УДК 32.019.51

Р. Ф. Черниш, О. В. Пірог, П. Ю. Грушевська

ЗАГРОЗИ ДЕРЖАВНІЙ БЕЗПЕЦІ УКРАЇНИ В ІНФОРМАЦІЙНІЙ СФЕРІ У РЕАЛІЯХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Сформульовано поняття «загрози державній безпеці України в інформаційній сфері», виокремлено зазначені загрози у реаліях російсько-української війни. Констатовано, що система забезпечення інформаційної безпеки як компонент системи забезпечення державної безпеки загалом характеризується відповідними силами та засобами. Разом з тим акцентовано увагу на основних напрямах діяльності державних органів (зокрема правоохоронних та спеціальних) для ефективного забезпечення державної безпеки України в інформаційній сфері.

Ключові слова: *державна безпека в інформаційній сфері, мережа «Інтернет», кібербезпека, кіберзагрози, національна безпека.*

Постановка проблеми. Для забезпечення демократичного розвитку України, підтримання євроінтеграційного курсу та збереження цілісності в умовах російсько-української війни необхідно активізувати масштабні процеси реформування. Це особливо стосується організації та функціонування національного сектору безпеки і оборони, демократичної трансформації ключових громадянських інститутів та впровадження сучасних принципів державного управління.

Із посиленням використання інформаційних технологій в умовах російсько-української війни контроль над інформаційними потоками перетворюється на одну з головних цілей протистояння. За таких обставин боротьба розгортається навколо впливу на думку громадськості. Протистояння в інформаційній сфері логічно призвело до початку так званої «гонки інформаційних озброєнь». Із розвитком інформаційних технологій та їхнім активним застосуванням у реаліях російсько-української війни питання забезпечення державної безпеки України в інформаційній сфері є вкрай актуальним. Наша держава має системно вдосконалювати концептуальні заходи інформаційної безпеки, адже інформаційні загрози національним інтересам значно динамічніші порівняно, наприклад, з економічними чи політичними.

Аналіз останніх досліджень і публікацій. Окреслена проблематика досліджувалася вітчизняними безпекознавцями, юристами, управлінцями, зокрема: С. Бєлаєм, А. Благодарним, В. Горбуліним, О. Довганем, М. Дзевелюком, І. Дороніним, В. Крутовим, В. Ліпканом, А. Марущаком, В. Петриком, В. Пилипчуком, В. Полевим, М. Присяжнюком, А. Тарасюком, Т. Ткачуком та багатьма іншими ученими.

Зазначені автори зробили вагомий внесок у розвиток правової та організаційної регламентації правовідносин в інформаційній сфері. Проте, незважаючи на досягнення українських і зарубіжних науковців, з огляду на надшвидкі темпи інформатизації, зокрема і поточного етапу – діджиталізації, значне коло питань порушеної проблематики дотепер залишається недостатньо дослідженим та потребує наукового обґрунтування з метою подальшої імплементації у практичну складову.

Метою статті є формулювання поняття «загрози державній безпеці України в інформаційній сфері», виокремлення зазначених загроз у реаліях російсько-української війни, розкриття основних заходів, спрямованих на протидію останнім, а також визначення основних напрямів діяльності державних органів (зокрема правоохоронних та спеціальних) з метою ефективного забезпечення державної безпеки України в інформаційній сфері.

Виклад основного матеріалу. Кожна країна на шляху свого розвитку стає перед викликом у пошуку нових напрямів та засобів протидії інформаційним загрозам. У контексті забезпечення інформаційної безпеки України потрібно враховувати, що держава входить до переліку країн, які найбільше піддаються інформаційним маніпуляціям з боку країни-агресора [14].

На думку авторів статті, певним резервом у цій протидії є вдосконалення організації роботи державних органів (зокрема правоохоронних та спеціальних) із забезпечення своєчасної цільової нейтралізації зазначених загроз (бажано на стадії підготовки їх реалізації або на початковому етапі).

За свідченням американського сенатора Джорджа Макговерна, «…один із способів завдати удару по нації – це обмежити потік інформації, обірвавши контакти між її споживачами, спорудити інформаційну стіну. Так в інтернаціональний лексикон увійшов новий термін – "інформаційний суверенітет". Водночас спроби окремої нації перекрити потік відомостей "ззовні" можуть сприяти не розвитку, а підриву її економіки. Крім цього, кожний технологічний зрив відкриває націю для вторгнення "ззовні"» [4].

У сучасних умовах «інформаційний потенціал» стає одним із найважливіших чинників

забезпечення національної безпеки поряд із «економічним потенціалом», «військовим потенціалом» тощо. Рівень розвитку й безпека інформаційного середовища активно впливають на стан політичної, економічної та інших складових національної безпеки України [10, с. 26].

Стрімкий розвиток глобального інформаційного простору й застосування інформаційно-комунікаційних технологій у всіх сферах життєдіяльності сприяють розширенню інформаційного суспільства в Україні та зумовлюють важливість проблем інформаційної безпеки. У таких умовах одним із головних завдань держави є створення комплексної системи оцінювання загроз інформаційного характеру та відповідного реагування з метою забезпечення державної безпеки в інформаційній сфері [11]. Для унормування зазначеної вище діяльності і законодавчого закріплення того, що забезпечення інформаційної безпеки України є однією з найважливіших функцій держави, 28 грудня 2021 р. було затверджено Стратегію інформаційної безпеки. У цьому документі визначено актуальні виклики і загрози національній безпеці України в інформаційній сфері, стратегічні цілі й завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних. Її метою є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами й заходами соціальної і політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина [12].

При цьому, як вважають автори, у такій комплексній системі суттєву роль повинні відігравати національні спецслужби з їхнім інформаційно-аналітичним потенціалом.

Загрози державній безпеці України в інформаційній сфері можна сформулювати як систему умов та чинників, що призводять чи можуть призвести до завдання шкоди важливим державним, суспільним й особистісним інтересам через можливий деструктивний вплив інформації на свідомість (підсвідомість) та поведінку громадян, а також через технічний вплив на інформаційні ресурси й інфраструктуру.

Система загроз державній безпеці України в інформаційній сфері може охоплювати такі категорії:

– загрози безпеці інформації та відповідній інфраструктурі, які містять ризики, пов'язані зі зловживанням, несанкціонованим доступом, пошкодженням або втратою інформації, а також атаками на інформаційну інфраструктуру (кібератаки або комп'ютерні віруси);

– загрози безпеці суб'єктів інформаційного напряму та соціальних зв'язків між ними від дій (впливів) інформаційного характеру, які містять маніпулювання інформацією з метою впливу на свідомість і поведінку громадян, формування потрібного враження та маніпуляції соціальними зв'язками з метою впливу на суспільний порядок [7, 9];

– загрози актуальному порядку реалізації прав та інтересів суб'єктів інформаційного напряму, які містять дії, спрямовані на порушення законів, прав і свобод, зокрема у сфері інформації (поширення дезінформації, дискредитація, перешкоди у доступі до інформації або обмеження свободи слова).

Як вважає У. Ільницька, до загроз національній безпеці України в інформаційній сфері варто зарахувати:

1) можливе обмеження свободи слова та вільного доступу громадян до інформації;

2) перекручення, викривлення, блокування, приховування та суб'єктивне відображення інформації;

3) незаконне поширення інформації;

4) поширення недостовірних відкритих даних;

5) інформаційне завоювання інших країн та руйнівне інформаційне вторгнення у державний інформаційний простір, коли держави з більшим інформаційним потенціалом використовують можливість посилення свого впливу через засоби масової інформації (ЗМІ) на населення і громадськість країни з меншими можливостями в інформаційній сфері;

6) створення й функціонування неконтрольованих інформаційних потоків у державному інформаційному просторі;

7) поширення через ЗМІ культу насильства, жорстокості;

8) уповільнене входження України в інформаційний простір світового масштабу;

9) нерозважливість національної інформаційної політики та брак важливої інфраструктури в інформаційній площині;

10) поширення дезінформації через Інтернет [6, с. 30].

Останнє положення дещо звужує можливості поширення дезінформації [16], оскільки із зазначеною метою можуть бути задіяні й інші джерела поширення (не лише мережа «Інтернет» чи соціальні мережі [1]).

Також, на думку авторів, до вказаних загроз доцільно віднести й неоперативність реагування державних органів (зокрема правоохоронних та спеціальних) на виклики і загрози державній безпеці в інформаційній сфері, яка прискорює негативні процеси та призводить до їх збільшення. Потрібно наголосити, що ця риса є характерною для більшості країн з перехідною економікою [3].

Питання забезпечення державних інтересів і державної безпеки у сфері отримання й використання інформації наразі є доволі актуальним. Інформаційна безпека забезпечується здійсненням єдиної державної політики в царині національної інформаційної безпеки, системою економічних, політичних та організаційних заходів, адекватних наявним і потенційним загрозам національним інтересам (особисті, суспільні й державні) в інформаційній сфері.

Для забезпечення й підтримання необхідного рівня державної безпеки в інформаційному просторі розробляється та впроваджується система юридичних норм, які регулюють відносини в інформаційній сфері. Вона передбачає визначення ключових напрямів діяльності органів державного управління, створення або реорганізацію органів і сил, що забезпечують інформаційну безпеку, а також формування механізму контролю за їхньою діяльністю.

Заслуговує на увагу думка В. Ліпкана, який зазначає, що процес формування ключових елементів системи забезпечення інформаційної безпеки ще не завершений. Урахування загальної несформованості системи забезпечення національної безпеки, невизначеності державної інформаційної політики є доцільним у поданому контексті. До того ж недосконаліть нормативно-правового регулювання досліджуваних процесів негативно впливає на якість державного управління в означеній сфері [8].

Отже, наведені вище прогалини у нормативно-правовій базі, що регулює правові відносини в інформаційній царині, становлять значні перешкоди для якісних змін у зазначеній сфері суспільних відносин. Недостатня чіткість та взаємопов'язаність заходів і теоретичних розробок із забезпечення інформаційної безпеки країни ускладнюють повну реалізацію державними органами їхнього обов'язку забезпечувати інформаційну безпеку як невід'ємну складову національної безпеки. Розроблення і реалізація ефективної системи протидії протиправним діянням, які містять ознаки злочинів в інформаційній сфері, потребують розвитку дієвих норм національного законодавства та відомчих нормативно-правових актів сектору безпеки і оборони.

Система забезпечення інформаційної безпеки як компонент системи забезпечення державної безпеки загалом характеризується відповідними силами та засобами. У цьому контексті *сили* можна розглядати як суб'єктний склад системи забезпечення інформаційної безпеки, тобто люди, організації, структури, спеціальні органи, які здійснюють захист інформації; *засоби* – як технології й різноманітні технічні, програмні, лінгвістичні, юридичні та організаційні ресурси. Вони містять телекомунікаційні канали, які використовуються для збирання, формування, аналізу, передавання або отримання інформаційних даних, пов'язаних із державною безпекою в інформаційній сфері, а також заходи, спрямовані на посилення зазначеної безпеки.

У сучасному інформаційному суспільстві кожен суб'єкт відіграє важливу роль у забезпеченні державної безпеки в інформаційній сфері. Завдяки синергетичним особливостям інформаційної безпеки будь-який із суб'єктів може одночасно бути об'єктом інформаційної безпеки та джерелом можливих загроз або каналом їх поширення. У зв'язку з цим успішність забезпечення інформаційної безпеки залежить не лише від спеціальних державних структур, але й від кожного суб'єкта інформаційних відносин, який повинен самозахищатися в інформаційній сфері. Водночас держава виступає особливим суб'єктом забезпечення інформаційної безпеки, оскільки має можливості прямої управлінської дії та використовує юридичні засоби для регулювання інформаційних відносин. Крім того, варто враховувати, що держава виконує особливу роль серед суб'єктів забезпечення інформаційної безпеки, адже лише вона має широкий потенціал, який містить не лише економічні, політичні та ідеологічні засоби опосередкованого впливу, але й пряму управлінську дію. Це означає, що держава може використовувати юридичні засоби для регулювання інформаційних відносин і впливати безпосередньо на забезпечення інформаційної безпеки [13].

Держава як суб'єкт забезпечення інформаційної безпеки несе підвищену відповідальність у забезпеченні безпеки в інформаційній сфері [2, с. 152]. Проте варто зауважити, що в сучасних умовах розвитку інформаційного суспільства кожен суб'єкт інформаційних відносин (громадяни, організації чи підприємства) самостійно відповідає за свою безпеку (зокрема в інформаційній сфері). Отже, спільна взаємодія держави й усіх суб'єктів інформаційних відносин у напрямі забезпечення зазначеної вище безпеки є ключовим чинником успіху в цій сфері.

Аналіз класифікацій загроз державній безпеці України в інформаційній сфері свідчить про брак єдиного усталеного підходу до виокремлення їхніх окремих видів, оскільки кожен із дослідників

окресленої проблематики застосовує відповідні суб'єктивні критерії, тому такий перелік доволі складно зробити уніфікованим та вичерпним. Автори погоджуються з думкою Р. Хмелевського, що «…навіть розгорнуті переліки загроз не можуть бути вичерпними та стабільними. Це пояснюється тим, що джерела загроз можуть бути різноманітними: людина, технічні засоби, моделі, алгоритми, програмні та технологічні схеми обробки, зовнішнє оточення тощо» [15].

У контексті російсько-української війни, за умови динамічної зміни оперативної обстановки, до *актуальних загроз забезпеченню державної безпеки України в інформаційній сфері* можна віднести такі:

– створення атмосфери бездуховності в українському суспільстві, спрямованої проти культури та історичної спадщини;

– маніпулювання громадською думкою й політичною орієнтацією населення з метою створення політичного напруження та хаосу;

– дестабілізація політичних відносин, конфлікти та недовіра між партіями, об'єднаннями й рухами;

– провокування соціальних, політичних, етнічних і релігійних зіткнень;

– недостатнє інформаційне забезпечення органів влади та управління, що може призвести до зниження ефективності їхньої роботи й помилкових управлінських рішень;

– дезінформація та дискредитація дій державних органів влади з метою зниження їхнього авторитету;

– ініціювання протестів, страйків, інших актів громадянської непокори;

– підрив авторитету держави на міжнародній арені та перешкоджання співпраці з іншими країнами;

– створення й посилення опозиційних організацій та рухів, включно з ультраправими та ультралівими організаціями;

– дискредитація національної самобутності та історичних фактів;

– зміна системи світоглядних цінностей і настанов;

– зменшення значення досягнень у науці, техніці, інших галузях, перекручування фактів з метою негативного впливу на рішення вищих органів державної влади;

– створення передумов для економічної, духовної або військової поразки та зниження бажання населення боротися й перемагати;

– пропагування агресором власного способу життя як прикладу для інших народів;

– підрив морального духу населення через «втому від війни», політичні скандали та зневіру в перемозі, що може призвести до зниження обороноздатності й бойового потенціалу Збройних Сил України;

– завдання шкоди критичній інфраструктурі, включно з машинно-технічними засобами, програмним забезпеченням та системами захисту від несанкціонованого доступу до інформації тощо.

У сучасних умовах можливо сформулювати такі *групи основних заходів, спрямованих на протидію традиційним і новим загрозам державній безпеці України в інформаційній сфері та усунення чинників, що призводять до їхнього виникнення*:

а) політико-дипломатичні заходи – політичні та дипломатичні зусилля для зміцнення міжнародної співпраці, укладення міжнародних договорів й угод, побудови союзів і партнерств з іншими країнами з метою забезпечення колективної безпеки в інформаційній сфері;

б) військові заходи – посилення обороноздатності країни, розвиток військової інфраструктури, модернізація військових сил та здійснення військових операцій для захисту державної безпеки України в інформаційній сфері;

в) правові (законодавчі) заходи – розроблення та ухвалення нормативно-правових актів з метою регулювання сфери інформаційної безпеки, включно з боротьбою з тероризмом, кіберзагрозами, кіберзлочинністю тощо;

г) інформаційно-психологічні заходи – проведення інформаційних кампаній, відповідний психологічний вплив на громадськість, формування позитивного іміджу країни, боротьба з дезінформацією та пропагандою, формування у населення «культури споживання інформації»;

д) економічні заходи – розвиток економічних секторів, залучення інвестицій, забезпечення економічної стабільності, боротьба з фінансовими загрозами в інформаційній сфері;

е) науково-технологічні заходи – наукові дослідження, розроблення технологій та інновацій, які спрямовані на виявлення, прогнозування й протидію новим загрозам в інформаційній сфері, включно з кібершпигунством та кібератаками на об'єкти критичної інфраструктури;

ж) організаційні (адміністративні й процедурні) заходи – розроблення та впровадження ефективних організаційних структур, процедур і політик, які сприяють забезпеченню інформаційної безпеки (може містити створення спеціалізованих відділів з інформаційної безпеки, визначення процедур контролю доступу до інформації, регулярну перевірку й оновлення систем безпеки тощо);

и) фізичні заходи – фізичний захист інформаційної інфраструктури, об'єктів зберігання даних (передусім об'єктів критичної інфраструктури), обмеження фізичного доступу до конфіденційної інформації та встановлення систем відеоспостереження й контролю;

к) технічні (апаратні й програмні) заходи – застосування спеціального апаратного і програмного забезпечення для захисту інформації, шифрування даних, виявлення й відновлення після інцидентів, резервне копіювання даних [5] та інші технічні засоби для забезпечення державної безпеки в інформаційній сфері.

Наведені заходи сприяють створенню комплексної системи забезпечення інформаційної безпеки, яка враховує різноманітні загрози та використовує різні методи для їхнього попередження й локалізації.

Висновки

З огляду на викладене вище з розвитком інформаційних технологій та їхнім активним застосуванням в умовах російсько-української війни питання забезпечення державної безпеки України в інформаційній сфері є доволі актуальним. За таких обставин наша держава має системно вдосконалювати концептуальні заходи інформаційної безпеки, оскільки інформаційні загрози національним інтересам значно динамічніші порівняно з економічними чи політичними. Водночас необхідно враховувати стрімку появу нових технологій, механізмів і засобів здійснення деструктивного інформаційного впливу на суспільство.

З урахуванням викликів сьогодення державні органи (також правоохоронні та спеціальні) повинні зосереджувати зусилля на напрямах аналітичної роботи, відстеження тенденцій, взаємозалежностей і явищ, що можуть становити загрозу державній безпеці (зокрема в інформаційній сфері).

З метою забезпечення державної безпеки України в інформаційній сфері, на думку авторів, основні зусилля державних органів (також правоохоронних та спеціальних) повинні бути спрямовані на такі ключові аспекти:

– активне реагування на загрози: удосконалення механізмів реагування на кібератаки та інші загрози у режимі реального часу;

– кібербезпека: забезпечення захисту комп'ютерних систем, мереж й інформації від кібератак, включно із застосуванням ефективних методів шифрування, виявлення та запобігання інцидентам, а також навчанням персоналу стандартам кібербезпеки;

– інформаційна розвідка: проведення аналізу та моніторингу інформаційного простору для виявлення потенційних загроз і ризиків; розвиток інформаційних систем для збирання та оброблення даних, виявлення дезінформації й маніпулятивної інформації;

– законодавчий та регуляторний фреймворк: оптимізація відомчої бази нормативно-правових актів, що регулюють діяльність в інформаційній сфері;

– міжнародне співробітництво: розвиток механізмів співпраці зі спецслужбами іноземних країн та міжнародними організаціями для обміну інформацією про загрози, розроблення спільних стратегій і стандартів, а також координації заходів забезпечення інформаційної безпеки;

– удосконалення системи навчання й підвищення кваліфікації: оновлення освітніх програм, навчальних планів та навчально-методичного забезпечення для підготовки й підвищення кваліфікації співробітників Служби безпеки України з питань забезпечення інформаційної безпеки;

– едукація та свідомість: підвищення рівня критичного мислення й обізнаності населення та представників органів державної влади і місцевого самоврядування з питань кібербезпеки, захисту персональних даних в інформаційній сфері (зокрема й шляхом їх навчання базовим принципам кібербезпеки та безпечного користування інформаційними технологіями).

Перелік джерел посилання

1. Formation and application of communication strategies through social networks: Legal and Organizational Aspects / Roman F. Chernysh et al. *International Journal of Management*. 2020. Vol. 11. No. 6. P. 476–488. DOI: https://doi.org/10.34218/IJM.11.6.2020.041.

2. Formation and formulation of state policy to ensure national security: Theoretical and Legal Aspects / M. Shilin et al. *Amazonia Investiga*. 2022. Vol. 11. No. 57. P. 152–161. DOI: https://doi.org/10.34069/AI/2022.57.08.16.

3. Investment Security Management in Transition Economies: Legal and Organizational Aspects / T. O. Vlasenko et al. *International Journal of Economics and Business Administration*. 2020. Vol. 8. No. 2. P. 200–209.

4. Дзевелюк М. В. Сервісна держава як функціональна модель сучасної держави. *Актуальні проблеми держави і права*. 2017. Вип. 78. С. 60–67.

5. Довгань О., Тарасюк А., Ткачук Т. Кібербезпека «суспільства знань» : монографія. Київ; Одеса : Фенікс, 2021. 176 с.

6. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політичні науки*. 2016. № 2-1. С. 27–32.

7. Інформаційно-психологічне протиборство : підручник. 2-ге вид., перероб. та доп. / В. М. Петрик та ін. ; за заг. ред. В. В. Бедь, В. М. Петрика. Київ : ВІПОЛ, 2018. 386 с.

8. Ліпкан В. А., Макименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. Київ : КНТ, 2006. 280 с.

9. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал*. 2009. URL: http://surl.li/nfhlyp (дата звернення: 10.05.2024).

10. Присяжнюк М. М., Климчук О. О., Тиква В. Л. Курс лекцій з навчальної дисципліни «Інформаційна безпека держави». Київ : Центр навчальних, наукових та періодичних видань, 2014. 244 с.

11. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України : рішення Ради національної безпеки і оборони України від 28 квітня 2014 р., уведено в дію Указом Президента України від 01.05.2014 р. № 449/2014. URL: http://surl.li/xzsbmu (дата звернення: 10.05.2024).

12. Про Стратегію інформаційної безпеки : рішення Ради національної безпеки і оборони України від 15 жовтня 2021 р., уведено в дію Указом Президента України від 28.12.2021 р. № 685/2021. URL: http://surl.li/uelqso (дата звернення: 10.05.2024).

13. Тихомиров О. О. Права людини: інформаційний вимір : монографія. Одеса : Юридика, 2023. 304 с.

14. Україна серйозно вражена інформаційними маніпуляціями РФ – дослідження Facebook. URL: http://surl.li/yjwjxf (дата звернення: 10.05.2024).

15. Хмелевський Р. М. Дослідження оцінки загроз інформаційній безпеці об’єктів інформаційної діяльності. *Сучасний захист інформації*. 2016. № 4. С. 65–70.

16. Черниш Р. Ф. Правовий досвід країн Європейського Союзу у сфері протидії поширенню фейкової інформації. *Підприємництво, господарство і право*. 2019. № 10. С. 123–128. URL: http://pgp-journal.kiev.ua/archive/ 2019/10/22.pdf (дата звернення: 10.05.2024).

Стаття надійшла до редакції 18.10.2024 р.

UDC 32.019.51

R. Chernysh, O. Piroh, P. Hrushevska

THREATS TO THE STATE SECURITY OF UKRAINE IN THE INFORMATION SPHERE IN THE REALITIES OF THE RUSSIAN-UKRAINIAN WAR

The article formulates the concept of "threats to the state security of Ukraine in the information sphere". They can be formulated as a system of conditions and factors that lead or may lead to damage to important state, public and personal interests due to the possible destructive impact of information on the

consciousness (subconsciousness) and behavior of citizens, as well as due to the technical impact on information resources and infrastructure.

It was established that the information security system as a component of the state security system is generally characterized by appropriate forces and means.

In this context, forces can be considered as the subject composition of the information security system, i.e. people, organizations, structures, special bodies that protect information; means – as technologies and various technical, software, linguistic, legal and organizational resources. They include telecommunications channels used to collect, form, analyze, transmit or receive information data related to state security in the information sphere, as well as measures aimed at strengthening said security.

At the same time, attention is focused on the main areas of activity of state bodies (including law enforcement and special) to effectively ensure the state security of Ukraine in the information sphere.

Keywords: *state security in the information sphere, Internet network, cyber security, cyber threats, national security.*

Черниш Роман Федорович – кандидат юридичних наук, доцент, експерт у сфері інформаційної безпеки
https://orcid.org/0000-0003-4176-7569

Пірог Олександр Вікторович – кандидат технічних наук, доцент кафедри комп'ютерної інженерії і кібербезпеки Державного університету «Житомирська політехніка»
https://orcid.org/0000-0003-4176-7569

Грушевська Поліна Юріївна – здобувачка вищої освіти другого (магістерського) рівня Поліського національного університету
https://orcid.org/0009-0009-5891-6656