УДК 340; 342.1
DOI https://doi.org/10.32838/1606-3716/2019.4/06

Шемчук В.В.
Таврійський національний університет імені В.І. Вернадського

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНА ОБОРОНА В КОНТЕКСТІ РОЗВИТКУ ВІТЧИЗНЯНОЇ ДОКТРИНИ Й ЗАКОНОДАВЧОЇ ОСНОВИ

У статті здійснено дослідження теоретичних основ і законодавчого забезпечення категорій «інформаційна безпека» та «інформаційна оборона». Проаналізовано доктринальну практику, різні підходи до розуміння природи й сутності інформаційної безпеки насамперед у юридичній науці, поряд із цим виокремлено своєрідні підходи й в інших галузях вітчизняної науки. Підкреслюється термінологічна невизначеність, неоднозначність та авторське бачення цієї категорії. Так, в узагальненому вигляді інформаційну безпеку доцільно розглядати крізь призму правовідносин, що виникають під час забезпечення стану захищеності інформаційного простору. Обґрунтованим є комплексне трактування сутності та гарантій забезпечення інформаційної безпеки держави як напряму державної політики у сфері національної безпеки і оборони, невід'ємної частини політичного, економічного, оборонного й інших складників національної безпеки. Це підтверджується аналізом положень Конституції України, Законів України: «Про національну безпеку України», «Про Концепцію Національної програми інформатизації», «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», «Про оборону України» тощо, у яких однозначно інформаційна безпека визнається одним із напрямів державної політики у сфері національної безпеки і оборони.

Інформаційна оборона є системою заходів захисту інформаційної та віртуальної сфери, що забезпечує готовність до інформаційного впливу, нападу інших держав, захист і розвиток інформаційного простору, підвищення обороноздатності Збройних Сил і цивільного населення до інформаційних атак незалежно від наявності збройних конфліктів. На законодавчому рівні в Україні розмежовано повноваження державних органів у сферах національної безпеки і оборони, визначено систему командування, контролю та координації операцій сил безпеки й сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони, забезпечуючи в такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони.

Відзначено взаємозалежність і взаємодоповнюваність досліджуваних понять, їх загальну спрямованість на забезпечення стану захищеності інформаційного простору, превентивних і захисних заходів, усунення інформаційних загроз і забезпечення безпечного розвитку національного інформаційного простору на сучасному етапі.

Ключові слова: *інформаційна безпека, інформаційна оборона, інформаційна політика, інформаційний простір, захист, законодавча основа.*

Постановка проблеми. Події останніх років актуалізують необхідність звернення до теоретичних і практичних аспектів таких категорій, як національна безпека, конституційний лад, суверенітет, територіальна цілісність, непорушність державних кордонів, оборона держави тощо. Іноді спостерігається термінологічна невизначеність, певна плутанина чи неоднозначність їх розуміння. На наше переконання, це змушує звернути увагу представників різних галузей сучасної науки до згаданих категорій, адже з'ясування їх природи, сутності, відмінностей і механізмів забезпечення є важливим як для пересічного громадянина, так і для високопосадовців, учених і загалом для вітчизняної й зарубіжної доктрин.

Аналіз останніх досліджень і публікацій. Варто констатувати, що різноманітні аспекти інформаційної сфери стали предметом досліджень різних галузей сучасної науки. Так, питання інформаційного суспільства, інформаційної політики, інформаційної безпеки аналізуються переважно представниками юридичної науки,

державного управління, натомість питання інформаційної війни, інформаційної оборони розглядаються набагато рідше у військових, технічних чи інших науках. Безумовно, теоретичну основу порушеної нами проблематики становлять наукові праці Р. Гули, І. Забари, В. Демиденко, О. Довганя, Н. Камінської, О. Кирилюк, О. Косогова, В. Ліпкана, А. Марущака, Н. Ніжник, А. Пазюка, В. Політанського, О. Сивака, С. Соловйова, В. Хорошко, Ю. Хохлачової, П. Ткачука, В. Цимбалюка та ін.

Відзначимо, що цими авторами в наукових працях аналізуються переважно питання інформаційної політики, інформаційних війн, інформаційної безпеки в Україні, натомість проблеми співвідношення категорій інформаційної безпеки та інших взаємопов'язаних категорій розглядаються вкрай рідко.

Постановка завдання. Метою статті є здійснення дослідження теоретичних основ і законодавчого забезпечення правових категорій «інформаційна безпека» та «інформаційна оборона», розкриття їх природи й сутності, а також їх співвідношення з огляду на політико-правові реалії української дійсності.

Виклад основного матеріалу дослідження. У сучасну епоху цифрових технологій, електронного урядування й переходу від індустріального чи постіндустріального суспільства до якісно нового інформаційного суспільства постають нові завдання та виклики. Вони стосуються практично населення й держав, світового співтовариства, на наше переконання, з часом вони лише загострюються. Тим паче їх вивчення та забезпечення реалізації безпосередньо покладається на відповідні органи й посадових осіб конкретних держав, бо фактично на національному рівні можливе встановлення певних регуляторів у тому числі зобов'язуючого чи забороняючого характеру в інформаційній сфері.

Підкреслимо, що, наприклад, відносини в глобальній мережі Інтернет ще не відзначаються наявністю уніфікованих міжнародно-правових стандартів обов'язкового характеру, засади регламентації таких відносин повинні держави визначати насамперед на внутрішньодержавному рівні в тому числі стосовно відповідальності за їх порушення, заподіяння збитків правам і свободам людини в інформаційній та інших сферах, національній безпеці тощо.

Поширеним є підхід до розкриття сутності інформаційної безпеки через більш широке поняття національної безпеки. Зокрема, він подається в енциклопедичній і довідковій літературі.

У багатотомній юридичній енциклопедії інформаційна безпека України визначається як один із видів національної безпеки, важлива функція держави. Інформаційна безпека України означає:

– законодавче формування державної інформаційної політики;

– створення можливостей досягнення інформаційної достатності для ухвалення рішень суб'єктами права;

– гарантування свободи інформаційної діяльності та права доступу до інформації;

– усебічний розвиток інформаційної структури;

– підтримка розвитку національних інформаційних ресурсів;

– створення й упровадження безпечних інформаційних технологій;

– захист права власності держави на стратегічні об'єкти інформаційної інфраструктури України;

– охорону державної таємниці;

– створення загальної системи охорони інформації;

– захист національного інформаційного простору України;

– установлення законодавством режиму доступу іноземних держав до національних інформаційних ресурсів;

– законодавче визначення порядку поширення інформаційної продукції зарубіжного виробництва на території України [1, с. 714].

Л. Наливайко трактує інформаційну безпеку як сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Ця безпека має включати ефективну протидію сукупності інформаційних загроз [2].

Л. Харченко, В. Ліпкан, О. Логінов визначили, що інформаційна безпека – це складник національної безпеки, процес управління загрозами та небезпеками, державними й недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України [3, с. 47].

О. Литвиненко під інформаційної безпекою розуміє єдність трьох складників: забезпечення захисту інформації; забезпечення захисту й контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності [4].

Можна також зустріти дещо інші концептуальні підходи до розуміння інформаційної безпеки, а саме:

1) статичний (безпека як стан захищеності інформаційного середовища/інформації, система гарантій тощо);

2) діяльнісний (безпека як процес її забезпечення, здатність держави ефективно захистити національні інтереси й цінності);

3) комплексний (безпека як стан і процес).

Т. Ткачук обґрунтував авторську позицію, що найбільш прийнятним, зважаючи на сучасну практику забезпечення інформаційної безпеки держави, є останній. За такого підходу вбачається за доцільне інформаційну безпеку держави розглядати як перманентний процес діяльності компетентних органів, спрямований на запобігання і протидію загрозам в інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час. Цей підхід базується на принципі, відповідно до якого основною метою забезпечення інформаційної безпеки є створення безпечного інформаційного середовища [5, с. 379].

Як бачимо, поширення набули структурний підхід до розуміння поняття «інформаційна безпека», за яким воно розглядається в контексті національної безпеки як її складник; діяльнісний підхід, що дає змогу розглядати інформаційну безпеку як процес, функцію держави, діяльність органів державної влади; підхід, згідно з яким інформаційна безпека розглядається в статичному стані, як певний стан захищеності чи стан правових норм; підхід, що дає змогу розглядати інформаційну безпеку як суспільні відносини.

П. Демченко розкриває кібернетичну безпеку як новітній напрям інформаційного складника в системі національної безпеки України. На його думку, в основу реалізації концепції кібернетичної безпеки України покладено саме норми Конституції України, що зумовлюється проголошенням захисту незалежності й суверенітету України, прав і свобод людини та громадянина, інтересів суспільства й держави загалом як основоположного завдання держави й обов'язку всього народу України [8].

На наш погляд, у теоретико-правових дослідженнях інформаційної безпеки доцільно її розглядати крізь призму правовідносин, що виникають під час забезпечення стану захищеності інформаційного простору. Отже, інформаційну безпеку можна визначити як правовідносини, що виникають під час здійснення превентивних і захисних заходів в інформаційному середовищі людини, суспільства та держави.

На законодавчому рівні можна зустріти визначення інформаційної безпеки. Так, у ст. 13 Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 № 537-V врегульовано його так: інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства й держави, за якого запобігають заподіянню шкоди через неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання й порушення цілісності, конфіденційності та доступності інформації [9]. У Законі України «Про національну безпеку України» від 21.06.2018 № 2469-VIII зміст інформаційної безпеки не розкривається, вона визнається одним із напрямів державної політики у сфері національної безпеки і оборони. Так само і в Законі України «Про Концепцію Національної програми інформатизації» від 04.02.1998 № 75/98-ВР інформаційна безпека називається невід'ємною частиною політичного, економічного, оборонного та інших складників національної безпеки, але саме поняття не деталізується.

Така термінологічна неоднозначність як на законодавчому рівні, так і на доктринальному рівнях може знизити ефективність заходів протидії руйнівному інформаційному впливу держав-агресорів, не дати належним чином забезпечити інформаційну безпеку, національну, іноді й міжнародну безпеку.

У свою чергу, видається ще більш проблемним визначення іншої досліджуваної нами категорії – інформаційної оборони. Зокрема, С. Соловйов інформаційною обороною називає систему оборони, спрямовану на захист і розвиток інформаційного простору, підвищення готовності Збройних Сил і цивільного населення до інформаційних впливів інших держав незалежно від наявності збройних конфліктів. При цьому він зазначає, що застосовувані нині терміни «інформаційне протиборство», «інформаційна протидія», під якими розуміють реакцію на інформаційні війни, інформаційно-психологічні операції, пропагандистські впливи, сповна не відображають ідеї інформаційної оборони, оскільки названі дії є відповіддю на дії супротивника. Інформаційна оборона передбачає включення інформаційної та віртуальної сфер до системи захисту на одному рівні з фізичною сферою, розрив між якими має бути мінімальний [10].

Інформаційна оборона, на відміну від протиборства, не означає лише реакцію на інформаційну операцію супротивника. Насамперед це готовність до інформаційного нападу, передбачення його основних характеристик (форм, спрямованості, строків). Інформаційна оборона повинна спрямовуватися на зменшення наслідків нападу, в ідеальному випадку на його недопущення, зменшення інтенсивності або використання сил супротивника для заподіяння шкоди йому самому.

У колективній монографії деякі вчені розкривають сутність інформаційної оборони так. Це вид інформаційного захисту, комплекс взаємопов'язаних та узгоджених за метою, завданням, місцем і часом адміністративно-розпорядчих, організаційно-штатних, координаційно-планувальних і техніко-регламентуючих заходів, які спрямовані на підтримання духовного потенціалу суспільства, морально-психологічного стану військ, збереження інформаційно-технічної інфраструктури національної безпеки, ефективної нейтралізації інформаційних атак та операцій противника, завдання максимальної шкоди морально-психологічному стану його суспільству, збройним силам і технічним засобам інформаційного агресії, створення необхідних умов для проведення власної наступальної інформаційної операції [11].

З-поміж принципів інформаційної оборони пропонується виокремити, по-перше, постійність – безперервне здійснення заходів щодо відслідковування дій потенційного суперника у фізичному, інформаційному, віртуальному просторах; розроблення й утілення стратегій впливу на супротивника в інформаційному та віртуальному просторах; підготовки фахівців застосування методів інформаційної роботи; створення цілеспрямованого, узгодженого між органами публічної влади та основними громадськими акторами інформаційного супроводу дій держави; проведення роз'яснювальної роботи з населенням. По-друге, комплексність – узгоджене використання різноманітного інструментарію, каналів, методів тощо для доставки власних смислів і захисту від чужих. Завдяки цьому створюється синергетичний ефект, досягається всеохопність цільових аудиторій, зменшується багатоваріантність сприйняття повідомлення. По-третє, оперативність – швидке реагування в інформаційному просторі на зміни в діях супротивника в усіх трьох просторах (ідеться як про загрози з його боку, так і використання в наших інтересах помилок супротивника, його проблем). Загалом це означає інформаційну перевагу, дає змогу запобігти подальшому просуванню ідей противника, мобілізувати персонал і громадськість до інформаційної оборони, зберегти чи розподілити ресурси. По-четверте, залучення населення – можливість для активної частини населення, лідерів громадськості взяти участь в інформаційно-комунікативній діяльності, наданні та отриманні консультацій, співпраці з військовими та фахівцями [10].

Серед значної кількості завдань інформаційної оборони можна виокремити:

– розвиток вітчизняного інформаційного простору, з відповідними гарантіями його забезпечення, а також включення до системи міжнародного (глобального) інформаційного простору;

– удосконалення законодавчої основи в цій сфері, впровадження передового зарубіжного досвіду й міжнародних стандартів;

– створення дієвих інформаційних і віртуальних продуктів, які б відображали національні інтереси, ідеологію й державну політику;

– інформаційний вплив на населення власної держави та країни-агресора;

– критичне сприйняття інформації, мовлення країн противника, а також тих, які можуть такими стати;

– розширення кола суб'єктів системи забезпечення інформаційної оборони, включаючи громадські інституції, тощо;

– запобігання перешкодам і загрозам і своєчасне усунення перешкод і загроз національній безпеці та обороні держави;

– розвиток національних інформаційних цінностей, патріотичне виховання молоді, підвищення кваліфікації та професіоналізму службовців тощо.

О. Косогов підкреслює значущість інформаційної безпеки як складової воєнної безпеки України, пояснюючи залежністю реалізації найбільш важливих інтересів України у воєнній сфері від інформаційних загроз. З-поміж інших загроз стабілізації воєнно-політичної обстановки та недопущення збройних конфліктів у Центральній Європі розглядаються такі: висунення територіальних претензій до України; втручання у внутрішні справи України; нестабільність воєнно-політичної обстановки навколо України; активізація сепаратистських сил і підтримання їх ззовні; заяви та акції, що дискредитують внутрішню й зовнішню політику України; войовничість політичного керівництва сусідніх країн; загострення міжетнічних і міжконфесійних суперечностей; нестабільність соціально-політичної обстановки в суміжних із Україною країн. Не виникає сум-

ніву, що всі ці загрози тією чи іншою мірою реалізуються на інформаційному рівні. Ідеться не про абсолютизацію інформаційних факторів у реалізації наведених загроз, а про те, що вони поряд з економічними, політичними, соціальними та іншими факторами є домінуючими. Тому ефективність своєчасного виявлення та нейтралізації розглянутих загроз національній безпеці у воєнній сфері істотно залежить від виваженості й активності заходів щодо забезпечення воєнної безпеки на інформаційному рівні. Отже, для ефективного функціонування системи воєнної безпеки України сукупність зазначених організаційно-технологічних та організаційно-правових заходів варто поєднати в систему управління інформаційною безпекою в межах забезпечення воєнної безпеки України [12].

Як бачимо, О. Косогов взаємопов'язано розглядає систему інформаційної безпеки в межах забезпечення воєнної безпеки України. Застосування основних напрямів забезпечення інформаційної безпеки – правового, організаційного, інженерно-технічного тощо – є необхідним для формування комплексної воєнної безпеки держави.

Звісно, така категорія, як «інформаційна оборона», має два змістові складники:

1) її внутрішній складник, що включає власне державу з відповідним населенням та інфраструктурою;

2) її зовнішній складник, який поширюється на керівництво країни-противника, населення країни-противника, міжнародні безпекові інституції та світове співтовариство загалом.

Як зазначалося вище, у Законі України «Про Концепцію Національної програми інформатизації» від 04.02.1998 № 75/98-ВР інформаційна безпека називається невід'ємною частиною політичного, економічного, оборонного та інших складників національної безпеки [13]. Видається, що оборонна та інформаційна безпека є складниками національної безпеки.

Аналіз положень Закону України «Про оборону України» від 06.12.1991 № 1932-XII (у редакції від 03.07.2019) засвідчує підхід законодавця до визначення оборони України як системи політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних, інших заходів держави щодо підготовки до збройного захисту та її захисту в разі збройної агресії або збройного конфлікту [14]. Цим Законом регламентовано основи та принципи національної безпеки і оборони, цілі й основні засади державної політики, що гарантуватимуть суспільству та кожному громадянинові захист від загроз. Водночас ним розмежовано повноваження державних органів у сферах національної безпеки і оборони, визначено систему командування, контролю та координації операцій сил безпеки й сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони, забезпечуючи в такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони.

Остання категорія є результатом новітніх тенденцій законотворчості в Україні, удосконалення національного законодавства з питань національної безпеки (її складника – інформаційної безпеки) та оборони України. Точніше, інформаційна безпека визнається одним із напрямів державної політики у сфері національної безпеки і оборони. Власне така політика підкреслює в черговий раз взаємозалежність і взаємодоповнюваність досліджуваних нами понять.

Висновки. Проведений аналіз теоретичних і законодавчих основ інформаційної безпеки та інформаційної оборони демонструє неоднозначність підходів до їх розуміння, визначення регулювання. На нашу думку, ці категорії мають міждисциплінарну й комплексну природу, свої особливості, спільні та відмінні характеристики, вивчаються вченими в різних науках: політології, військовій науці, державному управлінні, технічній науці та юриспруденції.

Інформаційна безпека спрямована на забезпечення стану захищеності інформаційного простору, передбачає здійснення превентивних і захисних заходів в інформаційному середовищі людини, суспільства та держави. На підставі низки законів, зокрема Конституції України, Законів України: «Про національну безпеку України», «Про Концепцію Національної програми інформатизації», «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», «Про оборону України» тощо, однозначно інформаційна безпека визнається одним із напрямів державної політики у сфері національної безпеки і оборони, невід'ємною частиною політичного, економічного, оборонного та інших складників національної безпеки.

Натомість інформаційна оборона становить систему заходів захисту, інформаційної та віртуальної сфери, що забезпечує готовність до інформаційного впливу, нападу інших держав, захист і розвиток інформаційного простору, підвищення обороноздатності Збройних Сил і цивільного населення до інформаційних атак незалежно від

наявності збройних конфліктів. Вона повинна спрямовуватися на зменшення ймовірності агресії, її недопущення, зменшення інтенсивності або використання сил супротивника для заподіяння шкоди йому самому.

Якщо гарантування інформаційної безпеки держави здійснюється на законодавчому рівні, то забезпечення інформаційної оборони регламентується переважно відомчими нормативними актами. Безперечно, ці категорії потребують подальшого вивчення, аналізу позитивного зарубіжного досвіду запобігання інформаційному протиборству, інформаційним війнам, усунення різного роду інформаційних загроз, безпечного розвитку інформаційного простору на сучасному етапі.

Список літератури:

1. Юридична енциклопедія : у 6 т. / редкол.: Ю.С. Шемшученко (відп. ред.) та ін. Київ: Укр. енциклопедія, 1998–1999. Т. 2 : Д – Й. 744 с.
2. Наливайко Л.Р. Інформаційна безпека та інформаційна політика в Україні: конституційно-правовий аспект. *Вісник Запорізького державного університету*. 2003. № 1. С. 60–65.
3. Харченко Л.С., Ліпкан В.А., Логінов О.В. Інформаційна безпека України: Глосарій / за заг. ред. Р.А. Калюжного. Київ: Текст, 2004. 180 с.
4. Литвиненко О.В. Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії) : автореф. дис. ... канд. політ. наук. Київ, 1997.18 с.
5. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : монографія. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 422 с.
6. Камінська Н.В. Міжнародна інформаційна безпека в умовах глобалізації та інтеграції. *Міжнародне право: виклики сьогодення :* матер. Міжнар. науково-практ. конф. (Київ, 20 грудня 2016 р.) Київ, 2016. С. 22–27.
7. Шемчук В.В. Теоретико-правові засади дослідження інформаційної безпеки. *Європейські перспективи*. 2019. № 2. С. 5–11.
8. Демченко П. Кібернетична безпека як новітній напрям інформаційної складової національної безпеки України: конституційно-правовий аспект. URL: http://publications.lnu.edu.ua/bulletins/index.php/law/article/view/9560.
9. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 № 537-V. URL: http://zakon4.rada.gov.ua/l.
10. Соловйов С.Г. Теоретичні засади інформаційної оборони. *Державне будівництво.* 2015. № 1. URL: http://www.kbuapa.kharkov.ua/e-book/db/2015-1/doc/1/06.pdf.
11. Інформаційна війна і національна безпека : монографія / П.П. Ткачук, Р.В. Гула, О.І. Сивак, О.М. Щурко, В.В. Шемчук. Львів: НАСВ, 2015. 265 с.
12. Косогов О.М. Інформаційна безпека у сфері оборони як складова воєнної безпеки України. *Системи обробки інформації*. 2016. Вип. 8 (145). С. 115–117.
13. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 № 75/98-ВР. URL: http://zakon4.rada.gov.ua/l.
14. Про оборону України : Закон України. *Відомості Верховної Ради України.* 1992. № 9. Ст. 106 (у редакції від 03.07.2019). URL: http://zakon4.rada.gov.ua/laws/show/1932-12.

Shemchuk V.V. INFORMATION SECURITY AND INFORMATION DEFENSE IN THE CONTEXT OF THE DEVELOPMENT OF DOCTRINE AND THE LEGISLATIVE BASIS

Article made the study of theoretical foundations and legislative support for the categories of "information security" and "information defence". Analyzed equipped in doctrine the practice, different approaches to the understanding of the nature and essence of information security, first of all, in legal science, this highlights the peculiar approaches and in other areas of domestic science. Terminology highlights the uncertainty, ambiguity and the intellectual vision of this category. So, according as information security appropriate to examine through the prism of relationships that arise when providing State protection of information space. Justified is the comprehensive understanding of the entity and the State of information security guarantees as the direction of the State policy in the field of national security and defence, an integral part of political, economic, defence and other components national security. This is confirmed by the analysis of the provisions of the Constitution of Ukraine, laws of Ukraine "On the National security of Ukraine", "On the concept of the National programme of informatization", "On the basis of the development of the information society in Ukraine 2007–2015 years of", "On the defence of Ukraine" etc., information security is recognized as one of the directions of the State policy in the field of national security and defence.

Information defense is a system of measures protection of information and virtual spheres, ensuring readiness for information exposure, attack other countries, protection, and development of information space, enhance the capability of the armed forces and the civilian population to information attacks regardless of the presence of armed conflicts. On the legislative level in Ukraine divine the powers of the State authorities in the areas of national security and defence, determine the henault systems in command, control and coordination of the operations of the security forces and Defence force, introduced a comprehensive approach to planning in the areas of national security and defence, ensuring in this way democratic civilian control over bodies and Security and defence sector groups.

Marked by interdependence of concepts, their overall focus on ensure State security, preventive and protective measures, information security threats and to ensure the safe development of the national information space at the present stage.

Key words: *information security, information defense, information policy, information space, defense, legal basis.*