Важливим інструментом протидії є концепція кіберстримування, яка передбачає формування здатності держави до ефективної відповіді на загрози. Її реалізація потребує розвитку кадрового потенціалу, міжнародної співпраці та впровадження сучасних підходів до кіберзахисту [2, с. 183]. Важливим аспектом є також підвищення рівня кіберграмотності населення. Це дозволяє зменшити вплив інформаційних атак та маніпуляцій. Крім того, держави активно впроваджують стратегії кібербезпеки на національному рівні.

Отже, кіберпростір є важливим елементом сучасної архітектури міжнародної безпеки, що визначає нові принципи взаємодії держав. Його значення постійно зростає, що потребує вдосконалення механізмів захисту та координації міжнародної діяльності у сфері кібербезпеки. У перспективі роль кіберпростору лише посилюватиметься, що робить необхідним подальший розвиток міжнародного співробітництва. Ефективна кібербезпекова політика стає важливою умовою забезпечення стабільності світового порядку.

ЛІТЕРАТУРА:

1. Козій А., Марченко Т., Шевченко В. Актуальні проблеми протидії кіберзлочинності в Україні. *Theoretical foundations of state and law*. 2022. P. 59–65.

2. Лугіна Н. А., Лучук А. М. Порівняльний аналіз вітчизняного та європейського законодавства з питань запобігання кіберзлочинності. *Ірпінський юридичний часопис*. 2023. № 1(10). С. 180–186.

3. Онищенко С., Глушко А. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. *Економіка і регіон*. Національний університет ім. Юрія Кондратюка. 2022. № 1 (84). С. 13–20.

4. Пелих А. О. Кіберпростір як новий вимір міжнародної безпеки // *Гілея: науковий вісник*. Київ, 2023. Вип. 182. С. 65–70.

УДК 351:004

Голда М.
аспірат Західноукраїнського національного університету

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Одним із наріжних каменів системи управління на всіх рівнях функціонування суб’єктів організованої діяльності – від підприємницьких структур, господарських організацій і бюджетних установ до органів та інституцій регіональної й загальнодержавної законодавчої та виконавчої влади – є належне інформаційне забезпечення. Без відповідної інформації не може бути прийняте жодне управлінське рішення. Роль інформаційного забезпечення невпинно зростає в умовах інформаційного суспільства та розвитку інформаційних технологій.

У сучасних умовах ефективність державного управління, функціонування господарського комплексу країни, діяльність підприємств, установ і організацій значною мірою залежать від рівня та досконалості інформаційного

забезпечення. Таким чином, інформація та робота з нею стають самостійним об'єктом дослідження, що потребує систематизації його елементів і складових, структурування, організації, планування та управління. У зв'язку з цим відповідного оформлення потребує і понятійний апарат.

Сегмент інформаційного забезпечення в системі організаційної та управлінської діяльності державних, господарських, соціальних та інших суспільних структур охоплює необхідність визначення ролі інформації, дослідження особливостей формування інформаційно-комунікаційного суспільства, класифікації інформаційних ресурсів, інфраструктури інформації. Окремий важливий блок інформаційного забезпечення охоплює питання законодавства та нормативно-правового регламентування, розгляду інформації як об'єкта правових відносин, правового регулювання захисту та обмеження доступу до відповідної інформації, системи правового регулювання відносин в інформаційні сфері. Особливу увагу при цьому слід приділяти дотриманню та забезпеченню національних інтересів України в інформаційній сфері [1, с.7].

Однією із визначальних по значенню складових діяльності в інформаційній сфері та інформаційному забезпеченні є інформаційна безпека. При цьому передумовами забезпечення її належного рівня безумовно є необхідність врахування та логічного дотримання відповідних теоретичних і методологічних імперативів, по-перше, в роботі з самою інформацією, по-друге, власне в процесі обґрунтування і формування адекватних механізмів інформаційної безпеки.

Стосовно роботи з інформацією в теоретико-методологічному плані принципово важливими є вимоги щодо формування відповідних інформаційних матеріалів. Вони повинні бути: *об'єктивними* (реально відображати дійсний стан та фактичну ситуацію щодо розглядуваних питань, тем чи проблем); *достовірними* (точно відображати реальну ситуацію, спиратися на факти, не допускати домислів, особистих трактувань, не видавати «бажане за дійсне»); *своєчасними* (надходити вчасно, до вироблення та прийняття відповідного управлінського рішення); *оптимальними* (бути достатніми для здійснення необхідного аналізу та вироблення оптимального рішення); *релевантними* – близькими до «адекватності», але водночас характеризувати не лише ступінь відповідності поставленому запиту, а й можливості практичного застосування результату [2, с.21].

Методологія роботи з формування відповідних масивів даних в контексті інформаційного забезпечення передбачає використання певних організаційних підходів щодо, по-перше, класифікації інформації за критеріями і видами, а також типами та видами джерел інформації; по-друге, виділенням етапів в самій системі роботи з інформацією у відповідних сферах чи галузях (збір інформації, обробка, попередній аналіз і порівняння, фільтрація, оцінка і систематизація, аналіз інформації і формування висновків для передачі за призначенням відповідно до запиту та формування бази даних по відповідній темі) [3, с.205].

Оскільки наявність відповідної інформації та інформаційне забезпечення діяльності щодо прийняття відповідних рішень передбачає досягнення певної мети та переслідує конкретні цілі, то не можна упускати з поля зору існування

певних ризиків та загроз щодо передбаченого використання конкретних інформаційних ресурсів. В зв'язку з цим на передній план виходять такі, наповнені відповідним змістом поняття, як захист інформації, інформаційна безпека та діяльність по забезпеченню інформаційної безпеки.

Об'єктивність існування ризиків та загроз щодо системи інформаційного забезпечення зумовлюється постійним конфліктом конкурентних інтересів між певними суб'єктами як всередині країни (внутрішні ризики і загрози), так і у міжнародних відносинах (зовнішні ризики і загрози). Такі конфлікти інтересів можуть виникати у різних галузях та сферах діяльності, зокрема технологічного, економічного, фінансового, політичного чи військового характеру. Це яскраво засвідчується подіями в глобалізованому світі впродовж останніх десятиліть. Таким чином інформація та інформаційні технології стають об'єктами зовнішніх і внутрішніх загроз, посилюючи проблему забезпечення інформаційної безпеки перед усім держави.

Вітчизняними авторами інформаційна безпека трактується як захищеність основних інтересів особи, суспільства і держави у сфері інформації, включаючи інформаційну й телекомунікаційну інфраструктуру і власне інформацію та її параметри, такі як повнота, об'єктивність, доступність і конфіденційність. При цьому зазначається, що інформаційна безпека є складовою національної безпеки, а її особливістю є те, що вона, як невід'ємна частина, входить до інших складових національної безпеки: економічної, воєнної, політичної безпеки тощо [4, с.10]. Більш широке тлумачення наповнення дефініції «інформаційна безпека держави» охоплює стан захищеності національних інтересів України в інформаційній сфері від загроз особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інформації, несанкціоноване поширення та використання інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій [5, с.175]. На рівні підприємницьких структур інформаційна безпека розглядається як захищеність цього виду діяльності від загроз в інформаційній сфері. При цьому множина завдань, виконання яких повинна забезпечити інформаційна безпека, залежить від характеру та особливостей відповідного виду діяльності, однак найбільш важливим елементом системи інформаційної безпеки фірми підприємства, корпорації є захист комерційної таємниці [6, с.33].

Таким чином, ефективне забезпечення інформаційної безпеки передбачає функціонування цілісної системи, що включає такі сегменти: визначення основних векторів політики держави у забезпеченні інформаційної безпеки; нормативно-правове регулювання; прогнозування та аналітична оцінка можливих загроз інформаційній безпеці на макро- та мікрорівнях; організація та координація функціонування уповноважених державних інституцій; матеріально-технічне і фінансове забезпечення даної сфери.

Література:

1. Біленчук П.Д., Борисова Л.В. та ін. Правові засади інформаційної безпеки України. Харків. 2018. 289 с.

2. Фліссак К.А. Методологічні вимоги до інформаційного забезпечення в економічній дипломатії. *Економічний часопис-XXI*, 2013. №3-4. С.20-23

3. Фліссак К.А. Економічна дипломатія у системі забезпечення

національних інтересів України: монографія. Тернопіль: Новий колір. 2016. 812 с.

4. Гур'єв В.І., Мехед Д.Б. та ін. Інформаційна безпека держави. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея». 2018. 166 с.

5. Шатун В.Т., Гладун О.В. Інформаційна безпека – невід'ємна складова національної безпеки України. *Наукові праці. Державне управління*. 2016. Вип. 255, том 267, С. 174-180

6. Носок С.О., Коломицев М.В., Стьопочкіна І.В. Управління інформаційною безпекою. Київ: КПІ ім. Ігоря Сікорського. 2025, 88 с.

УДК 343.9

Василова О. В.
к.ю.н., асистент кафедри кримінального права,
Чернівецький національний університет
імені Юрія Федьковича

АНАЛІТИЧНІ ІНСТРУМЕНТИ КРИМІНАЛЬНОГО АНАЛІЗУ

Прикладні інструменти і платформи кримінального аналізу становлять ключовий технологічний компонент сучасного інформаційно-аналітичного забезпечення правоохоронної діяльності. Їх використання забезпечує можливість систематизованої обробки значних обсягів цифрових даних, встановлення взаємозв'язків між об'єктами кримінального аналізу, виявлення закономірностей злочинної діяльності та формування обґрунтованих аналітичних висновків. У наукових працях вітчизняних вчених зазначено, що ефективність кримінального аналізу безпосередньо залежить від функціональних можливостей інструментальних платформ, рівня їх технологічної інтеграції та відповідності вимогам достовірності, відтворюваності й процесуальної допустимості отриманих результатів [1].

З метою систематизації сучасного інструментарію кримінального аналізу доцільним є проведення їх порівняльного аналізу за функціональними, технологічними та методологічними характеристиками. Узагальнення результатів сучасних українських і міжнародних наукових досліджень, а також практичних рекомендацій у сфері цифрової криміналістики та кримінального аналізу, дозволяє виділити основні методи кримінального аналізу, що застосовуються в умовах цифрового середовища, їх функціональне призначення, інформаційну основу, аналітичні можливості та процесуальне значення (табл. 1).