УДК 323
DOI https://doi.org/10.20535/2308-5053.2024.4(64).322732

ПУБЛІЧНІ КОМУНІКАЦІЇ ТА МЕНЕДЖМЕНТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: ЧИННИКИ ПОЛІТИЧНОЇ ДЕТЕРМІНАЦІЇ

Сергеєв В. С.,
доктор політичних наук, доцент,
професор кафедри міжнародних відносин і політичного менеджменту
Державного університету «Житомирська політехніка»
ORCID ID: 0000-0001-7859-0408
sergeev_vs@hotmail.com

Загурська-Антонюк В. Ф.,
доктор наук з державного управління,
доцент, завідувач кафедри
міжнародних відносин і політичного менеджменту
Державного університету «Житомирська політехніка»
ORCID ID: 0000-0003-3334-4494
kgn_zvf@ztu.edu.ua

Пащенко В. І.,
кандидат політичних наук, доцент,
доцент кафедри міжнародних відносин та політичного менеджменту
Державного університету «Житомирська політехніка»
ORCID ID: 0000-0003-4385-0286
pashchenko.v.i@gmail.com

Актуальність. У наш час публічний вираз політичних уподобань кожної аудиторії вимагає прискіпливої уваги в умовах загроз національній безпеці. Особливості менеджменту публічної медіабезпеки на сучасному етапі передбачають узгодження як позиції акторів на національному рівні, так і визначення вектору еволюції медіа-середовища на невизначений термін в майбутньому.

Мета статті – виявлення чинників політичної детермінації публічних комунікацій в безпековій сфері.

Результати дослідження. Ефективність публічного спілкування влада – суспільство може суттєво вплинути на те, наскільки успішно громада справляється з кризою та оговтується від неї. Успішна публічна комунікація під час кризи часто починається задовго до політичних подій. Інформація має бути представлена таким чином, щоб її було легко зрозуміти, з повторним акцентуванням ключових моментів, щоб гарантувати їх збереження.

Висновки. В умовах сучасної України актуалізується питання експертно-аналітичного забезпечення публічних комунікацій з метою прорахунку ефекту від політико-комунікаційної діяльності. Політико-менеджерські підходи для організації безпекових комунікацій передбачають узгодження позиції між основними політичними групами в суспільстві. Публічні безпекові комунікації мають бути спрямовані на європеїзацію політико-комунікаційного середовища в Україні.

Ключові слова: політичний менеджмент, національна безпека, публічні комунікації, медіа-середовище, діджиталізація, політичні інститути, безпекові виклики.

Вступ. Комунікаційний вимір політичного менеджменту виступає вагомою проблемою сучасної політичної науки. В умовах діджиталізації політичні актори шукають способи забезпечення політичних інтересів та зв'язку з ключовими соціальними групами. Публічний вираз політичних уподобань кожної аудиторії вимагає прискіпливої уваги в умовах загроз національній безпеці. Сучасний міждисциплінарний дискурс наук публічного управління, політології, права та соціології акцентує увагу на нових викликах та загрозах, які містяться в комунікаційних повідомленнях. Менеджмент публічної

медіабезпеки на сучасному етапі передбачає узгодження як позиції політичних акторів на національному рівні, так і визначення вектору політичної детермінації медіа-середовища на невизначений термін в майбутньому на глобальному рівні.

Відтак публічні безпекові комунікації вимагають експертно-аналітичного забезпечення, ретельної підготовки та цілеспрямованого втілення. Смислове поле політико-комунікаційної безпеки на національному рівні регулює методи та прийоми, які застосовують сучасні політичні інститути з метою усунути елементи нестабільності, які можуть мати місце в контексті громадсько-політичних взаємодій. Стратегічна архітектура національної безпеки має комунікаційну складову не лише в контексті трансляції інформації або забезпечення рівня її конфіденційності та збереження. Вона також має бути спрямована на досягнення конкретних результатів в установленні позитивних відносин з «профільними» (анагжованими) групами громадськості. В особливих умовах сучасної України належить розбудовувати національну систему кризової публічної комунікації в контексті національної безпеки з метою протидії комунікаційним нападам країни-агресора.

Аналіз публікацій. Розвиток суміжних предметних сфер національної безпеки в інформаційному вимірі цікавить багатьох зарубіжних вчених. К. Хене та Дж. Х. П. Елофф розглядають міжнародні стандарти інформаційної безпеки та їх впливають на створення політики безпеки (Höne, Eloff, 2002), Дж. О. Імоніана обговорює валідність різних моделей політики інформаційної безпеки, зокрема в контексті їх практичної реалізації. Також Дж. О. Імоніана оцінює кілька моделей на основі ефективності, масштабованості та адаптованості до різних організаційних середовищ. Проведений аналіз свідчить про те, що жодна модель не підходить для всіх, і політика має бути пристосована до конкретних потреб організації (Imoniana, 2004), І. Х. Аль-Маяхі та С. П. Мансур зосередилися на розробці політики інформаційної безпеки, наголошуючи на необхідності структурованого та методичного підходу. Вчені пропонують рекомендації для організацій щодо розробки політик безпеки, які забезпечують захист інформаційних активів, узгоджуючи ці політики з цілями організації та нормативними вимогами. Він наголошує на важливості ясності, гнучкості та участі всіх рівнів організації в процесі розробки (Al-Mayahi, Sa'ad, 2014), М. Нсох та низка співавторів зосередилися на відповідності політики безпеки інформаційних систем, у цьому документі досліджуються фактори, які впливають на поведінку відповідності в організаціях. Автори визначають організаційну культуру, обізнаність і навчання як ключові компоненти підвищення дотримання політики безпеки (Nsoh, Hargiss, Howard, 2015), Е. Аманква з колективом авторів розглядають концепції «культури дотримання політики інформаційної безпеки» та їх вплив на результати безпеки. Автори стверджують, що комплаєнс у безпековому середовищі – це не просто технічна проблема, а проблема, глибоко вкорінена в організаційній культурі (Amankwa, Loock, Kritzinger, 2021), Н. Масрек та інші вчені досліджують взаємозв'язок між ефективністю інформаційної безпеки та характером загроз безпеці. Автори підкреслюють, що мінливий ландшафт загроз безпеці вимагає постійного оновлення заходів і політик безпеки. Вони пропонують модель оцінки впливу різних загроз на ефективність існуючої політики безпеки (Masrek, Soesantari, Khan, Dermawan, 2021), М. Аббасі та М. Саадат пропонують механізм розробки надійних політик інформаційної безпеки, які забезпечують комплексний захист ІТ-систем. Автори наголошують на проактивному підході до розробки політики, включаючи передбачення загроз і регулярні оновлення для відповіді на нові технологічні виклики та нормативні зміни (Saadat, Abbasi, 2021). Наведені доробки підкреслюють важливість методичних підходів до комунікаційного забезпечення участі громадськості у прийнятті рішень та розробці демократичної політики безпеки. Вони обґрунтовують необхідність узагальнень стосовно того, як організаційна культура, міжнародні загрози і публічна комунікаційна поведінка влади відіграють вирішальну роль у політичній детермінації ефективності протидії безпековим викликам сьогодення.

Метою статті є виявлення чинників політичної детермінації публічних комунікацій в безпековій сфері. Завданням статті є розкриття потенціалу публічних комунікацій в рамках розв'язання ключових завдань національної безпеки.

Основний зміст. Спілкування з громадськістю під час криз безпеки відіграє ключову роль у підтриманні порядку, забезпеченні тривалого стану безпеки та наданні чіткої та точної інформації населенню. Це важливо для зменшення паніки, запобігання дезінформації та сприяння скоординованій реакції влади та громадян. Ефективність такого спілкування може суттєво вплинути на те, наскільки успішно громада поводиться в умовах кризи та відновлюється після неї. Класик комунікативної теорії Ю. Габермас слушно зазначав, що «публічна комунікація – це не просто передача інформації, а й сприяння спільному розумінню між комунікантами та громадськістю. Це вимагає оцінки суспільних цінностей, очікувань і проблем, що може значно вплинути на ефективність комунікаційних зусиль. Як стверджував Юрген Габермас, «публічний дискурс формується не лише змістом спілкування, але й умовами, за яких воно відбувається», підкреслюючи, що прозорість, інклюзивність і взаємна повага є вирішальними для змістовного діалогу» (Habermas, 1989, p. 56).

Під час криз національної безпеки (до них, зокрема, належать військова агресія, терористичні атаки, стихійні лиха, політичні заворушення тощо), демократична громадськість може звертається до публічної влади за оперативними поясненнями. Своєчасне публічне спілкування має вирішальне значення, оскільки громадяни мають запит на інформацію, оскільки прагнуть захистити себе та ефективно реагувати. Основна мета публічної кризової комунікації – надати чітку, стислу та надійну інформацію, яка дає можливість громадянам приймати обґрунтовані рішення. Це може включати відомості про маршрути евакуації, екстрені служби та вказівки, чого слід уникати. За висновками М. Буккі та Б. Тренча, «публічна діалогова комунікація – це процес взаємодії, переговорів і трансляції. Це не одностороння передача знань, а динамічна обмін, який формує як громадське сприйняття, так і наукові плани» (Bucchi, Trench, 2008, p. 145). З цієї точки зору важливість політично детермінованого діалогу та взаємодії для досягнення компромісів є основою успішної антикризової комунікації.

Відсутність своєчасної публічної комунікації між владою і громадою, або поширення неправдивої інформації, можуть призвести до плутанини, паніки та навіть фізичного ушкодження громадян. Наприклад, під час терористичних атак або ситуацій, пов'язаних із військовою небезпекою, належно організована публічна комунікація може врятувати життя, направляючи громадян у безпечне місце. І навпаки, затримки в спілкуванні можуть спричинити поширення неправдивих чуток і дезінформації, які своєю чергою, можуть посилити паніку й спричинити хаос. Шляхом уникнення подібних ситуацій є менеджмент діалогу з громадськістю. Відомий теоретик прагматичних засад політичної детермінації громадянського суспільства Джон Дьюї свого часу припускав, що громадський діалог має важливе значення для належного функціонування демократії, оскільки він заохочує обмін ідеями, критичні роздуми та прийняття обґрунтованих рішень. «Без спілкування немає колективного розуму чи громадської волі, а отже, і справжньої демократії», стверджував Дж. Дьюї (Dewey, 1927, p. 135). Політичний філософ слушно наголошував на основоположній ролі публічної комунікації в демократичному політичному процесі.

Підготовка ефективних публічних комунікаційних обмінів під час кризи як правило починається задовго до події. Уряди та інші державні інституції повинні мати заздалегідь розроблені антикризові комунікаційні плани, готові до виконання. Це включає в себе визначення конкретних речників, встановлення чітких каналів зв'язку та забезпечення того, щоб інфраструктура (наприклад, Інтернет, мобільні мережі) була достатньо надійними, аби відповідати збільшенню кризових запитів.

Під час кризових викликів для національної безпеки повідомлення мають бути чіткими, послідовними та регулярно оновлюватися. Публічна влада повинна уникати «жаргонізмів» або навпаки складної (наукової) мови, яка може заплутати громадськість. Інформація має бути представлена таким чином, щоб її можна було легко зрозуміти, з повторним акцентуванням ключових моментів, аби гарантувати збереження їх смислу. Узгодженість між різними комунікаційними платформами (наприклад, телебаченням, радіо, соціальними медіа тощо) також має вирішальне значення, оскільки суперечливі повідомлення можуть підірвати довіру до повідомлень влади. Як зазначив Т. ван Дейк, «публічна комунікація функціонує як міст між державою та громадянським суспільством, сприяючи активній громадянській позиції шляхом сприяння діалогу, надання інформації та сприяння публічним дебатам» (van Dijk, 2012, p. 152). Отже, публічні комунікаційні стратегії в рамках кризового реагування мають ключове значення для збільшення залучення громадськості та забезпечення поінформованості громадян. На цій основі вони будуть здатні до конструктивної поведінки. Означене, своєю чергою, забезпечить сприятливе політичне середовище для демократичних процесів інституалізації антикризової (безпекової) публічної комунікації.

За доби сучасних соціальних медіа кризова публічна комунікація розвинулася в напрямку охоплення не лише повідомлень за принципом «згори-донизу», але й через активну взаємодію з громадськістю. Інститути публічної влади повинні здійснювати моніторинг чуток та політично детермінованої неправдивої інформації в соціальних мережах і негайно реагувати на них. Це також дозволяє політичному менеджменту отримувати децентралізований зворотній зв'язок від громадськості в реальному часі, що надає можливість їм адаптувати свої стратегії відповідно до розвитку ситуації. Як зазначав М. Кастеллс, «у мережевому суспільстві комунікація стає все більш мультимодальною, включаючи комбінацію текстових, візуальних і звукових елементів. Комунікатори повинні орієнтуватися в цих нових медіа-ландшафтах, адаптуючи свої стратегії, щоб переконатися, що повідомлення резонують із дедалі більш фрагментованою та різноманітною аудиторією» (Castells, 2010, p. 111). Це підкреслює складність та еволюцію менеджменту антикризової публічної комунікації за доби цифрових технологій.

Розбудова довіри між владою та громадою має важливе значення для ефективної публічної комунікації в кризових ситуаціях. Дії центральних урядів та регіональних публічно-владних інституцій мають бути прозорими щодо наявної фактичної інформації та реального стану речей. Також необхідним є презентація конкретних заходів для врегулювання кризи та усунення її наслідків. Коли наявна

інформація мізерна або невизначена, краще це публічно визнати, ніж спекулювати чи приховувати деталі. Такі дії можуть підірвати довіру громадськості. Чесність і прозорість, навпаки, сприяють співпраці з громадськістю. Як зауважили М. Нісбет і Д. Шойфеле, «комунікація, особливо щодо суперечливих питань, повинна бути оформлена таким чином, щоб вона була змістовною та актуальною для культурні цінності та світогляд аудиторії, якщо цього не зробити, це може призвести до розмежування чи поляризації суспільства» (Nisbet, Scheufele, 2009, p. 1768). Означене висвітлює виняткове значення врахування політичної детермінації фреймінгу та культурного контексту в публічній комунікації щодо складних («незручних») тем.

Для того, аби охопити якомога ширшу аудиторію, кризова публічна комунікація повинна використовувати різноманітні платформи, включаючи традиційні ЗМІ (телебачення, радіо, газети), цифрові платформи (соціальні мережі, веб-сайти) та засоби прямого спілкування (екстрені сповіщення через SMS або додатки). Різні демографічні групи в отриманні інформації залежать від різних платформ, тому важливо адаптувати комунікаційну стратегію, щоб жодна група не залишилася непоінформованою. У зв'язку з цим як компонент комплексної політичної детермінації актуалізується правовий контекст публічної антикризової комунікації. Українська дослідниця А. Токарська вірно називає сучасну правову комунікацію засобом розв'язання конфліктного співбуття, який супроводжує процеси правороз уміння і правореалізації. Відтак вона творить психологічні основи для безпечної життєдіяльності людей. Однак поки що така морально-етична якість правової комунікації, як психолінгвістичне толерування стосунків – одне із найцінніших надбань загальносвітової і національної культури – залишається маловивченим соціальним явищем людських учинків (Токарська, 2012, с. 475).

Сучасні соціальні медіа відіграють подвійну роль під час реалізації державно-владних кампаній публічної комунікації в кризових умовах. З одного боку, це безцінний інструмент для швидкого поширення інформації та взаємодії з громадськістю. Під час кризових ситуацій в умовах російсько-української війни такі платформи, як Twitter, Facebook і Instagram, дозволяють публічній владі надавати безпекові оновлення та інструкції в реальному часі безпосередньо громадянам (Хнигічева, Новіков, Тимошенко, 2010). Крім того, ці платформи дозволяють інститутам влади й громадськості швидко й ефективно нейтралізувати дезінформацію. А. Токарська вірно ідентифікує толерантні підходи як здебільшого раціональні у пошуках згоди. Вони є виправданим інструментом для уникнення порушень норм законодавства щодо захисту прав і свобод громадян, для встановлення істини, для створення атмосфери оптимізму (за бажання встановити правду) і песимізму (як засобу протистояння агресії); для урівноваження позицій сторін, ступеня втручання у справу, для нівелювання демонстрації грубої сили і беззаконності; у поясненні загрози та запобіганні їй (Токарська, 2012, с. 477).

З іншого боку очевидно, що соціальні мережі та платформи, навпаки, можуть посилити поширення чуток і паніки. Як свідчить досвід російсько-української війни, неправдива інформація, або так звані «теорії змови», можуть швидко поширюватися, особливо якщо існує вакуум офіційної публічної інформації (див.: Компанцева, 2011). Це робить важливим для інститутів демократичної публічної влади активне відстежування активності та менеджерське залучення соціальних платформ. Вказане уможливлює ліквідацію впливу дезінформації, щойно вона з'являється, і надання регулярних надійних оновлень. Такі дії необхідні, оскільки, з погляду українських вчених О. Дзьобаня та О. Сосніна, глобалізація способу життя і джерел постачання інформації багато в чому вже дискредитували дії влади при визначенні національних інтересів і цінностей. Також йдеться про руйнування соціокультурної ідентичності громадян й зростання кількості факторів впливу так званої «м'якої сили». Це за собою більш жорсткі наслідки для життя народу і суверенітету країни, які ми сьогодні навіть не уявляємо (Дзьобань, Соснін, 2015, с. 25).

Незважаючи на всі зусилля, менеджмент демократичної публічної комунікації у кризовій ситуації пов'язаний із значними труднощами. Однією з головних політичних «пасток» є швидке поширення дезінформації, яке може відбуватися через соціальні мережі, з уст в уста чи навіть з боку респектабельних, «поважних» ЗМІ. Боротьба з ворожою дезінформацією вимагає проактивного підходу, коли інститути публічної влади й громадськості постійно відстежують і розглядають неправдиві повідомлення в «кризогенному» соціально-економічному середовищі. О. Дзьобань та О. Соснін вірно наголошують на втраті ціннісних орієнтирів в суспільстві при зростаючих ризиках відчуження суспільства від стабільної економічної діяльності в реальному секторі промисловості. Також вчені вірно говорять про посилення нерівності у доступі до новітніх знань, технологій тощо. Вказане веде до зростання соціальної й політичної напруженості в суспільстві (Дзьобань, Соснін, 2015, с. 25).

Ще одним викликом для безпекових владних мовників є комплексне охоплення всіх верств населення, особливо соціально вразливих груп. Ними є, як добре відомо, люди похилого віку, інваліди або ті, хто не має доступу до цифрових платформ. Традиційні медіа-канали, такі як радіо чи офлайнові громадські ініціативи, можуть відігравати важливу роль у включенні означених груп до вважливих процесів антикризового публічного інформування. О. Дзьобань та О. Соснін справедливо

вказують, що будучи системотворчим чинником життя суспільства, інформація активно впливає на стан політики, економіки, оборони, технічного прогресу, науки і культури, обслуговує інтереси особистості, суспільства і держави, стверджує життєві підвалини, сприяє стабільності суспільного і державного ладу, досягненню суспільної злагоди, зміцнення демократії, особистої безпеки, законності і правопорядку (Дзьобань, Соснін, 2015, с. 26).

Крім того, культурна та мовна різноманітність населення можуть створювати перешкоди для ефективного та відкритого публічного спілкування. Інститути демократичної публічної влади повинні гарантувати, що повідомлення про кризові події надаються зрозумілою мовою та враховують культурні особливості різних спільнот. Спілкування з громадськістю під час криз безпеки є критично важливим компонентом ефективного управління кризою. Це вимагає готовності політичного менеджменту до ухвалення рішень, прозорості та здатності доносити точну антикризову інформацію вчасно та доступно. Використання соціальних медіа, попри їх потужний потенціал, має бути контрольованим для запобігання поширенню дезінформації. На основі дотримання цих принципів, менеджмент публічно-владних комунікацій може забезпечити підтримання громадського порядку, мінімізувати шкоду та зміцнити довіру в умовах найважчих викликів національній безпеці.

Висновки. Таким чином, основними вимірами розкриття креативного потенціалу публічних комунікацій політико-менеджерського типу в безпековому полі є інституційна спроможність, тематична спрямованість та адресна досяжність цільових груп.

У першому вимірі в умовах сучасної України актуалізується питання експертно-аналітичного забезпечення публічних комунікацій з метою прорахунку ефекту від політико-комунікаційної діяльності. В рамках другого виміру лежить розробка стратегії опанування найбільш вигідних тем для просування безпекової стабільності. Третій вимір вимагає вірного налаштування технологічних цифрових засобів просування публічно-комунікаційного безпеку меседжу. Політико-менеджерські підходи для організації безпекових комунікацій передбачає узгодження позиції між основними політичними групами в суспільстві. Також на часі реалізація ініціативної політики основних гілок влади та компонентів громадянського суспільства тощо.

За умови координації державно-громадських публічних комунікацій з'явиться належна система протидії пропагандистським комунікаційним впливом російської федерації. Водночас публічні комунікації мають бути спрямовані на європеїзацію політико-комунікаційного середовища в Україні, в тому числі на основі нормативних обмежень та контролю за медіапростором. Перспективи подальшого розгляду теми даної статті є окреслення основних медіа-викликів національній безпеці сучасній Україні та вироблення стратегії їх політико-менеджерського упередження.

Sergeev V., Zagurska-Antoniuk V., Pashchenko V. Public communications and national security management: factors of political determination

Relevance. Nowadays, the public expression of political preferences of each audience requires careful attention in the face of threats to national security. The peculiarities of the management of public media security at the current stage involve the coordination of both the position of actors at the national level and the determination of the vector of the evolution of the media environment for an indefinite period in the future.

The purpose of the article is to identify the factors of political determination of public communications in the security sphere.

Research results. The effectiveness of public communication between government and society can significantly affect how successfully a community copes with a crisis and recovers from it. Successful public communication during a crisis often begins long before political events. Information should be presented in a way that is easy to understand, with key points re-emphasized to ensure retention.

Conclusions. In the conditions of modern Ukraine, the issue of expert-analytical provision of public communications with the aim of calculating the effect of political and communication activities is becoming actualized. Political-managerial approaches to the organization of security communications involve the agreement of the position between the main political groups in society. Public security communications should be aimed at the Europeanization of the political and communication environment in Ukraine.

Key words: political management, national security, public communications, media environment, digitalization, political institutions, security challenges.

Література:
1. Höne K., Eloff J. H. P. Information security policy – what do international information security standards say? Computers & Security. 21. 2002. no. 5. 402–409.
2. Imoniana J. O. Validity of information security policy models. Transinformação. 2004.16. no. 3. 263–274.
3. Al-Mayahi I. H., Mansoor S. Information Security Policy Development. Journal of Advanced Management Science. 2014. 2. no. 1. 135–139.
4. Nsoh M. W., Hargiss K., Howard C. Information Systems Security Policy Compliance. International Journal of Strategic Information Technology and Applications. 2015. 6. no. 2. 12–39.
5. Amankwa E., Loock, M., Kritzinger E. Information Security Policy Compliance Culture. International Journal of Technology and Human Interaction. 2021. 17. no. 4. 75–91.
6. Masrek M. N., Soesantari T., Khan A., Dermawan A. K. Examining the Relationship between Information Security Effectiveness and Information Security Threats. International Journal of Business and Society. 2021. 21. no. 3. 1203–14.
7. Saadat M., Abbasi M. U. Information Security Policy Development: the Mechanism to Ensure Security Over Information Technology Systems. Global International Relations Review. 2021. IV. no. III. 22–30.
8. Habermas J. The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society. MIT Press.1989. 344.
9. Bucchi M., Trench B. Handbook of Public Communication of Science and Technology. Routledge. NY. 2008. 368.
10. Dewey J. The Public and Its Problems. Swallow Press. 1927. 235.
11. van Dijk J. The Network Society. SAGE Publications. NY. 2012.456.
12. Castells M. Communication Power. Oxford University Press. L. 2010.240.
13. Nisbet M. C., Scheufele D. A. What's Next for Science Communication? Promising Directions and Lingering Distractions. American Journal of Botany. 2009. 96 (10). 1767–1778.
14. Токарська А. С. Толерантність комунікації як фактор психологічної безпеки. *Науковий* вісник Львівського державного університету внутрішніх справ. 2012. Серія психологічна. Вип. 2(2). 474–480.
15. Хнигічева А. М., Новіков О. М., Тимошенко А. О. Моделювання безпеки складних інформаційно-комунікаційних систем із використанням логіко-ймовірнісного методу. *Наукові* вісті Національного технічного університету України «Київський політехнічний інститут». 2010. № 6. 70–77.
16. Компанцева Л. Ф. Ефективна комунікація – новий тренд інститутів сектору безпеки. Сучасні інформаційні технології у сфері безпеки та оборони. 2011. № 1-2. 67–70.
17. Дзьобань О. П., Соснін О. В. Інформаційна безпека: нові виміри загроз, пов'язаних із інформаційно-комунікаційною діяльністю. Гуманітарний вісник Запорізької державної інженерної академії. 2015. Вип. 61. 24-34.

References:
1. Höne, K., Eloff J. H. P. (2002) Information security policy – what do international information security standards say? Computers & Security 21. no. 5. 402–409 [In English].
2. Imoniana, J. O. (2004) Validity of information security policy models. Transinformação. 16. no. 3. 263–274 [In English].
3. Al-Mayahi, I. H., Mansoor, S. (2014) Information Security Policy Development. Journal of Advanced Management Science. 2. no. 1. 135–139 [In English].
4. Nsoh, M. W., Hargiss K., and Howard C. (2015) Information Systems Security Policy Compliance. International Journal of Strategic Information Technology and Applications. 6. no. 2. 12–39 [In English].
5. Amankwa, E., Loock, M., Kritzinger, E. (2021) Information Security Policy Compliance Culture. International Journal of Technology and Human Interaction. 17. no. 4. 75–91 [In English].
6. Masrek, M. N., Soesantari, T., Khan, A., Dermawan, A. K. (2021) Examining the Relationship between Information Security Effectiveness and Information Security Threats. International Journal of Business and Society. 21. no. 3.1203–14 [In English].
7. Saadat, M., Abbasi M. U. (2021) Information Security Policy Development: the Mechanism to Ensure Security Over Information Technology Systems. Global International Relations Review, IV, no. III, 22–30 [In English].
8. Habermas, J. (1989). The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society. MIT Press.344 [In English].
9. Bucchi, M., & Trench, B. (2008). Handbook of Public Communication of Science and Technology. Routledge. NY. 368 [In English].
10. Dewey, J. (1927). The Public and Its Problems. Swallow Press.235 [In English].
11. van Dijk, J. (2012). The Network Society. SAGE Publications. NY.456 [In English].
12. Castells, M. (2010). Communication Power. Oxford University Press. L.240 [In English].

13. Nisbet, M. C., Scheufele, D. A. (2009). Whats Next for Science Communication? Promising Directions and Lingering Distractions. American Journal of Botany. 96(10). 1767–1778 [In English].
14. Tokarska, A. S. (2012) Tolerantnist komunikatsii yak faktor psykholohichnoi bezpeky. [Tolerance of communication as a factor of psychological safety]. Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav. Ceriia psykholohichna. Vyp. 2(2). 474–480 [In Ukrainian].
15. Khnyhicheva, A. M., Novikov, O. M., Tymoshenko, A. O. (2010) Modeliuvannia bezpeky skladnykh informatsiino-komunikatsiinykh system iz vykorystanniam lohiko-ymovirnisnoho metodu. [Security modeling of complex information and communication systems using the logical-probabilistic method]. Naukovi visti Natsionalnoho tekhnichnoho universytetu Ukrainy «Kyivskyi politekhnichnyi instytut». № 6. 70–77 [In Ukrainian].
16. Kompantseva L. F. Efektyvna komunikatsiia – novyi trend instytutiv sektoru bezpeky. [Effective communication is a new trend in security sector institutes]. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony. 2011. № 1-2. 67–70 [In Ukrainian].
17. Dzoban O. P., Sosnin O. V. (2015) Informatsiina bezpeka: novi vymiry zahroz, poviazanykh iz informatsiino-komunikatsiinoiu diialnistiu. [Information security: new dimensions of threats related to information and communication activities]. Humanitarnyi visnyk Zaporizkoi derzhavnoi inzhenernoi akademii. Vyp. 61. 24–34 [In Ukrainian].

Стаття надійшла до редакції 21.10.2024
Стаття рекомендована до друку 12.11.2024