.), розгляд різних видів загроз та атак (віруси, черв'яки, фішинг, DoS-атаки, SQL-ін'єкції та інші).

До форм і засобів набуття практичних навичок віднесено виконання вправ і лабораторних робіт із вирішення реальних задач у частині захисту інформації та виявлення загроз, використання спеціалізованих платформ та інструментів для симуляції атак і реакції на них.

Складовою приведеної моделі є кейс-аналіз гібридного інструментарію КЗ, результати якого приводять до висновків з конкретних КБ інцидентів та вивчення їхніх причин, наслідків і заходів, які можна було б вжити для їх попередження або подолання. Система законодавства приводить до формування етичних аспектів КБ та вивчення правових аспектів, пов'язаних із захистом інформації та боротьбою з кіберзлочинністю.

Взаємодія у сфері КЗ спрямована на розвиток навичок комунікації та співпраці, оскільки важливо вміти ефективно співпрацювати в команді для виявлення, аналізу та вирішення проблем безпеки.

Актуальність та постійне навчання націлюють на систематичне оновлення навчальних планів і матеріалів для відображення змін у сфері КБ, залучення студентів до самоосвіти та підтримка їх зацікавленості у вивченні нових технологій та методів оборони.

У сукупності визначені елементи складають основні компоненти методика формування КБ компетентності студентів, яка передбачає розвиток як технічної сторони проблеми, так і усвідомлення

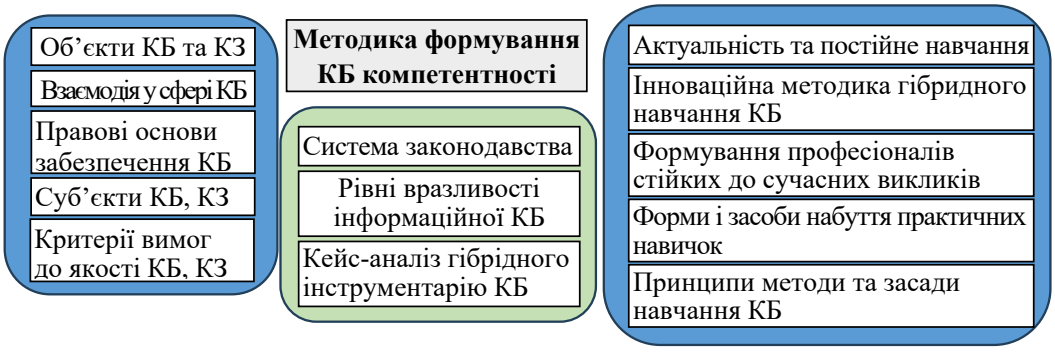

Рис. 1. Схематична модель методики формування КБ компетентності

важливості етики та стратегічного мислення у сфері КБ.

На базі ЦДУ [17] сформована ініціативна група студентів на чолі зі студентом спеціальності «Професійна освіта (Цифрові технології)» Денисом Павлюком, представники якої є волонтерами кіберполіції.

Висновки. Таким чином, у статті окреслені фундаментальні поняття й виклики глобальної КБ та кіберзагрози, визначена модель методики формування КБ компетентності студентів від кібератак на корпоративні системи до державно-санкційованих кіберспроб, загрози в Інтернеті, які прискорено стають все більш виразними та складними. Здійснений аналіз понять вказав на необхідність розроблення та прийняття загальних стандартів КБ, які мають засвоїти студенти в ході навчання. Зроблено висновок про підвищений інтерес студентів до захисту особистих даних і вимоги до їхнього зберігання й обробки на рівні, який відповідає сучасним стандартам конфіденційності.

Перспективи подальшого дослідження полягають у формуванні умов інноваційної КБ на рівні штучного інтелекту й машинного навчання, що передбачає виявлення та запобігання кібератак на ранній стадії.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Бурячок В.Л., Киричок Р.В., Складанний П.М. Основи інформаційної та кібернетичної безпеки: навч. посібн. К., 2018. 320 с. URL: http://surl.li/qjest

2. Гора І.В., Батюк О.В. Окремі питання захисту об'єктів критичної інфраструктури: зарубіжний досвід. *Соціально-правові студії*. 2021. Вип. 1 (11). С. 132–139.

3. Енциклопедія кібернетики: 2 т. / за ред. В.М. Глушкова. Київ: Гол. ред. Укр. рад. енциклопедії, 1973. 570 с.

4. Захист інформаційного та кіберпростору. URL: http://surl.li/qicnb

5. Ілляшенко О.О. Методи і засоби забезпечення виконання вимог до кібербезпеки систем на програмовній логіці: автореф. дис. … к.техн.н.: спец. 05.13.05. Нац. техн. ун-т «Харків. політехн. ін-т». Харків, 2018. 24 с.

6. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; ДНУ «Інститут інформації, безпеки і права НАПрН України»; НБУ ім. В.І. Вернадського. К., 2023. № 6 (червень). 153 с. URL: https://ippi.org.ua/sites/default/files/2023-6.pdf

7. Кібербезпека: запобігання, виявлення, обмеження, відновлення; Ужгор. нац. ун-т. URL: http://surl.li/ngnvm

8. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. К.: Кондор, 2019. 272 с.

9. Методика навчання в умовах гібридних загроз: посібник / Е. Балашов, М. Білоконь, Т. Борозенцева, М. Головянко, С. Гришко, Т. Жовтенко та ін. Харків: ТОВ «Технологічний центр груп», 2023. 84 с.

10. Порядок проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. Постанова Каб. Мін. України від 11.11.2020 № 1176.

11. Ріжняк Р.Я. Розвиток інформатики та інформаційних технологій у вищих навчальних закладах України у другій половині XX – на початку XXI століття: монографія. Кіровоград: Код, 2014. 436 с.

12. Садовий М.І. Особливості організації ергономічно-цифрового освітнього середовища. *Сучасна наука та освіта: стан, проблеми, перспек-тиви*: зб. Міжнар. наук.-практ. конф., 20-21.03.2023, Полтава. С. 175–178.

13. Садовий М.І., Трифонова О.М. Методика вивчення нормативних та методологічних джерел з формування концепції становлення фахівця. *Вісник Глухівського нац. пед. ун-ту ім. О. Довженка. Педагогічні науки.* Глухів, 2023. Вип. 51. С. 226–232. DOI: 10.31376/2410-0897-2023-1-51-226-232

14. Садовий М.І., Трифонова О.М. Розвиток технологічної та природничої освіти в умовах сталого розвитку. *Наукові записки НПУ ім.М.П. Драгоманова (пед.науки)*. 2016. Вип. CXXXII(132). С. 197–207.

15. Сініцин І.П., Ігнатенко П.П., Слабоспицька О.О., Артеменко О.В. Комплексний підхід до побудови системи кіберзахисту критичної інформаційної інфраструктури держави. *Захист інформації (Проблеми програмування)*. 2017. № 3. С. 128–148. URL: http://surl.li/qjesp

16. Сторчак А.С., Сидоркін П.Г., Микитюк А.В., Сальник С.В. Модель оцінки впливу загроз на стан захищеності систем електронних комунікацій. *Системи озброєння і військова техніка*. 2019. № 2. С. 46–54.

17. Трифонова О.М., Павлюк Д.А. Співпраця студентів спеціальності 015 Професійна освіта (Цифрові технології) зі стейкхолдером: департаментом кіберполіції України. *Управління розвитком ЗП(ПТ)О на засадах педагогічної логістики: стан, реалії, досвід:* матер. Всеукр наук.-практ. конф., м. Київ, 17.11.2022. Чернівці, 2022. С. 221–223.

18. Юдін О.К.,Бучик С.С. Державні інформаційні ресурси. Методологія побудови класифікатора загроз: монографія. Київ: НАУ, 2015. 214 с.