УДК 004.056
DOI https://doi.org/10.32782/pdu.2024.4.12

М. О. Шевчук
кандидат юридичних наук,
докторант кафедри конституційного, адміністративного та фінансового права
Хмельницького університету управління та права імені Леоніда Юзькова
https://orcid.org/0000-0001-7549-6344

ПОНЯТТЯ СУБ'ЄКТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Цю статтю присвячено дослідженню поняття суб'єкта інформаційної безпеки, яке є ключовим для забезпечення захисту інформаційного простору в контексті сучасних глобальних викликів. У роботі визначено суб'єктів інформаційної безпеки – суспільство, державу та особу (фізичну та юридичну). Особливу увагу приділено аналізу ролі кожного з цих суб'єктів у забезпеченні інформаційної безпеки, їхній взаємодії та реагуванню на загрози в інформаційному середовищі. Суспільство розглядається як колективний суб'єкт, здатний формувати загальну інформаційну культуру, розвивати ініціативи з підвищення медіаграмотності та здійснювати громадський контроль за дотриманням норм інформаційної безпеки. Роль держави проявляється в таких функціях, як формулювання та реалізація правових норм, розроблення національної політики в галузі інформаційної безпеки та співпраця з міжнародними організаціями. У роботі підкреслюється, що без відповідного державного регулювання неможливо досягти високого ступеня захисту інформаційного простору. Як суб'єктів, які безпосередньо беруть участь у реалізації заходів інформаційної безпеки, визначено фізичних та юридичних осіб. Особлива увага приділяється ролі юридичних осіб, які відіграють важливу роль у сфері кібербезпеки, конфіденційності даних і розвитку нових технологій. Також акцентується увага на питанні взаємодії суб'єктів інформаційної безпеки. Зазначається, що ефективне розв'язання сучасних загроз можливе лише за умови координації дій суспільства, держави та приватного сектору. Автори наголошують на важливості створення спільної платформи для обміну інформацією та досвідом, а також покращення співпраці між зацікавленими сторонами. Підсумком дослідження є формулювання висновків щодо важливості кожного із суб'єктів інформаційної безпеки та підготовка рекомендацій щодо оптимізації їхньої взаємодії задля досягнення високого ступеня захисту інформаційного середовища.

Ключові слова**:** *інформаційна безпека, суб'єкти інформаційної безпеки, суспільство, держава, фізичні особи, юридичні особи, інформаційний простір, кібербезпека, законодавче регулювання, взаємодія суб'єктів.*

Постановка проблеми. У сучасному світі інформація стала одним із базових ресурсів для розвитку суспільств, держав і підприємств. Водночас зі зростанням залежності від інформаційних технологій зростає і ризик виникнення загроз в інформаційному середовищі, таких як кібератаки, витоки інформації, дезінформація та інформаційний вплив. Ці виклики вимагають формування комплексної системи інформаційної безпеки з чітко визначеними учасниками, їхніми ролями та функціями для захисту інформаційного простору. Незважаючи на значну кількість досліджень у галузі інформаційної безпеки, проблема визначення суб'єктів інформаційної безпеки та їхньої взаємодії залишається актуальною. Це пов'язано з тим, що ефективна протидія сучасним інформаційним загрозам потребує узгоджених зусиль усіх суб'єктів – суспільства, держави, фізичних та юридичних осіб. Відсутність належного правового регулювання, недостатня взаємодія суб'єктів та низька обізнаність населення про механізми інформаційної безпеки суттєво ускладнюють забезпечення інформаційної безпеки. Розв'язання цієї проблеми

має велике наукове і практичне значення, оскільки пов'язане з розвитком національної та глобальної безпеки, впровадженням інноваційних технологій у сфері кіберзахисту та забезпеченням стабільного функціонування державних і приватних структур в умовах наростання інформаційних загроз. Тому вивчення суб'єктів інформаційної безпеки, їхніх повноважень та взаємодії є важливим кроком на шляху побудови ефективної системи захисту інформаційного простору.

Аналіз останніх досліджень. Дослідження ролі суб'єктів інформаційної безпеки в забезпеченні національної інформаційної безпеки є предметом численних наукових робіт як вітчизняних, так і міжнародних вчених, серед яких О. І. Безпалова, О. Г. Данильян, О. П. Дзьобань, М. М. Присяжнюк, Т. Ю. Ткачук, О. Д. Довгань, В. Т. Шатун та інші. Однак багато з цих досліджень мають фрагментарний характер, часто описуючи лише окремі аспекти діяльності суб'єктів інформаційної безпеки або вивчаючи вплив конкретних загроз на національне інформаційне середовище. Більшість досліджень обмежується аналізом окремих механізмів захисту або теоретичних підходів до регулювання сектору на національному рівні. Водночас на сьогодні не існує ані комплексних досліджень, які б узагальнювали всі аспекти взаємодії суб'єктів інформаційної безпеки, ані чітко сформульованих наукових концепцій чи моделей, які б охоплювали всі аспекти інформаційного середовища та його впливу на національну безпеку в контексті сучасних інформаційних загроз.

Метою цієї статті є визначення та систематизація суб'єктів інформаційної безпеки, зокрема суспільства, держави, фізичних та юридичних осіб, а також аналіз їхньої ролі, функцій та взаємодії у забезпеченні захисту інформаційного простору.

Виклад основного матеріалу. Інформаційна безпека – це багатоаспектне поняття, що містить сукупність заходів, процесів і механізмів, спрямованих на забезпечення захисту інформації від несанкціонованого доступу, неправомірного використання, несанкціонованої модифікації, несанкціонованого пошкодження або знищення. Інформаційна безпека охоплює як технічні, так і організаційні аспекти захисту інформаційного середовища з урахуванням інтересів усіх зацікавлених сторін, включно із суспільством, державою, фізичними та юридичними особами.

Концепція інформаційної безпеки заснована на забезпеченні конфіденційності, цілісності та доступності інформації. Під конфіденційністю розуміють запобігання несанкціонованому доступу до інформації, під цілісністю – збереження точності інформації та захист її від несанкціонованих змін, а під доступністю – забезпечення доступу авторизованих користувачів до інформації в потрібний час.

Інформаційна безпека охоплює й соціальні аспекти, оскільки є важливим засобом підтримання соціальної стабільності, збереження інформаційної культури та протидії дезінформації. На національному рівні інформаційна безпека забезпечується шляхом ухвалення відповідного законодавства, реалізації національної стратегії інформаційної безпеки та розвитку інфраструктури кібербезпеки.

З бурхливим розвитком інформаційних технологій інформаційна безпека набуває ще більшого значення, оскільки сучасний інформаційний простір є не лише засобом комунікації, а й форумом для економічної, політичної та соціальної взаємодії. Забезпечення інформаційної безпеки стає важливою умовою стабільного функціонування суспільств, держав і підприємств, а також ключовим чинником захисту прав і свобод людини в цифрову епоху.

Основні загрози інформаційній безпеці різноманітні та мають широкий спектр впливу на інформаційне середовище. Однією з найсерйозніших загроз є кіберзлочинність, включно з несанкціонованим доступом до інформаційних систем, крадіжкою даних, шкідливим ПЗ та атаками на комп'ютерні мережі, які можуть завдати серйозної фінансової та репутаційної шкоди організаціям і приватним особам.

Іншою важливою загрозою є соціальна інженерія. Соціальна інженерія – це маніпулювання людьми з метою отримання конфіденційної інформації. Соціальна інжене-

рія проявляється у фішингу, шахрайстві та інших методах психологічного впливу, які дають змогу зловмисникам отримати доступ до конфіденційних даних і систем. Соціальна інженерія – одна з найскладніших загроз, оскільки вона використовує психологію людини, що ускладнює її виявлення за допомогою автоматизованих засобів захисту.

До загроз інформаційній безпеці також належать інциденти, пов'язані з втратою або крадіжкою інформації. До них належать випадкові або навмисні витоки даних, неправильне зберігання або обробка. У таких випадках, особливо якщо йдеться про персональні дані та корпоративну інформацію, наслідки можуть бути вкрай серйозними, включно з юридичними наслідками та втратою довіри з боку клієнтів і партнерів. Ще одна важлива загроза – інформаційний вплив, що виявляється в поширенні дезінформації, маніпулюванні ЗМІ та фальшивих новин. Такі загрози можуть чинити істотний вплив на громадську думку, політичну стабільність та економічну ситуацію і є важливою частиною загроз інформаційній безпеці на національному рівні [4].

Загрози також можуть виникати через недосконалість інформаційних інфраструктур, таких як неадекватний захист програмного забезпечення, відсутність надійних механізмів резервного копіювання даних і слабкий контроль доступу до конфіденційної інформації. Це відкриває зловмисникам можливість використовувати технічні вразливості для атак на системи та витоку важливої інформації.

Поділ суб'єктів інформаційної безпеки – найважливіший аспект забезпечення ефективного захисту інформаційного простору. Такий поділ дає змогу чітко визначити ролі, обов'язки та відповідальність кожного із суб'єктів, які беруть участь у забезпеченні інформаційної безпеки, а також способи їхньої взаємодії для досягнення спільної мети – захисту даних та інформаційних систем від різних загроз. Визначення конкретних суб'єктів допоможе більш ефективно організувати заходи безпеки і знизити ризик помилок і недостатньої уваги до важливих аспектів захисту.

Розрізнення суб'єктів також важливе під час розроблення правових норм і політики в галузі інформаційної безпеки. Кожен суб'єкт – держава, суспільство, фізична або юридична особа – має свої права та обов'язки, визначені законом або міжнародними угодами. Таке розмежування сприяє чіткому визначенню відповідальності за порушення стандартів інформаційної безпеки, що, своєю чергою, вдосконалює систему правового регулювання в цій галузі.

Ще одним важливим фактором є те, що поділ відповідальності допомагає оптимізувати координацію між різними учасниками процесу забезпечення інформаційної безпеки. Без чіткого розподілу обов'язків між державою, суспільством та окремими людьми можуть виникнути прогалини в управлінні інформаційними ресурсами та неадекватна реакція на нові загрози. Наприклад, державна політика може залишатися неефективною без належної підтримки з боку громадян і бізнесу, а приватні компанії не зможуть вирішувати проблеми без відповідної правової бази.

Крім того, поділ організацій забезпечує більш чіткий механізм захисту інформації на різних рівнях. Це включає в себе технічні та організаційні заходи безпеки, які повинні бути реалізовані різними учасниками процесу. В іншому разі це загрожує неузгодженістю і збільшенням числа успішних атак і витоків даних. Тому чітке розмежування сторін є необхідною умовою для створення системи, здатної ефективно протистояти сучасним загрозам інформаційної безпеки.

Місце суспільства в забезпеченні інформаційної безпеки вкрай важливе. Це пов'язано з тим, що саме громадяни є суб'єктами інформаційної безпеки, оскільки саме вони виконують більшу частину роботи зі створення безпечного інформаційного середовища. Суспільство є не лише користувачем інформаційних ресурсів, а й активним учасником процесу захисту інформації та відіграє важливу роль у формуванні загальної інформаційної культури. Одна з основних функцій суспільства – підвищення рівня медіаграмотності та інформування громадян про

можливі загрози в інформаційному середовищі, такі як фішинг, шкідливе ПЗ та інші види кіберзлочинності.

Суспільство також може сприяти розвитку ефективних ініціатив у сфері інформаційної безпеки, зокрема, обговорюючи питання інформаційної безпеки на рівні органів державної влади та організовуючи кампанії з підвищення обізнаності щодо захисту персональних даних та кібергігієни. Завдяки активній участі в таких процесах суспільство може стати потужною рушійною силою змін на законодавчому рівні та в розвитку інфраструктури безпеки. Ініціативи громадян часто сприяють виявленню нових загроз і створенню нових технологічних рішень для їх подолання.

Ще один важливий елемент – контроль громадян за дотриманням стандартів інформаційної безпеки. Громадськість може впливати на поведінку компаній та державних установ, вимагаючи від них підвищення рівня захисту даних та інформаційних систем. Громадськість може вимагати прозорості політики обробки даних через організації споживачів, правозахисні організації та інші платформи, що може призвести до підвищення рівня захисту загалом.

Громадськість також є ключовою фігурою в разі кризи, коли виникають загрози національній безпеці або кібербезпеці. Виявлення громадянами потенційних кіберінцидентів і повідомлення про них дає змогу державам і приватним організаціям швидше реагувати на загрози. У цьому контексті для загальної стабільності інформаційного простору важливо, щоб кожен громадянин брав активну участь у забезпеченні своєї власної цифрової безпеки.

Громадські ініціативи допомагають у протидії інформаційним загрозам, підвищуючи обізнаність суспільства про ризики в інформаційному середовищі та створюючи механізми їх запобігання. Одним з основних напрямків таких ініціатив є просвітництво громадян і підвищення медіаграмотності. Оскільки багато загроз в інформаційному просторі виникають через неповне розуміння користувачами принципів безпеки та методів роботи, організації громадянського суспільства беруть активну участь у наданні людям знань про те, як розпізнати фальшиві новини, шкідливе ПЗ та інші види кібератак.

Важливою частиною діяльності громадянського суспільства є створення платформ для обміну інформацією та досвідом у сфері інформаційної безпеки. Такі платформи дають змогу користувачам бути в курсі загроз, що виникають, і дізнаватися про ефективні методи захисту. Крім того, організації громадянського суспільства часто організовують тренінги, семінари та кампанії, щоб допомогти людям зрозуміти важливість цифрової безпеки та освоїти основи захисту персональних даних і конфіденційної інформації.

Ініціативи громадянського суспільства також включають активну участь у розробці політики та законодавства в галузі інформаційної безпеки. Взаємодіючи з державними органами, бізнесом і міжнародними організаціями, громадськість може ініціювати зміни в законодавстві, спрямовані на поліпшення захисту від кіберзагроз і підтримку прав і свобод людини в цифровому середовищі. Іншим аспектом є контроль за дотриманням наявних норм і стандартів у сфері інформаційної безпеки, при цьому організації громадянського суспільства часто виступають незалежними спостерігачами.

Ще одним ефективним механізмом є участь громадськості у виявленні загроз та інформуванні про них. Численні онлайн-спільноти та платформи дають змогу користувачам обмінюватися інформацією про кіберінциденти, що дає змогу швидше реагувати на нові атаки або спроби маніпулювання. Крім того, взаємодія громадськості з владою і бізнесом може допомогти розробити більш ефективні стратегії протидії інформаційним загрозам і спільно вирішити проблему виявлення і нейтралізації кіберзлочинів.

Загалом громадські ініціативи є потужним інструментом забезпечення інформаційної безпеки, оскільки вони сприяють формуванню відповідального ставлення до захисту даних, розповсюдженню заходів безпеки та підвищенню оперативності й швидкості реагування на загрози. Вза-

ємодія громадськості, держави та приватного сектору є основою для побудови більш надійної та стійкої системи боротьби з інформаційними загрозами [1].

Колективна свідомість – елемент, що формує основу для ефективного захисту інформаційного простору. Це поняття включає в себе загальні переконання, цінності та соціальні норми, які визначають ставлення громадян до використання інформаційних технологій і захисту даних. В умовах цифрової трансформації та постійного розвитку нових технологій колективна обізнаність набуває особливого значення і слугує основою для формування загальної інформаційної культури, включно зі знаннями про кіберзагрози та способи їх запобігання.

Колективна обізнаність з акцентом на інформаційну безпеку має на увазі взаємне розуміння людьми важливості захисту персональних даних і спільне прагнення до створення безпечного інформаційного середовища. Високий рівень колективної обізнаності дає змогу громадянам виробити правильне ставлення до питань, пов'язаних із кібербезпекою, виявленням шкідливих програм і захистом від фішингу та інших форм онлайн-злочинності. У таких суспільствах кожен член спільноти дедалі більше вмотивований долучатися до підтримання безпеки інформаційного простору і вміти розпізнавати загрози та реагувати на них.

Важливим елементом колективної свідомості є спільна відповідальність за захист інформаційного простору. Усвідомлення громадянами своєї ролі у формуванні безпечного середовища може сприяти розробленню відповідних ініціатив і законодавчих заходів, спрямованих на забезпечення кібербезпеки. Наприклад, за підтримки держави та приватного сектору можуть бути реалізовані програми з підвищення медіаграмотності, розповсюдження знань про кібергігієну та навчання громадян основ захисту в Інтернеті.

Захист інформаційного простору через колективну обізнаність не обмежується індивідуальними діями. Він охоплює формування колективних зусиль на рівні організацій, громадських ініціатив та державної політики. Коли громадяни активно співпрацюють з державними органами та бізнесом, діляться своїм досвідом і знаннями, вони можуть побудувати більш стійку систему протидії інформаційним загрозам. Колективна обізнаність сприяє не тільки індивідуальній безпеці, а й стійкості всієї інформаційної інфраструктури.

Державні завдання в галузі інформаційної безпеки є ключовим елементом забезпечення національної безпеки та сталого розвитку в умовах глобалізації інформаційного середовища. Одним з основних завдань держави є створення і впровадження нормативно-правової бази, що регулює всі аспекти інформаційної безпеки. Це охоплює розроблення та впровадження законодавчих і нормативних актів у сфері захисту інформації, кібербезпеки, захисту персональних даних і боротьби з кіберзлочинністю. Держави мають забезпечити гармонізацію національних норм з міжнародними стандартами та їхню інтеграцію в глобальні механізми захисту інформаційного простору.

Другим завданням держав є створення ефективних систем моніторингу та реагування на інформаційні загрози. Вони мають бути оснащені інструментами для виявлення кіберзагроз і шкідливого ПЗ, а також засобами для швидкої нейтралізації таких загроз на всіх рівнях – від інфраструктури до персональних терміналів. Це також охоплює створення спеціалізованих агентств і організацій з кібербезпеки, які можуть координувати дії державних установ, приватного сектору та міжнародних партнерів у боротьбі з кіберзлочинністю.

Не менш важливим є завдання держави в галузі освіти та підвищення медіаграмотності населення. У сучасному світі зростає необхідність підготовки громадян до безпечної поведінки в інформаційному середовищі. Держави повинні проводити програми з навчання та інформування населення про основи інформаційної безпеки, щоб кожен володів знаннями, необхідними для захисту персональних даних і запобігання таким загрозам, як фішинг і шкідливе ПЗ. Воно також має активно сприяти розвитку дослідницьких та освітніх ініціатив у сфері кібербезпеки.

Ще одне завдання держави – захист критичної інформаційної інфраструктури.

Це включає в себе створення систем, що забезпечують стабільність і безпеку ключових секторів, які мають стратегічне значення для держави, таких як енергетика, транспорт і фінанси. Держави повинні забезпечити захист цих інфраструктур від кібератак, які можуть мати серйозні наслідки для національної безпеки [3].

Крім того, держави повинні відігравати важливу роль у міжнародному співробітництві в галузі інформаційної безпеки. З огляду на транснаціональний характер сучасних загроз, держави повинні активно співпрацювати з іншими державами та міжнародними організаціями для обміну інформацією, досвідом і ресурсами в боротьбі з кіберзлочинністю. Це включає в себе участь у міжнародних угодах, ініціативах і стандартах з кібербезпеки.

Загалом, завдання держав у сфері інформаційної безпеки включають створення нормативної бази, забезпечення кіберзахисту інфраструктури, просвіту населення та активне міжнародне співробітництво. Це дає змогу створити ефективну систему захисту від інформаційних загроз, яка є основою для стабільного функціонування держави в цифрову епоху.

Законодавство і національна політика в галузі інформаційної безпеки є основою для створення ефективної системи захисту інформаційного простору країни. У зв'язку зі стрімким розвитком інформаційних технологій і зростанням загроз у кіберпросторі держави повинні створити чітку нормативно-правову базу, що забезпечує надійний захист державних і приватних інформаційних ресурсів. Усі аспекти інформаційної безпеки, включно із захистом персональних даних, кіберзахистом, боротьбою з кіберзлочинністю та захистом критичної інфраструктури від можливих атак, мають бути закріплені на законодавчому рівні.

Важливим елементом законодавчого регулювання є ухвалення законів і підзаконних актів, що встановлюють правила оброблення та зберігання інформації, а також вимоги до захисту інформаційних систем і мереж. Таке законодавство має враховувати міжнародний досвід і відповідати останнім стандартам у сфері кібербезпеки, але водночас створювати національні механізми, які дають змогу ефективно реагувати на загрози. Також важливо встановити відповідальність за порушення правил інформаційної безпеки та передбачити механізми покарання осіб та організацій, які порушують ці правила.

Національна політика в галузі інформаційної безпеки охоплює розроблення та реалізацію національних стратегій, програм і планів, які визначають напрямок довгострокових зусиль у цій галузі. Важливо, щоб національна політика була комплексною і враховувала всі елементи інформаційної безпеки, а також включала ініціативи з розвитку інформаційних технологій, створення безпечної інфраструктури та підвищення рівня медіаграмотності. Вона також має бути спрямована на захист національних інтересів у глобальному інформаційному середовищі, де міжнародні норми і стандарти можуть мати значний вплив на національну політику.

Особливе значення має координація дій між державними органами, приватним сектором і громадянським суспільством. Відповідно до законодавства та державної політики важливо, щоб усі суб'єкти інформаційної безпеки мали чітке уявлення про свої права та обов'язки і координували свої дії щодо боротьби з кіберзлочинністю, захисту персональних даних і підтримання національної інформаційної безпеки.

Крім того, держави повинні активно співпрацювати з міжнародними організаціями та іншими державами для розроблення загальних стандартів і механізмів реагування на кіберзагрози. Така міжнародна співпраця є ключем до боротьби з транснаціональною кіберзлочинністю та забезпечення глобальної інформаційної безпеки. Обмін досвідом з міжнародними партнерами дасть змогу створити спільні інфраструктури для моніторингу та запобігання кіберзагрозам, а також обмінятися досвідом у розробленні законодавства в цій галузі. Правове регулювання і національна політика в галузі інформаційної безпеки є важливими інструментами забезпечення стійкості національних інформаційних інфраструктур і захисту державних і приватних інтересів у глобальному інформаційному просторі.

Фізичні та юридичні особи відіграють важливу роль у забезпеченні інформаційної безпеки, оскільки їхні права, обов'язки та функції безпосередньо впливають на захист національного інформаційного простору. Фізичні особи мають важливі права та обов'язки в інформаційному просторі, включно з правами на захист персональних даних, конфіденційність інформації та безпеку під час використання інформаційних технологій. Однак ці права також тягнуть за собою певні обов'язки. Громадяни повинні дотримуватися законів про інформаційну безпеку, не розголошувати конфіденційну інформацію, захищати персональні дані від несанкціонованого доступу і використовувати технології та послуги, що відповідають вимогам безпеки. Вони також мають бути готовими співпрацювати з державними органами та правоохоронними органами, якщо це необхідно, наприклад, у разі кіберзлочинів або інших загроз [5].

Юридичні особи, такі як компанії, організації та інші підприємства, повинні відігравати особливу роль у забезпеченні кібербезпеки. Будучи основними користувачами і розповсюджувачами інформаційних технологій, компанії роблять найважливіший внесок у захист інформаційного простору. Вони повинні розробляти і впроваджувати внутрішні політики, що забезпечують належний рівень захисту і сприяють забезпеченню безпеки своїх інформаційних систем і конфіденційних даних своїх клієнтів і партнерів. Це включає в себе впровадження новітніх технологій для запобігання кіберзагрозам, регулярне оновлення програмного забезпечення, установку антивірусних систем і навчання співробітників основам інтернет-безпеки та безпечного використання інформаційних технологій.

Юридичні особи за законом зобов'язані захищати інформацію, що має стратегічне значення для національної безпеки, і дотримуватися вимог щодо захисту персональних даних співробітників і клієнтів. Вони також відіграють ключову роль у розробці та підтримці стандартів кібербезпеки, особливо в корпоративному середовищі. Підприємства можуть співпрацювати з державними органами та іншими компаніями для створення безпечних інфраструктур і мінімізації ризиків, пов'язаних із кіберзлочинністю. Роль юридичної особи особливо важлива в умовах розвитку таких технологій, як блокчейн, штучний інтелект та Інтернет речей, коли питання безпеки стають дедалі актуальнішими не лише для компаній, а й для широкого кола споживачів та громадян.

Усі ці аспекти вказують на те, що фізичні та юридичні особи є активними суб'єктами інформаційної безпеки та повинні діяти відповідно до закону, враховуючи свої права та обов'язки в інформаційному середовищі та забезпечуючи належний рівень захисту як для себе, так і для інших учасників інформаційного простору.

Взаємодія суб'єктів інформаційної безпеки необхідна для ефективного захисту інформаційного простору від численних загроз. Координація дій суспільства, держав, фізичних і юридичних осіб створює систему, в якій кожен учасник сприяє у забезпеченні безпеки. Суспільство, як колективний суб'єкт, сприяє підвищенню обізнаності про загрози в інформаційному просторі та забезпечує рівень медіаграмотності громадян. Держави, своєю чергою, створюють нормативно-правову базу, розробляють національні стратегії кібербезпеки та координують дії з міжнародними партнерами. Фізичні та юридичні особи, як суб'єкти, що безпосередньо мають справу з даними, інформаційними технологіями та інфраструктурою, мають дотримуватися вимог законодавства та активно впроваджувати заходи щодо запобігання загрозам [2].

Важливість спільних дій у боротьбі з інформаційними загрозами неможливо переоцінити. Ефективний захист інформаційного простору можливий тільки в тому разі, якщо всі зацікавлені в інформаційній безпеці сторони об'єднаються для вирішення спільних завдань. Суспільство поширюватиме інформацію про загрози, що виникають, підтримуватиме ініціативи з підвищення медіаграмотності та допомагатиме формувати громадську думку про важливість кібербезпеки. Держави відіграватимуть свою роль і розроблятимуть політику для забезпечення спільного захисту та обміну інформацією

на національному та міжнародному рівні. Юридичні та фізичні особи, компанії та організації повинні проактивно реагувати на виклики, вдосконалювати свої інформаційні системи та підтримувати політику захисту та безпеки даних.

Водночас взаємодія між зацікавленими сторонами у сфері інформаційної безпеки не обходиться без проблем. Однією з головних є проблема узгодження інтересів різних сторін. Держави можуть встановлювати вимоги, які економічно або технічно складні для компаній. Водночас компанії можуть прагнути скоротити витрати на забезпечення безпеки, що може призвести до неадекватного впровадження заходів безпеки. Ще одна проблема полягає в тому, що громадяни мають різний рівень обізнаності про загрози та ставлення до кібербезпеки. Навіть за наявності законодавства та урядових ініціатив щодо боротьби з кіберзлочинністю громадяни можуть недооцінювати ризики та не завжди реагувати належним чином. Крім того, технології постійно розвиваються, що вимагає від суб'єктів інформаційної безпеки постійно вдосконалювати свої стратегії та підходи, щоб захиститися від нових видів загроз, таких як кібертероризм, кібершпигунство та атаки на критично важливу інфраструктуру.

Висновки. Основні висновки щодо концепції суб'єктів інформаційної безпеки вказують на важливість кожного учасника (суспільство, держава, фізичні та юридичні особи) у цьому процесі. Усі ці суб'єкти мають свої функції та завдання і доповнюють один одного для створення системи, здатної ефективно протистояти загрозам інформаційній безпеці. Суспільство, завдяки своїй колективній поінформованості, може значно підвищити рівень поінформованості щодо загроз та необхідності дотримання стандартів безпеки, а держава створює правову базу, координує дії на національному та міжнародному рівні та виконує контрольні функції. Фізичні та юридичні особи безпосередньо взаємодіють з інформаційними системами і тому несуть відповідальність за захист даних та підтримання належного рівня кібербезпеки.

Рекомендації щодо поліпшення співпраці між суб'єктами інформаційної безпеки вказують на необхідність зміцнення зв'язків між державами, компаніями та громадянами. Необхідно впроваджувати механізми обміну інформацією, створювати спільні платформи для співпраці та ділитися передовим досвідом. Держави мають запустити програми, спрямовані на підвищення рівня медіаграмотності громадян, і розробити комплексну стратегію зі стимулювання компаній до впровадження найкращих стандартів кібербезпеки. Підприємства повинні активно впроваджувати новітні технології для забезпечення захисту даних і співпрацювати з державними органами для створення надійної інфраструктури.

Перспективи розвитку інформаційної безпеки в бізнес-структурах передбачають постійне вдосконалення стратегій і технологій захисту в умовах швидко мінливого технологічного середовища. Розвиток таких галузей, як штучний інтелект, блокчейн та Інтернет речей, створює нові можливості, але також підвищує ризики, пов'язані з кіберзлочинністю та іншими загрозами. У зв'язку з цим важливо постійно адаптувати законодавство і національні стратегії до нових реалій. Інформаційна безпека має бути не проблемою лише окремих структур, а спільною метою для всіх учасників – держав, компаній і суспільства. Лише завдяки ефективній співпраці та взаємній підтримці в майбутньому буде досягнуто високого рівня захисту інформаційного простору.

Список використаної літератури:

1. Безпалова О. І. Адміністративно-правовий механізм реалізації правоохоронної функції держави : монографія. Харків : НікаНова, 2019. 544 с.
2. Данильян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: структура та напрямки реалізації: навчальний посібник. Х.: Фоліо, 2020. 285 с.
3. Присяжнюк М.М. Інформаційна безпека України в сучасних умовах. Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. 2018. Вип. 30. С. 42–46.
4. Ткачук Т.Ю., Довгань О.Д. Система інформаційної безпеки України: онтологічні виміри. Інформація і право. 2018. № 1 (24). С. 89–104.

5. Шатун В.Т. Інформаційна безпека – невід'ємна складова національної безпеки України. Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія». 2019. Т. 267. Вип. 255. С. 174–180.

Shevchuk M. The concept of the subject of information security

this article is dedicated to exploring the concept of the subject of information security, which is crucial for ensuring the protection of the information space in the context of modern global challenges. The study identifies the subjects of information security as society, the state, and the individual (both physical and legal entities). Particular attention is given to analyzing the role of each of these subjects in ensuring information security, their interaction, and their responses to threats in the information environment. Society is considered a collective subject capable of shaping a shared information culture, developing initiatives to improve media literacy, and exercising public oversight over compliance with information security standards. The role of the state is manifested in functions such as formulating and implementing legal norms, developing national policies in the field of information security, and cooperating with international organizations. The paper emphasizes that achieving a high level of information space protection is impossible without appropriate state regulation. Physical and legal entities are defined as subjects directly involved in implementing information security measures. Particular attention is paid to the role of legal entities, which play a significant part in cybersecurity, data confidentiality, and the development of new technologies. The article also highlights the issue of interaction between the subjects of information security. It is noted that effective resolution of modern threats is only possible through coordinated actions by society, the state, and the private sector. The authors emphasize the importance of creating a shared platform for the exchange of information and experiences, as well as improving collaboration among stakeholders. The study concludes with the formulation of insights regarding the importance of each subject of information security and the preparation of recommendations for optimizing their interaction to achieve a high level of information environment protection.

Key words: *information security, subjects of information security, society, state, physical entities, legal entities, information space, cybersecurity, legislative regulation, interaction of subjects.*