УДК 351.86

к.т.н. **Саєнко О.Г**(ВІТІ ім. Героїв Крут)
к.т.н., доц. **Шаціло П.В.** (ВІТІ ім. Героїв Крут)

DOI: https://doi.org/10.17721/2519-481X/2022/74-11

ІНСТИТУЦІОНАЛЬНЕ УПРАВЛІННЯ ОРГАНІЗАЦІЙНОЮ КОМПОНЕНТОЮ ОБ'ЄКТА ВІЙСЬКОВОЇ СФЕРИ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

Досягнення науково-технічного прогресу, особливо в галузі інформаційних технологій, суттєво впливають на розвиток економічної, соціальної, військової, культурної та інших сфер суспільства. Разом із тим інформаційні технології виступають як джерела розвитку, так і джерела загроз такому розвитку та діяльності суспільства взагалі.

Національна безпека являє собою складну багаторівневу функціональну систему, в якій безперервно відбуваються процеси взаємодії та протиборства інтересів держави, суспільства та особистості із загрозами цим інтересам – як внутрішніми, так і зовнішніми. Як цільова функція цієї системи виступає ступінь захищеності цих інтересів від загроз. Для організації захисту інформаційного простору держави необхідно розробляти шляхи протидії інформаційним агресіям з боку тих чи тих суб'єктів: зовнішнього агресора, іноземних спецслужб, транснаціональних компаній, кримінальних кланів тощо.

У статті розглянуто актуальну проблему управління організаційними компонентами об'єктів військової сфери в умовах інформаційної боротьби та реалізації механізмів інституціонального управління цими компонентами. Досягнення теорії організаційного управління і структурного системного аналізу дають змогу з площини декларацій про наміри інформаційної безпеки воєнних і оборонних об'єктів перейти в практичну площину розробки механізмів функціонування організаційними компонентами органів військового управління і механізмів управління ними та їх впровадження в процес функціонування системи управління інформаційною безпекою.

Ключові слова: інформаційне протиборство, інформаційна безпека, інформаційна війна, організаційна компонента, інституціональне управління.

Вступ та аналіз останніх досліджень. Сьогодні досягнення науково-технічного прогресу, особливо в галузі інформаційних технологій, суттєво впливають на розвиток економічної, соціальної, військової, культурної та інших сфер суспільства. Але разом із тим інформаційні технології виступають як джерела розвитку, так і джерела загроз такому розвитку та діяльності суспільства взагалі.

Як показує досвід останніх років, жодна держава не в змозі захистити себе, використовуючи лише військово-технічні засоби. Безпека дедалі більше стає комплексним завданням, яке включає політичні, економічні, інформаційні та інші заходи. Успішно виконувати це завдання можливо лише завдяки оптимальному застосуванню усіх форм та засобів протиборства, включаючи й інформаційне. В багатьох державах відбувається об'єднання в одне ціле сил та засобів інформаційно-психологічного впливу, призначених для досягнення воєнних, ідеологічних і політичних цілей; розвивається велика кількість концепцій формування політики національної безпеки.

Україна, як молода європейська держава, яка намагається стати рівноправним членом світової спільноти, також мусить дбати про захищеність свого інформаційного простору. Для цього необхідно на державному рівні розробляти шляхи протидії інформаційним агресіям із боку тих чи тих суб'єктів: зовнішнього агресора, іноземних спецслужб, транснаціональних компаній, кримінальних кланів тощо.

Цілком очевидно, що національна безпека являє собою складну багаторівневу функціональну систему, в якій безперервно відбуваються процеси взаємодії та протиборства інтересів держави, суспільства та особистості із загрозами цим інтересам – як внутрішніми,

так і зовнішніми. Як цільова функція цієї системи виступає міра захищеності цих інтересів від загроз.

Питання протидії інформаційним загрозам розглядались у роботах торського колективу Національного інституту стратегічних досліджень за редакцією В. Горбуліна [1], В. Кротюка [2], В. Алещенко [3], В. Антипенка [4], В. Богуша, О. Юдіна [5] та інших.

Інформаційна безпека (ІБ) як одна із складових національної безпеки держави являє собою стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через [6]:

– неповноту, невчасність та недостовірність інформації;

– негативний інформаційний вплив;

– негативні наслідки застосування інформаційних технологій;

– несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Складовими ІБ, які водночас є характеристиками основних властивостей інформації, як об’єкта захисту є:

– конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем;

– цілісність – означає неможливість модифікації неавторизованим користувачем;

– доступність – властивість інформації бути отриманою авторизованим користувачем, за наявності у нього відповідних повноважень, в необхідний для нього час.

Елементами системи забезпечення ІБ (у вузькому розумінні) є (рис. 1):

– нормативно-правові акти (НПА), які регламентують суспільні відносини в інформаційній сфері та встановлюють юридичні взаємовідносини;

– державні та недержавні організації, які забезпечують продукцією ринок інформаційних послуг;

– сукупність спеціально уповноважених органів держави, які контролюють дотримання інформаційного законодавства;

Практична діяльність зазначених суб’єктів, спрямована на розвиток вітчизняного інформаційного простору.

У цьому контексті ІБ потребує свого забезпечення на державному рівні.

У широкому розумінні до системи забезпечення ІБ необхідно віднести: Верховну Раду України; Президента України; регуляторні та контролюючі державні органи; споживачів інформації та інших суб’єктів.

Правове регулювання у сфері інформаційної безпеки буде тією чи іншою мірою стосуватися закріплених у Конституції прав особи на інформацію, положень про демократичний устрій, плюралізм думок тощо, законодавства про інформацію, про забезпечення національної (державної) безпеки, охорону державної та комерційної таємниці, діяльність засобів масової інформації, інтернету, а також питань захисту інформації з обмеженим доступом [7].

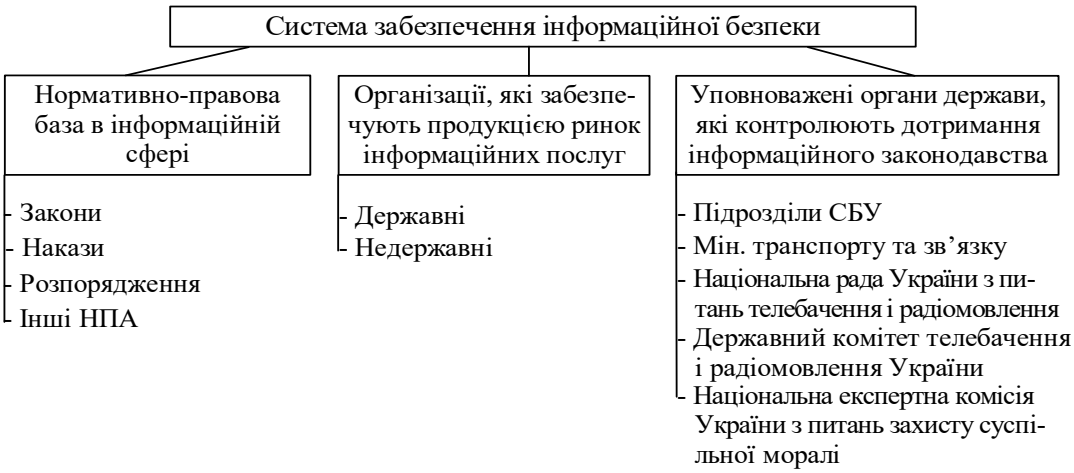

Рисунок 1 – Елементи системи забезпечення інформаційної безпеки

Слід зазначити, що на сьогодні у науковій літературі поки бракує єдиного погляду на зміст поняття «інформаційна безпека», а також не вироблено єдиного методологічного погляду до оцінки такого явища, як «інформаційна безпека суспільства». Так, існує твердження, що інформаційна безпека – це сукупність суспільних відносин, які забезпечують безпечні умови життя кожного члена суспільства, громадський порядок, безпеку державних, громадських чи особистісних інтересів [8].

Однак, не зважаючи на відсутність єдиного визначення поняття ІБ, значимість інформаційно-комунікаційних процесів у сучасному світі дає підстави розглядати забезпечення ІБ як одне з глобальних і пріоритетних завдань політики національної безпеки сучасної держави. У цілому ця політика повинна бути спрямована на мінімізацію або уникнення чинних чи потенційних внутрішніх або зовнішніх загроз ІБ держави у відповідності з цілями її розвитку [9].

В Указі Президента України «Про Доктрину інформаційної безпеки України» зазначається, що забезпечення інформаційної безпеки України має здійснюватися за такими принципами:

– свобода збирання, зберігання, використання та поширення інформації;
– достовірність, повнота та неупередженість інформації;
– обмеження доступу до інформації виключно на підставі закону;
– гармонізація особистих, суспільних і державних інтересів;
– запобігання правопорушенням в інформаційній сфері;
– економічна доцільність;
– гармонізація українського законодавства в інформаційній сфері з міжнародним;
– пріоритетність національної інформаційної продукції.

Прийняття Доктрини інформаційної безпеки закріпило офіційну систему поглядів на зміст стратегічних національних інтересів України в інформаційній сфері, погроз цим інтересам, методи протидії погрозам і систему забезпечення ІБ в довгостроковій перспективі [9]. Доктрина створила політичну основу узгодження діяльності органів державної влади з реалізації національних інтересів в інформаційній сфері й захисті їх від зовнішніх і внутрішніх погроз. Але оскільки навіть на принциповому рівні Доктрину ІБ не можна вважати цілком реалізованою, то це веде до досить критичних оцінок інформаційної політики і, водночас, діяльності держави як суб'єкта розвитку інформаційних відносин і забезпечення ІБ.

У свою чергу загрози національній безпеці України в інформаційній сфері представляють собою сукупність умов та чинників, які становлять небезпеку життєво важливим інтересам держави, суспільства й особи у зв'язку з можливістю негативного інформаційного впливу на свідомість та поведінку громадян, а також інформаційні ресурси та інформаційно-технічну інфраструктуру.

На сьогодні існує цілий комплекс інформаційних загроз, починаючи від відсутності яскравої ідентифікації України у глобальному інформаційному просторі та чіткої стратегії входження в світове інформаційне суспільство і закінчуючи ІБ окремо взятого громадянина [9].

Так, згідно з Законом України „Про основи національної безпеки України" [10] основними реальними та потенційними загрозами національній безпеці України в інформаційній сфері є:

– прояви обмеження свободи слова та доступу громадян до інформації;

– поширення засобами масової інформації культу насильства, жорстокості, порнографії;

– комп'ютерна злочинність та комп'ютерний тероризм;

– розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Однак, деякі автори [11, 12] доповнюють цей перелік загроз, відносячи до нього наступні загрози національній безпеці України в інформаційній сфері:

– розповсюдження ідей, що провокують конфлікти на національному, релігійному і соціальному ґрунті та масові заворушення, а також розпалення серед українського населення ідей сепаратизму;

– заклики щодо посягання з боку окремих груп та осіб на державний суверенітет, територіальну цілісність, економічний, науково-технічний і оборонний потенціал нашої держави;

– проведення на шкоду інтересам України спеціальних інформаційних операцій та актів зовнішньої інформаційної агресії;

– комп'ютерна злочинність;

– інформаційний тероризм;

– розвідувально-підривна діяльність іноземних спеціальних служб;

– розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– дискредитація політики держави та авторитету окремих державних діячів;

– прояви обмеження свободи слова і доступу громадян до інформації та інших їхніх прав і свобод;

– поширення ЗМІ культу насильства, жорстокості та інших проявів аморальності;

– намагання маніпулювати громадською думкою, зокрема шляхом поширення недостовірної, неповної або упередженої інформації;

– значний обсяг іноземної присутності в інформаційному просторі України;

– небезпечне для економічної незалежності України зростання частки іноземного капіталу у стратегічних галузях економіки, пов'язаних з інформаційною сферою;

– науково-технологічне відставання України від розвинутих країн;

– низька конкурентоспроможність продукції з обслуговування інформаційної сфери;

– нерозвиненість внутрішнього ринку високотехнологічної продукції та відсутність його ефективного захисту від іноземної технічної і технологічної експансії;

– зниження внутрішнього попиту на підготовку науково-технічних кадрів для наукових, конструкторських, технологічних установ та високотехнологічних підприємств, незадовільний рівень оплати науково-технічної праці, падіння її престижу, недосконаліть механізмів захисту прав інтелектуальної власності;

– відтік учених, фахівців, кваліфікованої робочої сили за межі України;

– інспірування інших деструктивних процесів в інформаційній сфері нашої держави.

Діяльність держави та її органів у сфері забезпечення ІБ є багатогранною: це захист державних секретів, дотримання та охорона конституційних прав громадян в інформаційній

сфері тощо. Через те організація діяльності держави щодо гарантування ІБ – це послідовний безперервний процес, спрямований на розробку і здійснення правових, організаційних, технічних та інших заходів у цій сфері. Крім цього, ІБ повинна забезпечуватися шляхом проведення цілісної державної програми відповідно до Конституції, чинного законодавства України та норм міжнародного права шляхом реалізації відповідних доктрин, стратегій, концепцій і програм, що стосуються національної інформаційної політики України [13].

На законодавчому рівні основні напрями державної політики з питань національної безпеки в інформаційній сфері визначені у Законі України «Про основи національної безпеки України»:

– забезпечення інформаційного суверенітету України;

– вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

– активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України;

– забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;

– вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Враховуючи практичну складову сьогодення слід зазначити, що, ІБ, як поняття в ході проведення відкритого протистояння або актів зовнішньої інформаційної агресії, набуває нових форм та методів поширення та застосування. Так аналіз бойових дій на сході України, вказує на використання інформаційних операцій для порушення ІБ держави. В ході воєнних дій інформаційна операція відбувається шляхом залучення множини інформаційних атак різного виду та напрямків. Метою таких атак може бути: порушення захищеності інформаційних, програмних та апаратних компонентів інформаційного простору, а також свідомість і психіка особового складу, який бере участь у воєнних діях.

У свою чергу спеціальні інформаційні операції та акти зовнішньої інформаційної агресії поділяються на такі види:

– направлені проти суб’єктів, що беруть участь у підготовці і прийнятті рішень;

– направлені на компрометацію та розповсюдження деструктивних дій щодо опонентів;

– направлені на політичну, економічну та іншу дестабілізацію.

З метою здійснення та реалізації деструктивних дій під час інформаційної агресії можуть застосовуватись методи дезінформації, пропаганди, диверсифікації суспільної думки, психологічного тиску, поширення слухів та міфів.

Загалом у військовій сфері виділяють два види інформаційної боротьби: інформаційно-технічний та інформаційно-психологічний.

У свою чергу у військовій та оборонній сфері об’єктами інформаційної зброї є: інформаційні ресурси стратегічного управління, науково-дослідні підрозділи військової галузі, системи зв’язку та управління військами, інформаційне забезпечення, інформаційні інфраструктури, морально-психологічний стан військ [14]. Перший вид інформаційної боротьби направлений на інформаційно-технічну інфраструктуру (інформаційні, інформаційно-телекомунікаційні системи, автоматизовані системи класу 1,2,3, радіоелектронні засоби) та інформаційний ресурс цих об’єктів, а другий вид інформаційної боротьби спрямовується на їх організаційні компоненти (як об’єднання оперативного складу, що бере участь у підготовці прийняття рішень).

Інформаційна боротьба під час протистояння ведеться на стратегічному, оперативному та тактичному рівнях. На стратегічному рівні інформаційне протистояння планують та координують вищі органи державної влади. На оперативному та тактичному рівнях ця діяльність здійснюється силами та засобами збройних сил, спеціальних служб, а також суспільно-політичними інститутами держави. Таким чином, інформаційна боротьба, об'єктами якої є військові формування та підрозділи (військові об'єкти), ведеться на оперативно-тактичному рівні.

Найбільш вагомим інструментом сучасної інформаційної боротьби з противником є інформаційна зброя. У сучасному світі за допомогою інформаційної зброї супротивники здатні вирішувати стратегічні завдання: здійснювати вплив на державні інтереси; дискредитувати органи влади; провокувати ворожість на суспільному ґрунті та інше.

Множина проблем в управлінні ІБ об'єктів військової сфери виникає через те, що за декларацією цілей ІБ йде низка дій і заходів, які мають віддалене відношення до цих цілей. У масштабах держави це проявляється, наприклад, у тому, що закони, які приймаються, не працюють, в масштабах, наприклад, об'єкта інформаційної боротьби в тому, що розпорядження керівництва призводять до результатів, які прямо протилежні запланованим. Причина полягає у тому, що мало прийняти закон чи розпорядження – необхідно розробити і запровадити механізми їх реалізації.

Стосовно організаційного компонента (ОК) органу управління військовим об'єктом такими механізмами є:

– механізми управління ОК (як сукупність процедур підготовки і прийняття рішень);

– механізми функціонування ОК (як сукупність правил і процедур, які регламентують взаємодію оперативного складу);

– моделі об'єкта, яким управляють.

Ці механізми використовує система управління інформаційною безпекою (СУІБ) військового об'єкта в процесі виконання покладених на неї завдань.

Методи і алгоритми рішення задачі синтезу оптимального механізму функціонування ОК характеризуються високою структурною і обчислювальною складністю [15]. Тому пропонується для побудови механізмів функціонування ОК застосувати наступні складові методології структурного аналізу і моделювання IDEF (IntegratedDefinition-цілісна точність) [10], яка базується на принципах системного аналізу:

– IDEF0 (FunctionModeling) методологія функціонального моделювання;

– IDEF1 (InformationModeling) методологія моделювання інформаційних потоків в середині системи;

– IDEF3 (ProcessDescriptionCapture) методологія документування технологічних процесів, які мають місце в системі. Має безпосередній зв'язок з методологією IDEF0;

– IDEF5 (OntologyDescriptionCapture) методологія онтологічного дослідження складних систем. За допомогою IDEF5 онтологія системи може бути описана термінами і правилами, на базі яких формуються достовірні твердження про стан системи в деякий момент часу та висновки про подальший її розвиток;

– DFD (DataFlowsDiagrams) методологія структурного аналізу систем, яка дозволяє описати зовнішні по відношенню до системи джерела і адреси, логічні функції, потоки і сховища даних, до яких система здійснює доступ.

Оскільки в процесі інформаційної боротьби ОК органу управління військового об'єкта знаходиться під інформаційним впливом 2-го виду, то управління інформаційною безпекою доцільно представити як управління наступних типів [16,17]:

– управління складом ОК;

– управління структурою ОК;

– інституціональне управління ОК;

– мотиваційне управління ОК;

– інформаційне управління ОК.

Інституціональне управління ОК можна визначити як управління обмеженнями і нормами діяльності осіб оперативного складу (агентів), які беруть участь у підготовці прийняття рішень. Сутність його полягає в тому, що СУІБ обмежує множину можливих дій і результатів діяльності членів ОК. Таке обмеження може здійснюватися правовими актами, директивами, наказами, розпорядженнями, нормами (у тому числі морально-етичними нормами), посадовими інструкціями та інше. Прийнято явні норми діяльності (наприклад, закони, накази, директиви, посадові інструкції) називати обмеженнями діяльності, а неявні норми (морально-етичні норми, службова етика) – спонукальними нормами діяльності.

У теорії управління соціальними системами моделі управління спонукальними нормами діяльності агентів практично не розглядались. Окремі моделі управління обмеженнями діяльності агентів розглянуті в роботі Новикова Д.А., Смирнова И.А., Шохиної Т.Е. «Механизмы управления динамическими активными системами», в якій множина допустимих дій агента залежить від параметра, який вибирає центр (у нашому випадку – СУІБ).

Задача обмеження діяльності осіб оперативного складу ОК органу управління об'єкта військового призначення, що діє в умовах інформаційної боротьби, може бути сформульована таким чином.

Задано:

– універсальна множина X дій агента;

– агент вибирає таку дію із множини A своїх допустимих дій, яка максимізує його цільову функцію $f(y)$, тобто $C(f,A) = Arg\max f(y);\ y \in A$.

Необхідно:

СУІБ вибрати обмеження $B \le X$ множини допустимих дій агента при умові, що агент вибере дію (діяльність) із множини: $C(f,B) = Arg\max f(y);\ y \in B$.

Нехай переваги СУІБ в такий момент інформаційної боротьби задані функціоналом $\Phi(y,A)$, який дає змогу порівнювати пари «дії агента-множина допустимих дій агента». Якщо вважати, що функціонал $\Phi(y,B)$ не залежить від множини B допустимих дій агента (тобто – введення тих чи тих обмежень дій агента не потребує від СУІБ відповідних затрат), то задача інституціонального управління ОК вироджується: СУІБ достатньо вибрати $B = \{x\}$,

де $x = Arg\max \Phi(y);\ y \in X$.

Висновки. Таким чином досягнення теорії організаційного управління і структурного системного аналізу дають змогу з площини декларацій про наміри інформаційної безпеки воєнних і оборонних об'єктів перейти в практичну площину розробки механізмів функціонування організаційними компонентами органів військового управління і механізмів управління ними та їх впровадження в процес функціонування СУІБ.

Враховуючи вказане, актуальним питанням залишається проведення оцінки ефективності використання методів, засобів, способів, підходів та механізмів забезпечення рівня ІБ, що повинне ґрунтуватися на аналізі вразливостей системи безпеки, загроз системі безпеки, ризиків здійснення порушень та інше.

Саме тому сучасний стан забезпечення національної та ІБ України в цілому, та об'єктів військової сфери, зокрема, потребує розробки науково обґрунтованої державної політики та стратегії в цій галузі, визначення системи національних цінностей, життєво важливих інтересів особистості, суспільства та держави, визначення зовнішніх і внутрішніх загроз цим інтересам, пошуку ефективних заходів для гарантування безпеки в усіх її сферах.

Отже, в умовах стрімкого розвитку інформаційних технологій, досягнень теорії організаційного управління та структурного системного аналізу, ефективний розвиток підходів у забезпеченні ІБ вимагає розробки не тільки різних методів протидії інформаційним агресіям з боку тих чи тих суб'єктів, а і розробки механізмів функціонування та управління

організаційними компонентами, які беруть участь у підготовці прийняття рішень і самі знаходяться під постійним впливом інформаційного тиску.

Можливими шляхами удосконалення державного управління забезпеченням ІБ можуть бути такі: удосконалення нормативно-правової бази; створення умов для ефективної участі України в міжнародному інформаційному обміні в межах єдиного інформаційного простору світу; унеможливлення поширення спеціальних технічних засобів прихованого отримання інформації; наукове обґрунтування шляхів та механізмів забезпечення ІБ України, оцінка сучасних методів ведення конфліктів та інше.

ЛІТЕРАТУРА:

1. Світова гібридна війна: український фронт / За заг. ред. В.П. Горбуліна. Національний інститут стратегічних досліджень. – К.: НІСД, 2017. – 496 с.

2. Війни інформаційної епохи: міждисциплінарний дискурс: монографія / за ред. В.А. Кротюка. Харків: ФОП Федорко М. Ю., 2021. 558 с.

3. Алещенко В. Інформаційно-психологічний вплив у ході збройної боротьби. Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. 2018. Вип. 1. С. 6-10.

4. Антипенко І.В. Гібридна війна в Україні як ризикоутворюючий чинник глобалізації. Ефективність державного управління. 2020. Вип. 4 (1). С. 13-26.

5. Богуш В., Юдін О. Інформаційна безпека держави. Київ : МК-Прес, 2005. 432 с.

6. Закон України „Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки”, від 09.01.2007 № 537-V [Електронний ресурс] / Верховна Рада України: Законодавство України. – Назва з титул. екрану. – Режим доступу до інформації: http://zakon.rada.gov.ua.

7. Конституція України від 28.06.1996 [Електронний ресурс] / Верховна Рада України: Законодавство України. – Режим доступу до інформації: http://zakon.rada.gov.ua.

8. Ліпкан В.А. Національна безпека України: [навч. посіб.] / В.А. Ліпкан. – [2-е вид.]. – К.: КНТ, 2009. – 576 с.

9. Указ Президента України „Про Доктрину інформаційної безпеки України” від 08.07.2009 № 514/2009 [Електронний ресурс] / Верховна Рада України: Законодавство України. – Назва з титул. екрану. – Режим доступу до інформації: http://zakon4.rada.gov.ua/laws/show/514/2009.

10. Закон України „Про основи національної безпеки України”, від 19.06.2003 № 964-IV [Електронний ресурс] / Верховна Рада України: Законодавство України. – Назва з титул. екрану. – Режим доступу до інформації: http://zakon.rada.gov.ua/go/964-15.

11. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / Петрик Валентин // Юридичний журнал. – 2009. – № 5. – Назва з титул. екрану. – Режим доступу до журналу: http://justinian.com.ua/article.php? id=3222.

12. Галамба М. Інформаційна безпека України: поняття, сутність та загрози [Електронний ресурс] / Галамба Микола // Юридичний журнал. – 2006. – № 11. – Назва з титул. екрану. – Режим доступу до журналу: http://justinian.com.ua/article.php?id=2463.

13. Соціально-правові основи інформаційної безпеки: Навч. посіб. / [Петрик В.М., Кузьменко А.М., Остроухов В.В. та ін.]; за ред. В.В. Остроухова. – К.: Росава, 2007. – 496 с.

14. Информационно-психологическаябезопасность в епоху глобализации: Учебноепособие / [Петрик В.М., Остроухов В.В., А.А. Штоквиш та ін.]; под ред. В.В. Остроухова. – К., 2008. – 544 с.

15. Методологія аналізу, моделювання та проектування систем і процесів IDEF: Навч.посібникґ/ П.В.Шаціло, В.В.Цуркан.: Вид-во ІСЗЗІ НТУУ „КПІ” 2011-146 с.

16. Новиков Д.А. Теорияуправленияорганизационными системами. М.: МПСИ. – 2005.– 584 с.

17. Психологическиепроблемыдеятельности в особыхусловиях / Под ред. Б.Ф. Ломова, Ю.Н. Забродина – М.: Наука, 1985. – 232 с.

REFERENCES:

1. V.P. Gorbulin, Svitovagibrydnaviina: Ukrainskii front. [World Hybrid War: the Ukrainian front] /ed. By V.P Gorbulin. National Institute for Strategic Studies. - K .:NISD, 2017. - 496 p.

2. V.A. Krotuk, Viinyinformatsiinoiepokhy: mizhdystsyplinarnyidyskurs: monographiia. [Wars of the information age: interdisciplinary discourse: a monograph] / ed. by V.A. Krotuk. Kharkiv: FedorkoM .FOP., 2021. 558 p.

3. V. Aleshchenko. Information and psychological influence during the armed struggle. Bulletin of the Taras Shevchenko National University of Kyiv. Military special sciences. 2018. Ed. 1. pp. 6-10.

4. I.V. Antipenko, Ukrainian hybrid war as a risk factor for globalization. Efficiency of public administration. 2020. Vip. 4 (1). pp. 13-26.

5. V. Bogush, O. Yudin, Information security of the state. Kyiv: MK-Press, 2005. 432 p

6. Law of Ukraine "Basic Principles of Information Society Development in Ukraine for 2007-2015", ed. 09.01.2007 № 537-V [Electronic resource] / The VerkhovnaRada of Ukraine: Legislation of Ukraine. Link: http://zakon.rada.gov.ua

7. Constitution of Ukraine of 28.06.1996 [Electronic resource] / VerkhovnaRada of Ukraine: Legislation of Ukraine. - Link: http://zakon.rada.gov.ua.

8. Lipkan V.A. NatsionalnabezpekaUkrainy [National Security of Ukraine]: [textbook. aid.] / V.A. Lipkan. - [2nd ed.]. - K .: KNT, 2009. - 576 p.

9. Decree of the President of Ukraine "Doctrine of Information Security of Ukraine" of 08.07.2009 № 514/2009 [Electronic resource] / The VerkhovnaRada of Ukraine: Legislation of Ukraine. - Link: http://zakon4.rada.gov.ua/laws/show/514/2009.

10. Law of Ukraine "Fundamentals of National Security of Ukraine", dated 19.06.2003 № 964-IV [Electronic resource] / The VerkhovnaRada of Ukraine: Legislation of Ukraine. - Title with title. screen. - Mode of access to information: http://zakon.rada.gov.ua/go/964-15.

11. Petryk V. The essence of information security of the state, society and person [Electronic resource] / PetrykValentyn // Legal magazine. - 2009. - № 5. - Link: http://justinian.com.ua/article.php? id = 3222.

12. Galamba M. Information security of Ukraine: concept, essence and threats [Electronic resource] / GalambaMykola // Legal magazine. - 2006. - № 11. – Link: http://justinian.com.ua/article.php?id=2463.

13. Sotsialno-pravovi osnovy informatsiinoi bezpeky [Socialand legal foundations of information security]: Trainingmanual. / [PetrikV.M, KuzmenkoA.M, OstroukhovV.Vetc.]; fored. V.V. Ostroukhova. – K. Rosava, 2007. - 496 p.

14. Informatsionno-psikhologicheskaia bezopasnost v epokhy globalizatsii [Informational and psychological security intheera of globalization]: Trainingmanual / [PetrikV.M., OstroukhovV.V., A.A. Stockvishandin.]; ed. V.V. Ostroukhova. - K., 2008, 544 p.

15. Metodologiia analizu, modeliuvannia system Iprotsesiv IDEF[Methodology of analysis, modeling and designof IDEFsystem sandprocesses]: Trainingmanual / PVShatsilo, VVTsurkan .: Publishing house ISZZINTUU "KPI"2011-146 p.

16. Novikov DA Teoriia upravleniia organizatsionnymi sistemami [Theory of organizational systems management]. M .: MPSI. - 2005.– 584 p.

17. Psikhologicheskii problemy deiatelnosti v osobykh usloviiakh [Psychological problems of activity in special conditions] / Ed. B.F. Lomova, Yu.N. Zabrodina - M .: Nauka, 1985. - 232 p.

PhD Saienko O.G., PhD Shatsilo P.V.

INSTITUTIONAL MANAGEMENT ORGANIZATIONAL COMPONENT OF OBJECT MILITARY SPHERE IN CONDITIONS INFORMATION WARFARE

Achievements of scientific and technological progress, especially in the information technology field, significantly affect the development of economic, social, military, cultural and other spheres of society. But at the same time, information technology acts as a source of development and a source of threats to this development and society in general. National security is a complex multilevel functional system with continuous processes of interaction and confrontation of state, society and the individual interests with threats to them - both internal and external. The purpose of this system is to protect these interests from threats. In order to organize the protection of the state information space, it is necessary to develop ways to counter information aggression by certain entities: external aggressors, foreign intelligence services, multinational companies, criminal clans, etc.

The article considers the topical problem of management of organizational components of military facilities in the conditions of information struggle and implementation of mechanisms of institutional management of these components. Advances in the theory of organizational management and structural systems analysis allow us to move from the plane of declarations of intent of information security of military and defense facilities to the practical plane of developing mechanisms for functioning of organizational components of military management and management mechanisms and their implementation in the information security management system.

Keywords: information confrontation, information security, information warfare, organizational component, institutional management.