Галіпчак Володимир Дмитрович

Державно-правовий механізм інформаційної безпеки України в умовах російської агресії

УДК 355.01:004.056.5
DOI https://doi.org/10.24195/2414-9616.2023-5.3

Галіпчак Володимир Дмитрович
аспірант кафедри політичних інститутів та процесів
Прикарпатського національного університету імені Василя Стефаника
вул. Шевченка, 57,
Івано-Франківськ, Україна
ORCID: 0009-0006-2501-0290

У статті розглядається система заходів, призначених для захисту інформаційної сфери України у відповідь на російську агресію. Стаття глибоко аналізує сучасний стан інформаційної безпеки України, фокусуючись на викликах, що виникають в умовах російської агресії та гібридної війни. Автор детально розглядає державно-правовий механізм, спрямований на захист інформаційного простору, та визначає ключові аспекти цього механізму. Здійснюється детальний аналіз правових та організаційних аспектів цього механізму, зокрема, створення спеціалізованих органів та регулювання кібербезпеки. Стаття розпочинається аналізом поточного стану інформаційної безпеки, ідентифікуючи актуальні проблеми та виклики. Далі вона фокусується на державно-правовому регулюванні, розглядаючи створення спеціалізованих органів та нормативно-правовий базис. Особлива увага приділяється кібербезпеці, зокрема заходам щодо захисту від кібератак та впровадженню новітніх технологій у цю сферу. Робиться аналіз ситуацій, коли інформаційна безпека була порушена через російську агресію. У заключній частині статті автор намагається визначити перспективи подальшого розвитку державно-правового механізму в умовах гібридної війни та непередбачуваних кіберзагроз. В основі статті лежить комплексна методологія дослідження, яка висвітлює не тільки стан інформаційної безпеки України, але й ретельно аналізує дієвість державно-правового механізму в умовах російської агресії та гібридної війни, включаючи в себе як державно- правовий аспект так і відображення конкретних прикладів. Актуальність роботи визначається нагостреним впливом російської агресії на інформаційну безпеку України та необхідністю адаптації державно-правового механізму до нових викликів. Автор аналізує вплив російсько-української війни на сферу інформаційної безпеки та пропонує шляхи подальшого розвитку та удосконалення заходів у цьому напрямку. Стаття слугує важливим джерелом для фахівців у галузі інформаційної безпеки, а також для владних структур, які цікавляться зміцненням захисту інформаційного простору в умовах гібридної війни та кіберзагроз.

Ключові слова: *інформаційна безпека, інформаційний простір, інформаційна загроза, кібербезпека, державно-правовий механізм, російська агресія.*

Вступ. У сучасному світі інформаційної вразливості та нестабільної політичної ситуації, питання забезпечення інформаційної безпеки стає визначальним елементом національного суверенітету. Особливо актуальним воно стає для України, яка, знаходячись в умовах російсько-української війни, стикається з високим рівнем інформаційних загроз і агресії. У даному контексті важливо дослідити, як державно-правовий механізм інформаційної безпеки України відповідає на виклики, що виникають у зв'язку із російською агресією. Розуміння цього механізму та його ефективності є ключовим для розбудови стійкого та надійного захисту інформаційного простору країни. У цій статті ми спробуємо розглянути не лише сам механізм захисту, а й його реальний вплив на ситуацію в умовах військового конфлікту. Аналіз законодавства, дій владних структур, а також вивчення практичних кроків, вжитих для забезпечення інформаційної безпеки, дозволить нам краще розуміти виклики, перед якими стоїть Україна, та шляхи вдосконалення її захисту в умовах реальної загрози російської агресії. Це дослідження надасть можливість краще вникнути в те, як владні структури та правові механізми реагують на постійну та розмаїту інформаційну небезпеку в умовах військового конфлікту. Російська агресія виявляється не лише на військовому полі, а й у кіберпросторі, в сфері дезінформації та маніпуляції громадською думкою. Саме тому, особливо важливо – розкрити взаємозв'язок між політично-правовими заходами та реальною інформаційною обстановкою. Наприклад, які законодавчі акти були прийняті для посилення захисту інформаційної сфери, як вони впроваджуються на практиці, та чи вистачає цього для ефективного протидії російській агресії. Дослідження спрямоване не лише на виявлення вразливостей української системи захисту інформації, але й на визначення конкретних шляхів її удосконалення. Розуміння механізму інформаційної безпеки є важливою передумовою для будь-якої держави, особливо тієї, яка зазнає впливу та повномасштабної агресї з сторони сусіда-ворога, і її результати можуть мати велике значення для подальшого розвитку і стійкості у цій боротьбі.

Мета статті. Мета цієї статті – детально розглянути та проаналізувати державно-правовий механізм інформаційної безпеки України в контексті російсько-української війни. Наша мета полягає в розкритті ефективності цього механізму, виявленні його сильних та слабких сторін, а також визначенні можливих шляхів вдосконалення для більш ефективного протидії інформаційним загрозам та агресії з боку Росії.

Завдання статті:

- Дослідити поняття державно-правового механізму: ретельний огляд законодавчих актів та структур, регулюючих інформаційну безпеку в Україні в умовах російсько-української війни.

- Проаналізувати роль державних інститутів: провести детальне дослідження ролі державних інститутів у виконанні завдань інформаційної безпеки в умовах війни.

- Визначити ефективність заходів: визначити, наскільки ефективно впроваджені заходи забезпечують інформаційну безпеку країни.

- Виявити вразливості та загрози: виявити потенційні вразливості і ідентифікувати конкретні загрози для інформаційної безпеки.

- Запропонувати заходи для вдосконалення: визначити конкретні рекомендації та заходи для вдосконалення системи інформаційної безпеки України.

- Підняти свідомість громадськості: провести аналіз ефективності інформаційних кампаній та заходів для підвищення розуміння громадськості щодо інформаційної безпеки та її важливості в умовах військового конфлікту.

Ці завдання спрямовані на глибоке вивчення та оцінку державно-правового механізму інформаційної безпеки України в контексті російсько-української війни. Їх виконання передбачає виявлення ефективності існуючих заходів, визначення слабких сторін та пропозиції конкретних заходів для підвищення рівня захисту інформаційного простору країни.

Методи дослідження. Здійсненню та реалізації дослідження сприяє застосування чіткої структурованої методології. Ця методологія дозволяє здійснити комплексний та систематичний аналіз державно-правового механізму інформаційної безпеки, зокрема в контексті російсько-української війни, та виявити шляхи для подальшого вдосконалення цього механізму. До основних мето дів дослідження можемо віднести: аналіз законодавства та нормативних актів (оцінка ключових правових документів, що регулюють інформаційну безпеку в Україні. Акцент на вивченні конкретних положень, які стосуються захисту інформаційного простору в умовах російсько-української війни), державно-правовий аналіз інституціональної діяльності (глибокий аналіз ролі та дії державних структур у контексті інформаційної безпеки, орієнтований на розкриття особливостей функціонування та ефективності в умовах військового конфлікту), оцінка ефективності заходів інформаційної безпеки (використання методів аналізу та вивчення практичної реалізації заходів забезпечення інформаційної безпеки для визначення їхньої ефективності в умовах воєнного конфлікту), аналіз вразливостей та загроз (використання методів виявлення і системного аналізу для ідентифікації потенційних вразливостей і загроз системи інформаційної безпеки), стратегічний аналіз реакції на інформаційні загрози (застосування стратегічного підходу для аналізу реакції влади на конкретні інформаційні загрози та визначення перспективних напрямків вдосконалення системи захисту), аналіз інформаційних кампаній та громадської свідомості (вивчення інформаційних кампаній з точки зору їх впливу на свідомість громадськості та рівень їхньої інформованості щодо інформаційної безпеки в умовах військового стану та війни зокрема). Дана методологія дозволяє здійснити високоспеціалізований аналіз державно-правового механізму інформаційної без.пеки, враховуючи особливості його функціонування в умовах геополітичної напруженості

Результати. В сфері державно-правового механізму інформаційної безпеки в Україні та за кордоном існують численні наукові досягнення відомих дослідників. Зокрема, слід згадати про О. Волкова (видатний український юрист та дослідник, який активно працює в галузі інформаційної безпеки [1]. Автор праць «Правові аспекти забезпечення кібербезпеки в Україні», де розглядається правове регулювання сфери кібербезпеки в контексті української дійсності. Його наукові статті та монографії висвітлюють питання правового забезпечення інформаційної безпеки та впливу цього на сучасну державну політику), М. Літинську (вчений-юрист, спеціалізується на проблемах інформаційної безпеки та кіберправа. Її дослідження зорієнтовані на аналіз правового врегулювання в галузі кібербезпеки та правової відповідальності за кіберзлочини. Авторка праці «Кіберправо: правові аспекти захисту інформаційної безпеки», де розглядаються актуальні питання юридичного регулювання у сфері кібербезпеки та кіберзахисту) та ін. [3]. Говорячи, про коло зарубіжних вчених, слід викоремити Р.Кларка («Кібервійна», де розглядаються актуальні питання юридичного регулювання у сфері кібербезпеки та кіберзахисту) [9], Дж. Нує (автор концепції «М'яка сила» та «Сила майбутнього», де він розглядає вплив інформаційного простору на владу та визначає роль кібербезпеки у сучасних міжнародних відносинах), К. Зеттера («Зворотній відлік до нуля: Стакснет та запуск першої цифрової зброї» [10], де детально розглядається історія створення та вплив комп'ютерного вірусу Стакснет на кібербезпеку та геополітику) [11]. Ці та інші вчені внесли значний вклад у розуміння та розвиток сфери інформаційної безпеки. Усі вони сприяють вдосконаленню стратегій інформаційної безпеки, а їхні наукові висновки та рекомендації відіграють важливу роль у формуванні політики та заходів для захисту від кіберзагроз.

У світлі сучасних геополітичних турбулентностей, поняття «інформаційна безпека» стає

не лише актуальним, але й критично важливим для забезпечення стабільності та суверенітету країни. Україна, яка зазнає впливу російської агресії, стикається з непередбачуваними викликами та загрозами в інформаційному просторі. У цьому контексті, дослідження державно-правового механізму інформаційної безпеки набуває особливої важливості. Визначення ключових термінів у нашому дослідженні є першоважним кроком для розкриття сутності державно-правового механізму та інформаційної безпеки в умовах російської агресії. «Державно-правовий механізм» визначається як система законів та інституцій, спрямована на забезпечення функціонування держави та захист її інтересів. «Інформаційна безпека» охоплює комплекс заходів, спрямованих на захист інформаційного простору від загроз та агресії [4].

Актуальність цієї теми визначається не лише концептуально, але й практично. Сучасна реальність, в якій держава опиняється під впливом російської агресії, вимагає перегляду та вдосконалення механізмів захисту від інформаційних загроз. Відновлення та зміцнення національної безпеки України неможливе без системного аналізу та вдосконалення державно-правового механізму інформаційної безпеки. У цьому контексті наше дослідження є не лише актуальним, але й необхідним для формування ефективних стратегій захисту від інформаційних загроз в умовах геополітичних напружень.

Аналізуючи державно-правовий механізм інформаційно безпеки України, слід перш за все зупинитися на огляді основних законодавчих актів та структур, що регулюють інформаційну безпеку в Україні. Це свідчить про наявність комплексного підходу до захисту інформаційного простору. Законодавча база та відповідні структури забезпечують ефективність заходів інформаційної безпеки в умовах внутрішніх та зовнішніх загроз. Сюди перш за все відносять:

1. Закон «Про інформацію» (він визначає основні принципи обробки, зберігання та передачі інформації, а також встановлює вимоги до захисту конфіденційної інформації та протидії її незаконному використанню).

2. Закон «Про кібербезпеку» (визначає основні напрями та завдання в галузі захисту кіберпростору. Він встановлює відповідальність за кіберзлочини, а також регулює взаємодію державних інститутів, підприємств та громадян у сфері кібербезпеки).

3. Закон «Про захист інформації в інформаційно-телекомунікаційних системах» (визначає правила та вимоги до захисту інформації в інформаційно-телекомунікаційних системах. Він встановлює стандарти кіберзахисту, обов'язкові для впровадження суб'єктами інформаційно-телекомунікаційних систем) [7].

4. Державна служба спеціального зв'язку та захисту інформації (відіграє ключову роль у координації та реалізації заходів з захисту інформації в Україні. Вона надає консультації суб'єктам інформаційної діяльності, а також бере на себе функцію розслідування інцидентів у сфері інформаційної безпеки).

Роль державних інститутів у здійсненні державно-правового механізму інформаційної безпеки в Україні полягає в координації заходів, визначенні стратегічних напрямків, розслідуванні та запобіганні інцидентам. Однією з ключових ролей в забезпеченні інформаційної безпеки в Україні відіграє Державна служба спеціального зв'язку та захисту інформації. Їй доручено розробку та впровадження заходів з кіберзахисту, контроль за дотриманням стандартів безпеки в інформаційно-телекомунікаційних системах, а також розслідування інцидентів у сфері інформаційної безпеки. Міністерство внутрішніх справ відіграє важливу роль у боротьбі з кіберзлочинністю. Воно веде розслідування та приймає превентивні заходи щодо протидії кіберзлочинності, здійснює взаємодію із зовнішніми та внутрішніми партнерами з метою забезпечення безпеки в інформаційному просторі. Рада національної безпеки та оборони України є вищим органом державного управління у сфері безпеки та оборони. Вона визначає стратегічні напрями розвитку інформаційної безпеки, враховуючи загальнодержавні інтереси та виклики, що випливають із геополітичних та технологічних тенденцій. Комітет з питань національної безпеки та оборони Верховної Ради грає роль законодавчого органу, що формує та вдосконалює законодавство у сфері інформаційної безпеки. Ці органи взаємодіють для забезпечення суверенітету країни в інформаційному просторі та впровадження ефективних заходів безпеки [5].

В умовах сучасної глобалізації та інформаційних технологій російська агресія стає багатогранною загрозою, виявляючи свої впливові та дестабілізуючі наслідки в інформаційному просторі. Зупинимось на аналізі специфічних загроз, що виникають внаслідок російської агресії в інформаційному просторі.

– Дезінформація та пропаганда (однією з основних загроз є системна дезінформація та пропаганда, спрямована на спотворення образу України в світовому інформаційному просторі. Російська агресія виявляється у виробленні та розповсюдженні фейкових новин, які мають на меті підривати довіру до української влади та викликати міжнаціональні конфлікти).

– Кібератаки та кібершпигунство (російська агресія в інформаційному просторі супроводжується активними кібератаками та кібершпигунством. Вони спрямовані на різноманітні об'єкти, включаючи державні установи, критичну інфра-

структуру та приватні компанії. Атаки цільовані на отримання конфіденційної інформації та порушення роботи важливих систем).

− Маніпулювання громадською думкою (російська агресія активно використовує соціальні мережі та інші онлайн-платформи для маніпулювання громадською думкою. За допомогою ботів, фейкових акаунтів та агресивної інформаційної кампанії, створюються штучні обставини, що впливають на громадську думку та політичний ландшафт).

− Порушення кібергігієни та кіберзагрози громадянам (включає в себе спроби впливати на кібергігієну громадян, щоб отримати доступ до їх особистої інформації. Фішингові атаки та використання шкідливих програм призводять до порушення конфіденційності та безпеки особистих даних) [6].

Наводячи конкренті приклади, коли нформаційна безпека була порушена внаслідок російської втручання, слід сказати, про кібератаки на енергетичну інфраструктуру, розповсюдження фейкових новин через медіа: російські агенти активно використовують медіа для поширення неправдивої інформації, щоб спотворити події та викликати негативне ставлення до української влади; спроба втручання в політичні процеси через соціальні мережі.

Україна, зіштовхуючись з постійною інформаційною агресією, активно вдосконалює свій державно-правовий механізм для забезпечення інформаційної безпеки. Деякі приклади успішних заходів та проєктів свідчать про високий рівень адаптації та реагування на виклики, а саме:

1. Створення Національного центру кібербезпеки: у 2018 році Україна створила Національний центр кібербезпеки, який відповідає за аналіз, координацію та реагування на кіберзагрози. Цей центр є ключовим елементом в системі захисту від кібератак та впроваджує заходи щодо підвищення кібербезпеки в усіх сферах.

2. Закон «Про заборону пропаганди комуністичного та націонал-соціалістичного тоталітарних режимів»: в Україні прийнято закон, що забороняє публічне поширення символіки комуністичного та націонал-соціалістичного тоталітарних режимів. Цей крок спрямований на запобігання маніпуляціям та спробам переписати історію через використання відповідної пропаганди.

3. Активна робота в інформаційних мережах: Україна активно використовує свою інформаційну присутність для протидії агресивній пропаганді. Зокрема, створено англомовний медіацентр «Україна Today», який поширює об'єктивну інформацію про події в Україні, збиваючи міфи та фейки.

4. Закон «Про кібербезпеку»: прийнятий в 2017 році закон «Про кібербезпеку» встановлює правила та заходи для захисту кіберпростору. Він визначає обов'язки операторів критичної інфраструктури, регулює взаємодію з іншими країнами у сфері кібербезпеки та встановлює порядок реагування на інциденти [8].

5. Проєкт «Стопфейк»: ініційований громадськими активістами, проєкт «Стопфейк» працює на виявленні та розкритті фейкової інформації. Цей інструмент дозволяє швидко реагувати на дезінформацію та надає можливість громадянам отримувати достовірну інформацію.

Ці приклади та низка інших заходів на державному, правовму та громадських рівнях, свідчать про те, що Україна активно впроваджує інноваційні та комплексні заходи для протидії інформаційній агресії. Реалізація цих заходів вимагає взаємодії різних секторів суспільства та поглиблення розуміння суті інформаційних викликів. Вивчення реакції українського уряду та громадськості на інформаційну агресію виявляється комплексним та взаємодійним підходом. Реакція українського уряду на інформаційну агресію виявляється системною та спрямованою на захист національної безпеки. Національний центр кібербезпеки забезпечує аналіз та реагування на кіберзагрози, а прийняття законів щодо інформаційної безпеки встановлює правовий фреймворк для боротьби з дезінформацією.

Громадськість активно включена в процес виявлення та протидії інформаційній агресії. Ініціативи громадян, такі як розробка онлайн-платформ для перевірки інформації та ангажованість у соцмережах, грають ключову роль у формуванні оповіщеної та інформованої громадськості. Підвищення інформаційної грамотності серед населення виступає як стратегічний напрямок [2]. Проекти та освітні заходи ставлять за мету формування навичок критичного мислення та розуміння особливостей інформаційного середовища. Головною рисою реакції українського уряду та громадськості є взаємодія та співпраця. Міжнародна співпраця у сфері інформаційної безпеки покликана забезпечити обмін досвідом та ресурсами для ефективного протидії глобальним інформаційним викликам. Засоби масової інформації в Україні акцентують на дотриманні етичних стандартів та високої журналістської доброчесності, надаючи громадянам якісні та достовірні інформаційні джерела.

Цей глибокий та об'єднаний підхід свідчить про готовність українського суспільства та його лідерів реагувати на інформаційні загрози, зберігаючи високий рівень інформаційної безпеки та відповідальності перед громадянами.

Висновки. Таким чином, слід підсумувати, що механізм державно-правового інформаційного захисту України складає цілу систему законодавчих та урядових заходів, спрямованих на захист національної інформаційної сфери в умовах сучасних загроз та викликів, зокрема,

в умовах російської агресії. Він спрямований на підвищення стійкості країни до кіберзагроз, забезпечення конфіденційності та цілісності інформації, а також формування інформаційної оборони як ключового компонента національної безпеки. Висновки стосовно державно-правового механізму інформаційної безпеки України в умовах російської агресії вказують на важливість та необхідність комплексного та динамічного підходу до забезпечення національної безпеки в цифровому столітті. Державні ініціативи, такі як створення Національного центру кібербезпеки та прийняття законодавства про кібербезпеку, свідчать про готовність уряду реагувати на високотехнологічні загрози. Громадська активність та ініціативи, спрямовані на виявлення та опровердження дезінформації, відображають важливу роль громадян у формуванні інформаційної оборони. Підсумовуючи, варто зазначити, що ефективне забезпечення інформаційної безпеки потребує поєднання зусиль уряду, громадян та міжнародних партнерів. Постійна готовність до інновацій та удосконалення механізмів боротьби стає стратегічним завданням для збереження національної безпеки в умовах сучасних викликів та ризиків, зумовлених повномасштабним вторгненням на територію нашої країни, задля збереження свого суверенітету та розвитку держави і нації як такої.

ЛІТЕРАТУРА:

1. Біленчук П. Д., Борисова Л. В., Неклонський І. М., Собина В. О. (2018). *Правові засади інформаційної безпеки України:* монографія / за ред. П.Д.Біленчука. Харків, 289 с.

2. Герасимов, І. (2018). *Інформаційна війна ізоляції: російська агресія проти України в медійному просторі.* Інститут медіафорсайт. Вінниця, 22-24 с.

3. Іванов, О. (2019). *Інформаційна безпека України: сучасний стан та виклики.* Національний інститут стратегічних досліджень. Київ, 124 с.

4. Кормич Б. (2003). *Інформаційна безпека України: організаційно-правові основи:* Навч. посібник. Київ, Кондор, 384 с.

5. Лісовський, О. (2021). К*ібербезпека та інформаційна війна: виклики та загрози.* Львів: Магнолія, 16-23 с.

6. Тарасюк А. (2020). *Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи*: монографія. Фенікс, Київ, 400 с.

7. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7.

8. *Про основи національної безпеки україни: Закон україни від 19.06.2003 р. No 964-IV / Верховна Рада україни. Відомості Верховної Ради* україни. 2003. No 39. Ст. 351.7.

9. Clarke, R. A., & Knake, R. K. (2019). *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats.* Penguin Press, 162 p.

10. Friedman, A., & Singer, P. W. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford University Press, 43-46 p.

11. Singer, P. W., & Friedman, A. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* Crown, 124 p.

REFERENCES:

1. Bilenchuk P. D., Borisova L. V., Neklonsky I. M., Sobina V. O. (2018). Pravovi zasady informatsiynoi bezpeky Ukrainy: monohrafiya / za red. P.D. Bilenchuka. Kharkiv, 289 s.

2. Herasymov, I. (2018). Informatsiyna viyna izolyatsii: rosiyska ahresiya proty Ukrainy v mediynomu prostori. Instytut mediaforsayt. Vinnytsia, 22-24 s.

3. Ivanov, O. (2019). Informatsiyna bezpeka Ukrainy: suchasnyi stan ta vyklyky. Natsionalnyi instytut stratehichnykh doslidzhen. Kyiv, 124 s.

4. Kormych B. (2003). Informatsiyna bezpeka Ukrainy: orhanizatsiyno-pravovi osnovy: Navch. posibnyk. Kyiv, Kondor, 384 s.

5. Lisovskyi, O. (2021). Kiberbezpeka ta informatsiyna viyna: vyklyky ta zahrozy. Lviv: Magnoliia, 16-23 s.

6. Tarasiuk A. (2020).Kiberbezpeka Ukrainy na suchasnomu etapi derzhavotvorennia: teoretyko-pravovi osnovy: monohrafiya. Feniks, Kyiv, 400 s.

7. Ukaz Prezydenta Ukrainy «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku «Pro Stratehiiu informatsiinoi bezpeky». URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7.

8. Pro osnovy natsionalnoi bezpeky Ukrainy: Zakon Ukrainy vid 19.06.2003 p. No 964-IV / Verkhovna Rada Ukrainy. Vidomosti Verkhovnoi Rady Ukrainy. 2003. No 39. St. 351.7.

9. Clarke, R. A., & Knake, R. K. (2019). The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. Penguin Press, 162 s.

10. Friedman, A., & Singer, P. W. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 43-46 s.

11. Singer, P. W., & Friedman, A. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown, 124 s.

State-legal mechanism of information security in Ukraine in the context of Russian aggression

Halipchak Volodymyr Dmytrovych

Postgraduate Student at the Department of Political Institutions and Processes
Vasyl Stefanyk Precarpathian National University
Shevchenka str., 57, Ivano-Frankivsk, Ukraine
ORCID: 0009-0006-2501-0290

The article examines the system of measures designed to protect the information sphere of Ukraine in response to Russian aggression. The article deeply analyzes the current state of information security in Ukraine, focusing on the challenges that arise in the conditions of Russian aggression and hybrid warfare. The author examines in detail the state-legal mechanism aimed at protecting the information space and defines the key aspects of this mechanism. A detailed analysis of the legal and organizational aspects of this mechanism is carried out, in particular, the creation of specialized bodies and regulation of cyber security. The article begins with an analysis of the current state of information security, identifying current problems and challenges. Next, it focuses on state-legal regulation, considering the creation of specialized bodies and the normative-legal basis. Special attention is paid to cyber security, in particular measures to protect against cyber attacks and the introduction of the latest technologies in this area. An analysis is made of situations when information security was violated due to Russian aggression. In the final part of the article, the author tries to determine the prospects for the further development of the state-legal mechanism in the conditions of hybrid warfare and unpredictable cyber threats. The article is based on a comprehensive research methodology, which highlights not only the state of information security in Ukraine, but also carefully analyzes the effectiveness of the state-legal mechanism in the conditions of Russian aggression and hybrid war, including both the state-legal aspect and the reflection of specific examples. The urgency of the work is determined by the heightened impact of Russian aggression on Ukraine's information security and the need to adapt the state-legal mechanism to new challenges. The author analyzes the impact of the Russian-Ukrainian war on the field of information security and suggests ways of further development and improvement of measures in this direction. The article serves as an important resource for specialists in the field of information security, as well as for authorities interested in strengthening the protection of the information space in the conditions of hybrid warfare and cyber threats.

Key words: *information security, information space, information threat, cyber security, state-legal mechanism, Russian aggression.*