Вісник Львівського університету. Серія філос.-політолог. студії. 2024. Випуск 55, с. 231–239
Visnyk of the Lviv University. Series Philos.-Political Studies. Issue 55, p. 231–239

ПОЛІТИЧНІ НАУКИ

УДК 341.232
DOI https://doi.org/10.30970/PPS.2024.55.28

СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ШИРОКОМАСШТАБНОГО ВТОРГНЕННЯ РОСІЙСЬКИХ ВІЙСЬК В УКРАЇНУ

Ольга Анісімович-Шевчук
Національний університет «Львівська політехніка»,
Інститут гуманітарних та соціальних наук,
кафедра політології та міжнародних відносин
вул. Митрополита Андрея, 5, 79013, м. Львів, Україна
https://orcid.org/0000-0003-0428-6459

Світлана Матвієнків
Прикарпатський національний університет імені Василя Стефаника
факультет історії, політології і міжнародних відносин,
кафедра політичних інститутів та процесів
вул. Шевченка, 57, 76018, м. Івано-Франківськ, Україна
https://orcid.org/0000-0002-7719-7791

Акцентується увага на захисті інформаційно-комунікаційного простору держави в умовах сьогоднішньої російсько-української війни. Наголошується на важливості забезпечення безпеки інформації, оперативному реагування на інформаційно-комунікативні загрози та небезпеки. Мета дослідження – здійснити аналіз сформованої системи забезпечення інформаційної безпеки України після широкомасштабного вторгнення російських військ в Україну. Для цього використано системний аналіз, метод кейс-стаді, проаналізовано нормативно-правові та наукові джерела, урядові сайти тощо.

У статті зазначається, що проблема функціонування сучасного національного інформаційного простору як сфери інформаційних обмінів, складається з розгалуженої системи структур. Національний інформаційний простір включає інформаційно-телекомунікаційну інфраструктуру та ресурси, які забезпечують взаємодію громадян, держави, організацій, сприяючи задоволенню їх інформаційно-комунікаційних потреб на території України, забезпечуючи національний інформаційний суверенітет. Наголошено на важливості реалізація єдиної інформаційної політики, яка є пріоритетним завданням національної безпеки держави. Відзначено, що за роки незалежності в Україні сформовано законодавчі основи системи забезпечення інформаційної безпеки. Національні інформаційні ресурси мають відомчий, міжвідомчий характер та охоплюють інформаційні ресурси органів державної влади і управління, місцевого і регіонального самоврядування; державної статистики, архівного, бібліотечного та музейного фондів тощо. При цьому обумовлюється, що право власності на інформаційні ресурси забезпечує національний суверенітет держави. Наголошується, що політика інформаційної безпеки України реалізується системою інститутів публічної влади та інститутами громадянського суспільства. Наводяться приклади співпраці у сфері забезпечення безпеки інформаційно-комунікаційного простору України.

Ключові слова: інформаційна безпека, інформація, комунікація, війна, інформаційно-комунікаційний простір, інформаційно-комунікаційна інфраструктура та ресурси, органи державної влади, національна безпека.

Сьогодні практично неможливо знайти сферу, яка б не зазнала впливу інформаційно-комунікативних технологій: політика, право, економіка, медицина, освіта, культура, релігія, сфера послуг і розваги тощо. «Інформаційний бум у буквальному розумінні охопив суспільство загалом і окрему особистість зокрема, змінив їх спосіб життя, сформував нові виклики і загрози» [6]. Гостроти проблематиці додає також те, що інформаційна складова стала безумовним об'єктом інформаційно-технічних та інформаційно-психологічних впливів, дезінформування в умовах сьогоднішньої російсько-української війни. А потреба у безпечних засобах накопичення, систематизації, зберіганні, пошуку, передачі інформації постійно зростає.

Сьогодні Україна перебуває в складній ситуації, зумовленій широкомасштабним вторгненням російських військ на територію нашої держави, веденням конвенціонально-гібридної війни. Важливим аспектом постає необхідність забезпечення безпеки інформації, оперативного реагування на інформаційно-комунікативні загрози та небезпеки. Низка фахівців до 24 лютого 2022 року вважали, що в нашій державі відсутня належна система інформаційної безпеки, яка б могла забезпечити виявлення, аналіз інформаційних загроз національній безпеці Україні, а також здійснення протидії цим загрозам. Однак вже більше двох років активних бойових дій та ведення інформаційних, економічних та іншого гібридного характеру дій з боку ворога, демонструє належний рівень захисту вітчизняного інформаційного простору, спроможність протидії інформаційно-кібернетичним загрозам і небезпекам.

Метою дослідження є здійснити аналіз забезпечення інформаційної безпеки України в умовах сьогоднішньої російсько-української війни. Для цього використано системний аналіз, метод кейс-стаді, проведено аналіз нормативно-правових та наукових джерел.

Проблемам функціонування сучасного національного інформаційного простору як сфери інформаційних обмінів, що складається з розгалуженої системи структур та мають забезпечувати створення нової інформації, зберігання та захист наявної, а також організацію її використання, у своїх дослідження неодноразово присвячували увагу українські науковці: В. Бебик, І. Боднар, М. Гаврильців, К. Захаренко, Т. Мужанова, Г. Почепцов, В. Савіцький, С. Чукут та Т. Джига, О. Юдін та В. Богуш та багато інших. Автори відзначають, що національний інформаційний простір – це сфера діяльності, що включає інформаційну і телекомунікаційну інфраструктуру та ресурси, які забезпечують взаємодію громадян, держави, організацій та сприяють задоволенню їх інформаційно-комунікаційних потреб на території України та мали б гарантувати національний інформаційний суверенітет.

Варто відзначити, що за роки незалежності в Україні сформовано законодавчі основи системи забезпечення інформаційної безпеки. У Конституції України, прийнятій 28 червня 1996 року, зазначено про важливість забезпечення інформаційної безпеки України, яка є однією з найважливіших функцій держави, гарантує кожному громадянину права в інформаційній сфері: свободу думки й слова, свободу вираження поглядів і переконань, право вільно збирати, зберігати, використовувати й поширювати інформацію тощо [10]. Концептуальні засади інформаційної безпеки як складової національної безпеки викладені також в низці нормативно-правових актів, наприклад, Законі України «Про національну безпеку України» (2018), Указі Президента «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» (2017), Указі Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» (2015), Указі Президента України від 15 березня 2016 року «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України»

(2016) тощо. Практично не задовго до широкомасштабного вторгнення російських військ в Україну прийнято «Стратегію інформаційної безпеки» (Указ Президента України від 28 грудня 2021 року), реалізація якої розрахована на період до 2025 року [16], а 20 березня 2023 року Кабінет Міністрів України видав розпорядження про заходи з реалізації «Стратегії інформаційної безпеки на період до 2025 року» [14].

Детально питання функціонування елементів інформаційного простору, інформаційних ресурсів відображені в низці Законів України «Про інформацію» (1992), «Про друковані засоби масової інформації (пресу) в Україні» (1992), «Про телебачення і радіомовлення» (1993), «Про доступ до публічної інформації» (2011), «Про Суспільне телебачення і радіомовлення України» (2014), «Про Національну систему конфіденційного зв'язку» (2002), «Про захист персональних даних» (2010), «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» (2007) тощо. Загалом в нормативно-правових та наукових джерелах представлено декілька підходів до розуміння сутності інформаційних ресурсів. Зокрема, під інформаційними ресурсами мають на увазі сукупність даних, організованих для отримання достовірної інформації в різних сферах знань і практичної діяльності, або особливий вид ресурсів, що ґрунтуються на ідеях і знаннях, нагромаджених у результаті науково-технічної діяльності людей і подані у формі, придатній для збирання, реалізації та відтворення. Визначення поняття інформаційних ресурсів наведено також в Законах «Про науково-технічну інформацію» (1993), «Про національну програму інформатизації» (1998).

Загалом система національних інформаційних ресурсів має відомчий та міжвідомчий характер та охоплює інформаційні ресурси: органів державної влади і управління, місцевого і регіонального самоврядування; державної статистики (державний, обласний, районний рівні); архівного, бібліотечного та музейного фондів; фіскальної служби, правоохоронних і силових структур; науково-технічної інформації; матеріального виробництва тощо. А право власності на інформаційні ресурси забезпечують національний суверенітет держави, у структурі якого важливе місце посідає саме інформаційний суверенітет. Тобто інформаційний суверенітет – це право держави на формування і здійснення національної інформаційної політики відповідно до нормативно-правових актів держави, міжнародного права. Пов'язана інформаційна політика з діяльністю засобів масової інформації та системами комунікації, інформаційними агентствами, бібліотеками, архівами, а також виробленням та використанням новітніх інформаційно-комунікаційних технологій та упровадженням електронного урядування, наприклад, Е-уряд, Е-банкінг, електронним документообігом тощо.

Враховуючи пряму військову агресію з боку рф в Україну, активне поширення державою-агресором дезінформації, викривленням відомостей, а також «з метою донесення правди про війну, забезпеченням єдиної інформаційної політики в період дії України правового режиму воєнного стану» [17] встановлено, що «в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки, забезпечення якої реалізується шляхом об'єднання усіх загальнонаціональних телеканалів, програмне наповнення яких складається переважно з інформаційних та/або інформаційно-аналітичних передач на єдиній інформаційній платформі стратегічної комунікації – цілодобовому інформаційному марафоні «Єдині новини #UAразом» [17]. Також Указом Президента України введено в дію рішення РНБО України від 18 березня 2022 року «Про нейтралізацію загроз інформаційній безпеці держави», відповідно до якого «Адміністрації Державної служби спеціального зв'язку та захисту інформації України, Концерну радіомовлення, радіозв'язку та телебачення спільно з ТОВ «Зеонбуд» доручено забезпечити

стале функціонування об'єктів цифрового ефірного мовлення та безперебійну трансляцію телевізійних каналів, цілодобовий моніторинг ефірної мережі, обладнання головної станції мультиплексування, супутникових та наземних каналів зв'язку; резервування супутникових каналів доставки програм та обладнання головної станції мультиплексування; резервну доставку телеканалів до цифрових передавачів із залученням альтернативного оператора супутникового зв'язку [15]. Проте сьогодні цей телемарафон викликає багато питань [8].

При цьому варто обумовити, що поняття інформаційних загроз є значно ширше і науковці та законодавство розуміє під ним «потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні» [20], а не лише ретранслюванню цілодобових новин на одній платформі. Адже «інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом» [20].

Відповідно збалансована державна інформаційна політика України має формуватися як складова частина її соціально-економічної, культурно-політичної політики. Не випадково у ст. 17. Конституції України зазначено: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [10]. Тому інформаційну безпеку розуміють як сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз, тобто створення ефективної протидії інформаційним загрозам, де головною інформаційною загрозою національній безпеці є загроза впливу іншої сторони на інформаційну інфраструктуру держави, її інформаційні ресурси, на суспільство, свідомість, підсвідомість особи з метою нав'язати (бажану для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної, державної діяльності, керувати поведінкою у необхідних для іншої сторони напрямах. Варто відзначити, що у контексті протидії дезінформаційним впливам в Україні функціонують ГО «Детектор медіа», ГО «Інститут масової інформації», платформи: «Stop Fake», «VoxUkraine», база даних «Антологія брехні», вебсайт «FactCheck» та інші.

Загрози національній безпеці також, звичайно, можуть проявлятися в обмеженні свободи слова та доступу до публічної інформації, поширенні засобами мас-медіа культу жорстокості, комп'ютерній злочинності та комп'ютерному тероризмі, розголошення інформації, яка становить державну таємницю, або іншу інформацію з обмеженим доступом, спрямовану на задоволення потреб і забезпеченні захисту національних інтересів держави і суспільства, а також намаганні маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, або упередженої інформації [18]. Тому досліджуючи питання інформаційної безпеки необхідно говорити про системність. Систему суб'єктів забезпечення інформаційної безпеки можна визначити як організовану державою сукупність

суб'єктів – органів законодавчої, виконавчої, судової влади, громадських організацій, посадових осіб та окремих громадян, об'єднаних цілями та завданнями щодо захисту національних інтересів в інформаційній сфері, що здійснюють узгоджену діяльність у межах законодавства [11].

Відповідно політика інформаційної безпеки реалізується в Україні системою інститутів публічної влади та інститутами громадянського суспільства, зокрема законодавчим органом – Верховною Радою України, в якій за питання інформаційної безпеки відповідають такі комітети: Комітет з питань гуманітарної та інформаційної політики, Комітет з питань свободи слова, Комітет з питань освіти, науки та інновацій, Комітет з питань цифрової трансформації та інші комітети, що тісно між собою мають взаємодіяти [2]. Обов'язки щодо захисту персональних даних покладено на Уповноваженого Верховної Ради України з прав людини [12].

Президент України як глава держави і Верховний головнокомандувач, здійснює координуючу і контролюючу діяльність органів виконавчої влади у сфері національної безпеки та оборони, є Головою Ради національної безпеки і оборони (РНБО) України. У структурі Секретаріату РНБО діє Служба з питань інформаційної безпеки та кібербезпеки, Служба з питань інформаційних технологій, Служба доступу до публічної інформації та зв'язків із засобами масової інформації [21]. Вищий орган у системі органів виконавчої влади – Кабінет Міністрів України, у структурі якого при Міністерстві цифрової трансформації України є Державна служба спеціального зв'язку та захисту інформації України, Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку. При Міністерстві культури та інформаційної політики України створено Державну службу України з етнополітики та свободи совісті, Державний комітет телебачення і радіомовлення України, Український інститут національної пам'яті УІНП, Державне агентство з питань мистецтва та мистецької освіти. Міністерству освіти і науки України підпорядкована Національна комісія зі стандартів державної мови та Державна служба якості освіти України, Міністерству юстиції України – Державна архівна служба України [7]. В Україні також функціонують інші міністерства та відомства, які мають координувати свою діяльність та діяти відповідно до Конституції України та Законів України, зокрема Служба безпеки України (СБУ), Міністерство внутрішніх справ України, Міністерство оборони України та Служба зовнішньої розвідки України. Окрім того, виконання певних завдань та програм в інформаційній сфері здійснюють й інші органи державної влади України: Міністерство юстиції України, Міністерство закордонних справ України, Міністерство інфраструктури України і т. д.

Наприклад, у структурі СБУ створений Ситуаційний центр забезпечення кібербезпеки. Кіберфахівці Служби цілодобово відповідають за інформаційну безпеку країни, а саме: протидіють розвідкам іноземних держав у кіберпросторі, займаються боротьбою з кібертероризмом і кібершпигунством, протидіють спробам розхитати ситуацію в країні через різноманітні інформаційні «вкиди». Як зазначено на офіційному сайті СБУ їхня особлива увага зосереджена: «… на виявленні та нейтралізації цільових кібератак. Найчастіше їх проводять на замовлення спецслуж іноземних держав. Зазвичай це загрози підвищеної складності. Об'єктами таких кібератак стають важливі комунікаційні системи державних органів і системи керування об'єктів критичної інфраструктури» [19].

Варто наголосити, що саме після початку широкомасштабного вторгнення російських військ в Україну 2022 року, в нашій державі створено також додаткові центри (підрозділи) забезпечення кібербезпеки, або кіберзахисту, наприклад, в Державній службі спеціального зв'язку та захисту інформації України, Національному банку України, Збройних

Силах України і т. д. Розбудовується Національна телекомунікаційна мережа, забезпечується функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, діє урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA [4]. CERT-UA функціонує в складі Державної служби спеціального зв'язку та захисту інформації України. У структуру Державної служби також включено Державний центр кіберзахисту, Національний центр оперативно-технічного управління мережами телекомунікацій, Галузевий державний архів, Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» [4]. З метою отримання важливих (секретних) документів в Україні в структурі Служби є й Головне управління урядового фельд'єгерського зв'язку. Урядовий фельд'єгерський зв'язок – це приймання, обробка, перевезення та доставка (вручення) кореспонденції, що містять відомості, які становлять державну таємницю, службову інформацію, дипломатичну кореспонденцію керівників держави (президента, керівника парламенту, уряду, державних органів, органів військового управління, закордонних дипломатичних установ, органів місцевого самоврядування) [4].

Активно розвивається співпраця України у сфері кібербезпеки з іноземними партнерами (Сполученими Штатами Америки, Сполученим Королівством Великої Британії і Північної Ірландії тощо), поглиблюється співробітництво з країнами ЄС та НАТО, проводяться кібернавчання за участю інших держав та міжнародних організацій. Наприклад, Україна проводить активне співробітництво у галузі безпеки інформації, створенні комп'ютерних мереж у рамках програми НАТО «Наука заради миру та безпеки» («Безпека через науку»). Також в контексті міжнародної співпраці сьогодні реалізується проект в межах EU4DigitalUA за підтримки Європейського Союзу з Міністерством оборони України, який впроваджує естонська Академія електронного управління, щодо формування електронного реєстру призовників, військовозобов'язаних та резервістів «Оберіг». Проект EU4DigitalUA «підтримує цифрову трансформацію та гармонізацію України з Єдиним цифровим ринком ЄС, включаючи цифрову трансформацію, посилену кібербезпеку та захист даних і т. д.» [24].

Отже, сучасний національний інформаційний простір як сфера інформаційних обмінів складається з розгалуженої системи структур, що забезпечують створення нової інформації, її зберігання та захист. Держава загалом зобов'язана захищати свій національний інформаційний простір, його розвиток і використання в інтересах власного суспільства, громадян і держави. А державна інформаційна політика в Україні, як сукупність напрямів діяльності держави в інформаційній сфері, покликана носити системний характер й регулювання та захищати інтереси громадянина, суспільства і держави. Незважаючи на те, що в Україні накопичено велику кількість інформаційних ресурсів, створено ряд інформаційних центрів, функціонує мережа публічних, наукових й освітніх бібліотек, архівів, впроваджено електронне урядування (система «Дія», «e-Health» тощо), обсяги інформації постійно збільшуються, питання формування та використання національних інформаційних ресурсів залишаються постійно актуальними і складними для вирішення. Адже національні інформаційні ресурси – це вся належна Україні інформація, включаючи окремі документи і масиви документів, незалежно від змісту, форми, часу і місця їх створення, форми власності, а також кінцеві результати інтелектуальної, творчої діяльності, зафіксовані на будь-яких носіях інформації, доступні для використання особою, суспільством і державою через засоби масової інформації та телекомунікації, архіви, бібліотеки, музеї, фонди, банки даних, публічні виступи, художньо-виконавську діяльність тощо, які повинні

належним чином охоронятися. Національні інформаційні ресурси – це основа інформаційного суверенітету України. І варто погодитися з дослідниками, які стверджують, що «існуюча інфраструктура державних інститутів інформаційної безпеки України мусить вибудовуватися за принципом стримувань і противаг, відповідно, що державні інститути повинні постійно перебувати під громадським контролем, бути відкритими до комунікації зі ЗМІ, прозорими у своїх рішеннях та звітності, зрозумілими для міжнародних партнерів» [6, с. 4]. Адже тільки держави з розвинутою інформаційною інфраструктурою здатні ставати конкурентоспроможним суб'єктом сучасного міжнародного глобального середовища. При цьому важливо розуміти і завжди пам'ятати, що «…великі геополітичні протистояння найчастіше ведуться не на полі головних супротивників, а у просторі вразливих суспільств та нестабільних держав. Неспроможність цих держав давати адекватні інформаційні відповіді кваліфікується як підстава для інформаційної експансії та поступового поглинання, навіть без очевидного застосування сили» [6, с. 5–6]. Тому варто наголосити, що національну безпеку України в інформаційній сфері потрібно розглядати як інтегральну цілісність персональної, публічної (суспільної), комерційної (корпоративної) й державної безпеки. Адже державна політика забезпечення інформаційної безпеки обумовлена змістом національних інтересів держави, суспільства та людини.

Список використаної літератури

1. Боднар І.Р. Інформаційна безпека як основа національної безпеки. *Механізм регулювання економіки.* 2014. № 1. URL: https://core.ac.uk/download/pdf/141443493.pdf
2. Веб-сайти комітетів Верховної Ради України. *Верховна Рада України: офіційний вебпортал парламенту України.* URL: https://www.rada.gov.ua/documents/contacts/228558.html
3. Гаврильців М.Т Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал.* 2020. № 2. С. 200–203.
4. Державна служба спеціального зв'язку та захисту інформації України: офіційна сторінка. URL: https://cip.gov.ua/ua/news/zakladi-ta-ustanovi-2024
5. Закон України «Про основні засади забезпечення кібербезпеки України». *Відомості Верховної Ради.* 2017. № 45. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
6. Захаренко К.В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири: автореф. дисерт. на здобуття наук. ступеня докт. політ. н. за спец. 23.00.02 – політичні інститути та процеси. Львів, 2021. 35 с.
7. Інші органи виконавчої влади. *Урядовий портал: Єдиний веб-портал органів виконавчої влади України.* URL: https://www.kmu.gov.ua/catalog
8. Єрохін Б. За великі гроші і без результату: чи потрібен Україні телемарафон? *Медіакритика.* 18.05.2024. URL: http://mediakrytyka.lnu.edu.ua/ohlyady-analityka/za-velyki-hroshi-i-bez-rezultatu-chy-potriben-ukrayini-telemarafon.html
9. Кібербезпека в інформаційному суспільстві: інформаційно-аналітичний дайджест. № 10. (жовтень). К., 2022. URL: http://ippi.org.ua/sites/default/files/2022-10.pdf
10. Конституція України. *Офіційне інтернет-представництво Президента України.* URL: https://www.president.gov.ua/ua/documents/constitution/konstituciya-ukrayini-rozdil-i
11. Мужанова Т.М. Інформаційна безпека держави: навчальний посібник. URL: https://nubip.edu.ua/sites/default/files/u34/posibnik_ibd_muzhanova_2019.pdf
12. Омбудсман України: *офіційний сайт*. URL: https://ombudsman.gov.ua/uk/pro-nashu-robotu
13. Почепцов Г. Інформаційна політика : навч. посіб. К.: Знання, 2006. 663 с.

14. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року. *Верховна Рада України: Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80#n14
15. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Про нейтралізацію загроз інформаційній безпеці держави» № 151/2022. *Верховна Рада України: офіційний вебпортал парламенту України.* URL: https://zakon.rada.gov.ua/laws/show/151/2022#Text
16. Про Стратегію інформаційної безпеки. *Верховна Рада України: Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n14
17. Рішення «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану», введено в дію Указом Президента України від 19.03.2022 року № 152/2022. *Верховна Рада України: офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/n0004525-22#n2
18. Савіцький В.Т. Інформаційна безпека в системі національної безпеки України. *Університетські наукові записки.* 2017. № 62. URL: http://old.univer.km.ua/visnyk/1728.pdf
19. Ситуаційний центр забезпечення кібербезпеки. *Служба безпеки України: офіційний сайт* URL: https://ssu.gov.ua/sytuatsiinyi-tsentr-zabezpechennia-kiberbezpeky
20. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.2021 № 685/2021. *Верховна Рада України: офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text
21. Структура Апарату Ради національної безпеки і оборони України. *Рада національної безпеки і оборони України: офіційний сайт.* URL: https://rnbo.gov.ua/ua/Aparat-Rady-natsionalnoi-bezpeky-i-oborony-Ukrainy.html
22. Чукут С.А., Джига Т.В. Інформаційна політика в Україні: опорний конспект лекцій / Національна академія державного управління при Президентові України. К., 2007. 94 с.
23. Юдін О.К., Богуш В.М. Інформаційна безпека держави: навчальний посібник. Харків: Консум, 2005. 576 с.
24. EU4DigitalUA. *Фінансується Європейським Союзом.* https://eufordigital.eu/uk/discover-eu/eu4digitalua/

THE INFORMATION SECURITY ENSURING SYSTEM OF THE STATE IN THE CONDITIONS OF A LARGE-SCALE INVASION OF RUSSIAN ARMY INTO UKRAINE

Olha Anisimovych-Shevchuk
Lviv Polytechnic National University,
Institute of Humanities and Social Sciences,
Department of Political Science and International Relations
Metropolitan Andrey str., 5, 79013, Lviv, Ukraine

Svitlana Matviienkiv
Vasyl Stefanyk Precarpathian National University,
Faculty of History, Politology and International Relations,
Department of Political Institutions and Processes
Shevchenko str., 57, Ivano-Frankivsk, 76018, Ukraine

The attention on the protection of the information and communication space of the state in the conditions of today's Russian-Ukrainian war is focused. The importance of ensuring information security, prompt response to information and communication threats and dangers is emphasized. The purpose

of the study is to carry out the analysis of the formed system of ensuring information security of Ukraine after the large-scale invasion of Russian troops into Ukraine. System analysis, case study method, regulatory and scientific sources, government sites, etc. were analyzed.

The article notes that the problem of the functioning of the modern national information space as a sphere of information exchanges consists of an extensive system of structures. The national information space includes information and telecommunication infrastructure and resources that ensure the interaction of citizens, the state, and organizations and contribute to meeting their information and communication needs on the territory of Ukraine and ensure national information sovereignty.

The importance of the implementation of a unified information policy, which is a priority task of the national security of the state, is emphasized. It was noted that during the years of independence in Ukraine, the legislative foundations of the information security system were formed. The system of national information resources has a departmental, interdepartmental nature and covers information resources of state authorities and management, local and regional self-government; state statistics, archival, library and museum funds, etc. At the same time, it is stipulated that the ownership of information resources ensures the national sovereignty of the state. It is emphasized that the information security policy of Ukraine is implemented by the system of institutions of public authority and institutions of civil society. Examples of cooperation in the field of ensuring information security of the information and communication space of Ukraine are given.

Key words: information security, information, communication, war, information and communication space, the information and communication infrastructure and resources state authorities, national security.