АДМІНІСТРАТИВНЕ ТА ІНФОРМАЦІЙНЕ ПРАВО

УДК.342.355.01.08

В. Л. Ортинський
директор Навчально-наукового інституту права та психології
Національного університету "Львівська політехніка"
д-р юрид. наук, професор

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ: ПРАВОВИЙ ТА СОЦІОЛОГІЧНИЙ АСПЕКТИ

Розгляунто питання підвищення ефективності забезпечення інформаційної безпеки у Збройних силах України з позиції адміністративно-правового та соціологічного аспектів. Розглянуто управління забезпеченням інформаційної безпеки, особливості інформаційного впливу на військовослужбовців, зв'язок з боєздатністю військових колективів, модель оптимізації адміністративно-правового регулювання інформаційної безпеки у Збройних силах, системне застосування методів інформаційно-аналітичної роботи, їх взаємозв'язок.

Ключові слова: інформаційна безпека, Збройні сили, інформаційний вплив, інформаційна безпека військовослужбовця.

В. Л. Ортынский

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВООРУЖЕННЫХ СИЛАХ УКРАИНЫ: ПРАВОВОЙ И СОЦИОЛОГИЧЕСКИЙ АСПЕКТЫ

Рассмотрены вопросы повышения эффективности обеспечения информационной безопасности в Вооруженных силах Украины с позиции административно-правового и социологического аспектов. Рассмотрены управление обеспечением информационной безопасности, особенности информационного воздействия на военнослужащих, связь с боеспособностью воинских коллективов, модель оптимизации административно-правового регулирования информационной безопасности в Вооруженных силах, системное применение методов информационно-аналитической работы, их взаимосвязь.

Ключевые слова: информационная безопасность, Вооруженные силы, информационное воздействие, информационная безопасность военнослужащего.

V. L. Ortynsky

THE PROBLEMS OF INFORMATION SECURITY IN THE ARMED FORCES OF UKRAINE IN THE LEGAL AND SOCIOLOGICAL ASPECTS

The article raises questions efficiency of information security in the Armed Forces of Ukraine from the standpoint of administrative, legal and sociological aspects. We consider information security management, particularly the impact of information on military personnel, communication with the combat capability of military groups, model optimization

administrative and legal regulation of information security in the Armed Forces, systemic application of methods of information-analytical work, their relationship.

Key words: information security, military, informational influence, information security serviceman.

Постановка проблеми. Сепаратизм та військова агресія на сході України створюють реальну загрозу національній безпеці держави, що своєю чергою потребує наукового аналізу на удосконалення діяльності структур, які забезпечують захист територіальної цілісності держави. У військових формуваннях розвинених країн світу триває активний розвиток і використання потенціалу сучасних інформаційних технологій під час забезпечення боєготовності військ. У Збройних силах НАТО є підрозділи з функціями протидії інформаційного впливу ворога та забезпечення інформаційної безпеки військовослужбовців. Між процесом управління військами і інформаційною безпекою військовослужбовців існує взаємозв'язок: чим вищий рівень безпеки, тим вищий рівень керованості.

Завдяки науково-технічному потенціалу і інтенсивному розвитку інформаційно-комунікативних мереж інформація може мати і позитивний, і негативний вплив не тільки на політичне мислення, спільність, культуру суспільства, а й на інформаційне середовище військовослужбовців. У зв'язку з цим, одним з перспективних напрямків досліджень у військовій галузі стають розробки концепцій переходу від керованої зброї до керованих конфліктів з нарощуванням інформаційної складової. Однак Україна, опинившись перед небезпекою невідворотного інформаційного впливу, починає вживати відповідних заходів. Питання інформаційної безпеки у правовому та соціологічному аспектах, особливо пошук засобів і шляхів управління нею, набувають важливого значення.

Ступінь наукової розробленості проблеми. Проведений аналіз спеціальної літератури дає змогу зробити висновок, що сучасне інформаційне право має достатню теоретико-методологічну та інформаційно-статистичну базу. Дослідження у сфері інформаційної безпеки у Збройних силах доцільно розділити на п'ять груп. Першу групу об'єднують результати дослідницької діяльності вчених з виявлення загальних принципів і методів наукового аналізу інформаційної безпеки. До другої групи входять дослідники нормативно-правового регулювання діяльності телекомунікаційних систем. Третю групу утворюють вчені, які вивчали окремі проблеми управління інформаційною безпекою у військовому середовищі. Четверта група складається з учених, що розробляють методологічний і категоріально-понятійний апарат під час дослідження інформаційних процесів. П'ята група представлена зарубіжними вченими, які вивчали природу інформації, розробляли теорії створення інформаційного суспільства. Значний внесок у розвиток досліджуваної проблеми зробили: В. Гавловський, В. Гриценко, Р. Калюжний, Б. Кормич, А. Марущак, П. Мельник, В. Цимбалюк, М. Швець, У. Ліппман, М. Мак-Люен, Р. Райх, Е. Тофлер, К. Уайнбергер, Ф.Уебстер, К. Шеннон, П. Швейцер та інші.

Мета дослідження – на основі аналізу функціонального стану адміністративно-правового управління інформаційною безпекою в Збройних силах розглянути напрями оптимізації.

Виклад основного матеріалу. Узагальнення вітчизняного та зарубіжного досвіду вивчення інформаційної безпеки та управління нею дали змогу розглядати управління інформаційною безпекою в Збройних силах як систематичний вплив на інформаційне середовище формуванням інформаційного поля з метою регулювання якості інформаційних потоків, які дозволяють успішно виконувати поставлені завдання, враховуючи реальну обстановку.

Вивчаючи теоретико-методичні підходи щодо наукового дослідження адміністративно-правового управління інформаційною безпекою загалом та в конкретних соціальних умовах – ведення бойових дій на сході держави та розвитку Збройних сил інтерпретується як системний процес, що передбачає організаційно-управлінський і правово-інформаційний компоненти, має складну структуру взаємопов'язаних елементів, які безпосередньо і опосередковано впливають на суспільні відносини. Можливість реалізації управління інформаційною безпекою військово-службовців збільшується переважно в умовах розширення інформатизації суспільства, яка стала атрибутом високорозвинених країн.

Інформаційна модель діяльності органів управління щодо формування інформаційної безпеки військовослужбовців являє собою, з позиції структурно-функціонального підходу, сукупність взаємопов'язаних напрямів, які об'єднують: облік і корекцію зовнішнього інформаційного середовища; формування інформаційного поля в Збройних силах; забезпечення інформаційної безпеки та мінімізацію незахищеності військовослужбовців; створення можливостей задоволення потреб військовослужбовців.

Зміст правового забезпечення інформаційної безпеки становлять: система понять інформаційної сфери, механізми виявлення ознак виникнення правовідносин, які підлягають регулюванню, закономірності формування нормативної бази правового забезпечення інформаційної безпеки в умовах ведення бойових дій та способи їх аналізу; теоретичний аналіз сукупності норм позитивного права, що регулюють відносини у сфері загроз безпеці основних об'єктів військових інтересів в інформаційній сфері, і норм, що визначають компетенцію суб'єктів протидії цим загрозам; специфічні для цієї галузі правові методи протидії загрозам; правові методи організації діяльності основних суб'єктів забезпечення інформаційної безпеки.

Правове забезпечення інформаційної безпеки являє собою комплексний напрям правового регулювання відносин у галузі протидії загрозам безпеки об'єктів військових інтересів в інформаційній сфері на основі норм конституційного, цивільного, адміністративного, кримінального, трудового та інформаційного права, а також напрямок здійснення організаційно-правових заходів щодо протидії цим загрозам. Основними об'єктами військових інтересів в інформаційній сфері є інформація, інформаційна інфраструктура і інформаційної безпека військовослужбовців.

Формування нормативної бази правового регулювання відносин у галузі протидії загрозам безпеки об'єктів військових інтересів в інформаційній сфері передбачає такі основні етапи: аналіз правових характеристик об'єкта військових інтересів в інформаційній сфері; аналіз змісту загроз безпеки об'єктів військових інтересів в інформаційній сфері; аналіз нормативного правового забезпечення безпеки об'єктів військових інтересів в інформаційній сфері; розробка пропозицій щодо вдосконалення норм, що регулюють відносини в галузі забезпечення безпеки цих об'єктів.

Структура нормативної бази правового регулювання відносин у галузі протидії загрозам безпеки об'єктів військових інтересів в інформаційній сфері містить такі складові: правове забезпечення безпеки інформації в формі відомостей; правове забезпечення безпеки інформації у формі повідомлень; правове гарантування безпеки інформаційної інфраструктури; правове забезпечення інформаційної безпеки військовослужбовців.

Правова протидія загрозам безпеці інформації у формі відомостей спрямована на нормативне регулювання відносин у сфері протидії застосуванню спеціальних технологій нав'язування відомостей за допомогою здійснення індивідуального психологічного насильства з використанням спеціальних інформаційних технологій, що ґрунтуються на поширенні масової інформації, а також правових норм, що регулюють відносини у сфері протидії пропаганді духовних і моральних цінностей, що суперечать прийнятим в українському суспільстві, та на нормах конституційного, адміністративного та кримінального права.

Правова протидія загрозам безпеці інформації у формі повідомлень спрямована на нормативне регулювання відносин у сфері забезпечення збереженості документів та ґрунтується на нормах цивільного, адміністративного, інформаційного, трудового та кримінального права.

Правову протидію загрозам безпеці інформаційної інфраструктури спрямовано на нормативне регулювання відносин у сфері забезпечення схоронності телекомунікаційних об'єктів, працездатності засобів зв'язку, раціонального використання радіочастотного ресурсу, обслуговування абонентів мережі зв'язку, стійкого функціонування мереж зв'язку, інформаційних і комп'ютерних систем, інформаційних мереж і інших організаційно-технічних систем, призначених для підвищення ефективності діяльності суб'єктів інформаційної сфери, а також виробництва та поширення продукції засобів масової інформації. Ця протидія ґрунтується на нормах конституційного, адміністративного, інформаційного та кримінального права.

Правове забезпечення захищеності від загроз інформаційній безпеці військовослужбовців спрямоване на нормативне регулювання відносин у галузі реалізації гарантій: надання інформації, необхідної для реалізації законних інтересів; надання зацікавленим суб'єктам інформаційної сфери, а також представників засобів масової інформації, доступу до відкритої суспільно значимої інформації, що накопичується в державних органах; державної підтримки засобів масової інформації; поширення масової інформації державними органами; захисту військовими органами інформації для обмеженого доступу. Ця протидія ґрунтується на нормах конституційного, цивільного, адміністративного, інформаційного та кримінального права.

Нормативне регулювання відносин у галузі організаційно-правової діяльності суб'єктів забезпечення інформаційної безпеки спрямоване на встановлення компетенції військових органів зі здійснення правозастосовної практики в галузі протидії загрозам безпеки основних об'єктів військових інтересів в інформаційній сфері, а також на координацію цієї діяльності уповноваженими посадовими особами та органами. Ця діяльність ґрунтується на нормах конституційного і адміністративного права.

Результати аналізу законодавчих (законів України, постанов Кабінету Міністрів України) та відомчих (наказів, директив, вказівок Міністрів оборони та внутрішніх справ України) актів, а також документів без обмеження доступу, що стосуються інформаційного забезпечення і інформаційної безпеки у Збройних силах показують, що в загальній структурі змістовного аспекту управління інформаційною безпекою в Збройних силах реальні інформаційні потреби військовослужбовців не знаходять належного відображення [1; 2; 3; 4]. Перешкодами для управління інформаційною безпекою у соціальному аспекті в Збройних силах є недостатнє та неповне заповнення інформаційного поля, що формується, відсутність належної уваги органів управління до даного процесу, консерватизм управління в інформаційному середовищі.

Підвищення загальноосвітнього рівня військовослужбовців ініціює якісніший рівень інформаційних відносин у службово-професійній сфері та необхідність перегляду низки управлінських рішень з управління інформаційною безпекою в Збройних силах, оскільки не завжди і не повною мірою враховуються вимоги військовослужбовців щодо задоволення інформаційних потреб. Зазначене вимагає розроблення сучасної моделі оптимізації адміністративно-правового регулювання інформаційної безпеки в Збройних силах, яка охоплювала би регулівну діяльність органів державного та військового управління щодо підвищення результативності впливів інформаційного макросередовища та мікросередовища під час функціонування суб'єктів управління державного, відомчого та міжособистісного рівня, надаючи комплекс взаємопов'язаних напрямів і способів їх практичної реалізації, орієнтованих на відтворення умов інформаційної безпеки військовослужбовців.

Ефективне управління інформаційною безпекою військовослужбовців є, з одного боку, найважливішою умовою захисту від негативного інформаційного впливу, з іншого, критерієм якості інформаційного забезпечення діяльності Збройних сил.

В умовах мирного стану відбувається порівняно достатнє задоволення потреб військовослужбовців і органів військового управління в інформації. В умовах бойових дій, коли виникають стресові ситуації, відзначається максимальна потреба військовослужбовців у певній інформації. Проявляється дефіцит об'єктивної інформації. Відбувається перерозподіл інформаційних потоків і рівень задоволення інформаційних потреб знижується.

У процесі оптимізації управління інформаційною безпекою необхідно враховувати вплив і можливості зворотного зв'язку, без якого немислимий весь процес управління, оскільки на кожному етапі процесу обміну інформацією відбувається деяке спотворення первинного сенсу. Це може виразитися в нестачі підготовлених кадрів і втрати деперсоналізації діяльності.

Удосконалення управління інформаційною безпекою в Збройних силах у правовому та соціологічному аспектах вимагає реалізації комплексу заходів щодо оптимізації організаційно-технологічних і нормативно-правових основ управління в управлінській ланці та всебічного розвитку інформаційного забезпечення. Формування інформаційних потреб військовослужбовців на необхідному якісному рівні потребує науковий підхід до процесу управління інформаційною безпекою та наповнення інформаційного поля і в правовому, і в соціологічному аспектах.

Управління інформаційною безпекою має тенденцію, яка динамічно розвивається, виявляючи істотний вплив на функціонування і ефективність діяльності не тільки органів військового управління, але і загалом на військові колективи. Це передбачає всебічне врахування правового аспекту систематичного впливу на інформаційне середовище формуванням інформаційного поля з метою регулювання якості інформаційних потоків щодо стабілізації інформаційного впливу на військовослужбовців, що дають змогу успішно виконувати поставлені завдання, враховуючи реальний стан.

Узагальнений досвід вітчизняних і зарубіжних дослідників в галузі вивчення інформаційної безпеки та її управління дає змогу розуміти сутність правового змісту управління інформаційною безпекою в Збройних силах як використання функцій і можливостей управління потоками в інформаційному середовищі для регулювання ступеня і характеру впливу на ключові канали з урахуванням оцінки інформаційного впливу в інтересах підвищення рівня інформаційної захищеності Збройних сил як самостійної інституційно-організаційної структури.

Сучасний стан управління інформаційною безпекою в соціологічному аспекті у Збройних силах недостатньо забезпечує відтворення необхідних інформаційних відносин, але водночас перебуває у функціональному стані і не допускає ескалації напруженості.

У разі оптимізації управління інформаційною безпекою у Збройних силах на сучасному етапі їх розвитку і організаційно-штатного реформування необхідна реалізація суб'єктами управління та фахівцями в галузі інформаційної безпеки спеціальних прийомів щодо цілеспрямованого інформаційного впливу, за якого враховуються соціально-професійні та соціально-демографічні характеристики військовослужбовців при задоволенні інформаційних потреб. Вирішення проблем управління інформаційною безпекою військовослужбовців залежить від розуміння значущості управління, готовності та бажання посадових осіб, які мають статус суб'єкта управління, вийти на новий рівень забезпечення інформаційної безпеки. Недооцінка її ролі, відмова від цілеспрямованого формування громадської думки, в комплексі з застосуванням інноваційних засобів інформаційного забезпечення, істотно ускладнюють реалізацію Збройними силами своїх функцій, особливо завдань з підтримки інформаційної безпеки військовослужбовців у бойових ситуаціях і забезпечення їх готовності до виконання поставлених завдань.

Для того, щоб інформація відповідала потребам військового управління, потрібен цілеспрямований процес організації, що ґрунтується на новітніх технологіях, нових тенденціях розвитку прикладних адміністративно-правових досліджень. Більшість аналітичних завдань повинні виконуватися в режимі прямого інформаційного моделювання, спостереження за керуванням інформаційним середовищем, не виключаючи традиційну стадію аналізу матеріалів (публікацій). При цьому з боку фахівців, що постачають інформацію, і з боку органів військового управління, як її споживача, потрібні постійні зусилля.

У Збройних силах України циркулює різноманітна за характеристиками, видами і функціями військова інформація, яку активно використовують в процесах управління, навчання та виховання військовослужбовців. Вона об'єктивно має широкий спектр кількісно-якісних характеристик і вимог. Чим вища відповідність якості використовуваної військової інформації до висунутих до неї вимог, тим вища ефективність військової діяльності. Це одна з найважливіших аксіом інформаційної роботи в Збройних силах.

Духовний світ військовослужбовців формується на основі інформації і під впливом цілеспрямованого проведення інформаційної роботи. Впливаючи на всі сфери психіки, зокрема на почуття військовослужбовців, вона робить вирішальний вплив на поведінку та військову діяльність особового складу. Такі компоненти духовного світу особистості військовослужбовця, як модель світу (світогляд), соціальні установки, віра, переконання, мотиви, мають складну інформаційну основу. За допомогою військово-соціальної інформації поряд з іншими засобами можна формувати духовний світ, систему моральних цінностей військовослужбовців і впливати на їх активність у справі захисту держави. Тому системне застосування методів інформаційно-аналітичної роботи значно підвищує можливості інформаційного забезпечення і, як наслідок, інформаційної безпеки військовослужбовців усіх категорій. З одного боку, ці методи дають змогу забезпечити високу якість військово-соціальної інформації, а з іншого, здатні слугувати провідником державної інформаційної політики у військах, яку здійснюють органи інформаційного забезпечення.

Поряд з адміністративно-правовими методами регулювання системи інформаційного забезпечення виступають нові інформаційні технології. Оптимальне поєднання традиційних, нових, масових і індивідуальних інформаційних технологій в управлінській діяльності посадових осіб органів військового управління та органів інформаційного забезпечення є важливим чинником підвищення її ефективності.

У зв'язку з активним розвитком за кордоном сил і засобів інформаційно-психологічної боротьби підвищується актуальність проблем інформаційної безпеки військ, інформаційно-психологічної протидії, що вимагає не тільки їх наукового вивчення, а й пошуку адекватних шляхів побудови ефективної системи інформаційного захисту як важливого компонента сучасної системи інформаційного забезпечення військ і у правовому, і в соціологічному аспектах. Необхідно особливо виділяти заходи безпеки під час роботи в комп'ютерних мережах, які все ширше використовуються в повсякденних умовах органами військового управління, установами та закладами військових формувань України.

У бойовій обстановці своєчасне виявлення та аналіз (моніторинг) форм, методів і засобів інформаційного впливу ворога, протидія його ворожим і підривним акціям, підтримання нормального інформаційного режиму діяльності військ, проведення цілеспрямованої інформаційно-виховної роботи з особовим складом поряд з іншими заходами дають змогу виконувати завдання завоювання інформаційної та морально-психологічної переваги над ворогом, що є важливим чинником перемоги в сучасних бойових діях.

Сьогодні образ Збройних сил України набуває бажані контури в громадській думці українців і громадян іноземних держав, тому українські електронні та друковані засоби масової інформації повинні більше розповідати про досягнення армії, щоб підтримувати значимість і силу української армії. Сформоване уявлення про Збройні сили необхідно підтримувати за допомогою реалізації сучасних управлінських і інформаційних технологій, що вже неодноразово доведено на прикладах реформаційних процесів в арміях НАТО. Вигляд і репутація армії – це, насамперед, інформаційний ресурс їх впливу на якісну зміну Збройних сил України, найважливіша складова процесу їх подальшої модернізації та розвитку.

Висновки. Реалізація інформаційної безпеки у правовому та соціологічному аспектах у Збройних силах можлива за допомогою оптимального застосування інноваційних технологій з комплексним диференційованим безперервним інформаційним впливом на особистість військовослужбовця. Це передбачає регулярне отримання максимального обсягу інформації суб'єктами управління, яка відтворює зміни в часі і в просторі основних характеристик учасників управління і особливо ступеня задоволення їх інформаційних потреб. Якісне задоволення інформаційних потреб військовослужбовців забезпечує створення передумов до підвищення рівня інформаційної безпеки – ефективного, цілеспрямованого, чітко структурованого за напрямами інформаційного впливу, що враховує особливості військовослужбовців. У результаті управління інформаційною безпекою має бути реалізовано керуючий вплив на стан боєздатності, налагоджено регулярне отримання максимального обсягу соціологічної інформації суб'єктами управління.

1. Проект Указу Президента України "Про Доктрину інформаційної безпеки України". Державний комітет телебачення та радіомовлення України. 12.06.2014. Департамент інформаційної політики. [Електронний ресурс]. – Режим доступу: http://comin.kmu.gov.ua/control/uk/publish/ article?art_id=113319&cat_id=61025. 2. Про захист інформації в інформаційно-телекомунікаційних системах 05.07.1994 № 80/94-ВР // Відомості Верховної Ради. – 1994. – N 31. – Ст. 286. 3. Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України "Про інформацію" та Закону України "Про доступ до публічної інформації": Закон України від 27.03.2014 № 1170-VII // Відомості Верховної Ради. – 2014. –№ 22. – Ст.816. 4. Про основи національної безпеки України: Закон України від 19.06.2003 № 964-IV // Відомості Верховної Ради. – 2003. – № 39. – Ст.351.