УДК 355.318:355.433.4:316.776.23

І. І. Ліпатов

ВИМОГИ ДО СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ БЕЗПЕКИ ВІЙСЬКОВОСЛУЖБОВЦІВ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Розглянуто зміст підсистем і елементів системи забезпечення інформаційно-психологічної безпеки Національної гвардії України, вимоги до їх створення, а також види власного забезпечення системи, завдяки яким вона здатна виконувати свою цільову функцію.

Ключові слова: *інформаційний простір, інформаційно-психологічний вплив, підсистеми і елементи системи забезпечення інформаційно-психологічної безпеки, види власного забезпечення системи.*

Постановка проблеми. Національна гвардія України (НГУ) виконує завдання з забезпечення громадської безпеки. У процесі виконання службово-бойових завдань (СБЗ) під час проведення спеціальних операцій на свідомість особового складу і групову свідомість формувань НГУ з боку протидіючих сил здійснюється негативний інформаційно-психологічний вплив (ІПВ), який знижує ефективність виконання ними СБЗ. Тому виникає потреба в забезпеченні інформаційно-психологічної безпеки (ІПБ) особового складу.

У Доктрині інформаційної безпеки України [1] визначено національні інтереси України в інформаційній сфері, актуальні загрози національним інтересам і національній безпеці України в інформаційній сфері, пріоритети державної політики в інформаційній сфері та механізм її реалізації. Однак у механізмах її реалізації не визначено роль і місце Міністерства внутрішніх справ України як органу виконавчої влади із забезпечення національної безпеки в інформаційній сфері, а також НГУ як складової сектора безпеки й оборони України, хоча ці структури є головними виконавцями забезпечення державної і громадської безпеки.

У [1] не враховано те, що під час виконання СБЗ формуваннями НГУ постає необхідність внутрішнього забезпечення ІПБ особового складу і населення. Це потребує створення системи забезпечення ІПБ особового складу формувань НГУ, яка дозволить гвардії адекватно реагувати на інформаційно-психологічні загрози, що виникають, і ефективно виконувати СБЗ. Створення такої системи неможливе без визначення науково обґрунтованих вимог до неї.

Аналіз останніх досліджень і публікацій. Теоретико-методологічну базу організації та забезпечення інформаційної, психологічної, інформаційно-психологічної безпеки громадян, суспільства, держави, протидії негативному ІПВ на військовослужбовців і їх захисту під час виконання ними СБЗ становлять праці таких вітчизняних і зарубіжних науковців: В. М. Богуш, Г. В. Грачов, І. В. Замаруєва, О. Г. Караяні, В. Г. Крисько, О. В. Литвиненко, А. Г. Лук'янець, О. А. Матеюк, І. К. Мельник, М. О. Попов, Г. Г. Почепцов, С. П. Расторгуєв, А. О. Рось, А. В. Манойло, В. Б. Толубко, В. О. Фомін, А. І. Черняк, В. П. Шейнов, О. К. Юдін та ін.

Аналіз цих та інших праць свідчить про те, що в наукових дослідженнях наводяться різні аспекти ІПБ, але немає наукового обґрунтування вимог до системи забезпечення ІПБ військовослужбовців, військових колективів НГУ від зовнішнього і внутрішнього негативного ІПВ під час виконання СБЗ. Це викликало суперечність між потребою створення системи забезпечення ІПБ під час виконання СБЗ і недостатністю наукового обґрунтування вимог до неї.

Актуальність створення системи забезпечення ІПБ військовослужбовців, її недостатнє теоретичне обґрунтування і практичне розроблення саме й обумовило потребу у визначенні вимог до системи забезпечення ІПБ військовослужбовців НГУ.

Метою статті є визначення вимог до системи забезпечення інформаційно-

психологічної безпеки військовослужбовців Національної гвардії України.

Виклад основного матеріалу. Розвиток інформаційно-телекомунікаційних технологій зумовив появу інформаційного простору з новими комунікаційними можливостями. Це спричинило виникнення нових інформаційно-психологічних загроз національній безпеці держави. Так, подання і поширення в засобах масової комунікації спеціально підготовленої інформації під виглядом новин переводять її до розряду прихованого негативного ІПВ [2]. Наслідком дії негативних ІПВ на свідомість особового складу та групову свідомість формувань НГУ під час виконання СБЗ є зниження ефективності їх діяльності. Запобігти можливим негативним наслідкам, спричиненим ІПВ, можна лише завдяки створенню надійної системи забезпечення інформаційно-психологічної безпеки (ІПБ) особового складу, яка дозволить: здійснювати моніторинг інформаційного простору, аналізування інформаційно-психологічних впливів і визначення ступеня їх загрози, а також прогнозування розвитку ситуації; здійснювати заходи протидії щодо нейтралізації загроз; проводити заходи індивідуального і групового захисту свідомості військовослужбовців і групової свідомості військових колективів.

Як зазначалося нами раніше [3], система забезпечення ІПБ особового складу формувань НГУ має складатись із зовнішніх і внутрішніх елементів забезпечення ІПБ особового складу.

Внутрішній елемент забезпечення ІПБ особового складу НГУ, який розглядається нами, має нараховувати три підсистеми: перша – моніторингу, аналізування і прогнозування негативного ІПВ; друга – протидії негативному ІПВ; третя – захисту від негативного ІПВ. Кожна з підсистем, у свою чергу, поділяється на елементи.

Перша підсистема має три елементи: моніторинг, аналізування і прогнозування негативного ІПВ.

Друга підсистема також включає три елементи: організація запобіжних заходів; зрив і нейтралізація негативного ІПВ противника; здійснення інформаційно-психологічного впливу на свої сили, протидіючі сили й населення.

Елементів третьої підсистеми також три: навчання методам і способам обробки та оцінювання інформації; формування колективного соціально-психологічного захисту військових колективів; формування індивідуального психологічного захисту особового складу.

Оскільки сьогодні наявний інформаційний простір переважно представлений ресурсами Інтернету, елемент моніторингу (першої підсистеми) має охоплювати всі можливості щодо пошуку інформації, а саме [4]: пошукові системи, тематичні каталоги ресурсів, сайти новин, RSS-повідомлення, інформаційні агентства, які здійснюють он-лайн відеотрансляцію новин з урахуванням їх особливостей щодо висвітлення інформації.

Створення першої підсистеми, елементом якої є моніторинг, дозволить сформувати базу даних пошукових ресурсів, наявних в Інтернеті. Список інформаційних ресурсів має формуватися таким чином, аби вони, доповнюючи один одного, максимально охоплювали інформацію за певною темою відповідно до встановлених пошукових обмежень.

Другий елемент першої підсистеми – аналізування інформаційно-психологічних впливів і визначення ступеня їх загрози – має пов’язуватися з обробкою знайденого матеріалу. Вирішуючи це завдання, необхідно організувати автоматичне реферування знайденої інформації.

Для візуалізації знайденої інформації з метою її подальшого аналізу доцільно скористатися технологією побудови семантичних мереж. Порівняння семантичних мереж різних текстів дозволяє встановити ступінь їх змістової близькості, що може використовуватися для автоматичної класифікації документів за заданими рубриками, їх пошуку за подібністю заданого тексту, а також поділу інформаційного масиву на класи документів близького змісту [5].

Визначення рівня негативного ІПВ передбачає наявність компетентних експертів у цій галузі знань. На основі статистичної обробки даних, отриманих за результатами моніторингу інформаційного простору, у подальшому можливо встановити значення періодів спостереження і визначити для них відповідні критерії рівня ескалації загального негативного ІПВ відносно певних осіб або груп військовослужбовців.

Результати оцінювання мають становити підґрунтя для здійснення прогнозування – третього елемента першої підсистеми – негативного ІПВ і розроблення рекомендацій щодо забезпечення інформаційно-психологічної безпеки особового складу під час виконання СБЗ в умовах негативного ІПВ.

Створюючи другу підсистему, елементом якої є організація запобіжних заходів, необхідно формувати банк даних дієвих

запобіжних (профілактичних) заходів щодо поширення неправдивих чуток серед особового складу, тривожних висловлювань і протиправних дій, спрямованих на зниження морально-психологічного стану особового складу формувань НГУ. Сформований банк сприятиме вибору дієвих запобіжних заходів протидії НІПВ.

Другий елемент підсистеми – зрив і нейтралізація негативного ІПВ противника – має пов'язуватись із розробленням варіантів зриву й нейтралізації негативного ІПВ, можливістю вибору оптимального варіанта його нейтралізації за вибраним критерієм, із прийняттям рішення стосовно нейтралізації негативного ІПВ, підготовкою й реалізацією рішення щодо його зриву та нейтралізації.

Третій елемент підсистеми протидії негативному ІПВ має спрямовуватися на проведення інформаційно-психологічних заходів (акцій, психологічних операцій), розрахованих на свої сили і населення в районі виконання СБЗ, ведення бойових дій. Це потребує створення банку даних змісту та спрямованості інформаційно-психологічних операцій, акцій за різних умов виконання СБЗ.

Третя підсистема складається з трьох елементів: навчання методам і способам обробки й оцінювання інформації; формування колективного соціально-психологічного захисту військових колективів; формування індивідуального психологічного захисту особового складу.

Створення третьої підсистеми, елементом якої є навчання методам і способам обробки й оцінювання інформації, потребує системи підготовки військовослужбовців, яка формуватиме в них навички і вміння обробки й оцінювання інформації, здатність визначати деструктивний інформаційно-психологічний вплив і протистояти йому.

Другий і третій елементи потребують розроблення моделей елементів підсистем, здатних забезпечити інформаційно-психологічну безпеку як окремих військовослужбовців, так і військових колективів.

Поєднавши функції та завдання трьох підсистем [3, 6] в умовах сучасного інформаційного простору, система забезпечення інформаційно-психологічної безпеки особового складу під час виконання СБЗ має забезпечити:

– періодичний автоматизований збір і тематичний пошук негативної, деструктивної інформації, що становить зміст негативних ІПВ, які створюють загрози у відкритих джерелах інформації;

– автоматичну й автоматизовану обробку текстових матеріалів, виділення з них об'єктів інтересу і пов'язаних із ними фактів;

– класифікацію різномовних текстів за єдиними критеріями;

– автоматичну лінгвістичну обробку;

– відбір відомостей із банку текстової інформації або бази знань на вимогу оператора;

– інтегрування й узагальнення знань, які містяться в різномовних текстах із певної предметної галузі;

– перевірку на наявність дезінформації даних, які містяться в різномовних текстах і в їх сукупності;

– виявлення закономірностей у певній предметній галузі та їх формування на змістовому рівні;

– збереження в базі даних отриманої інформації, а також надання авторизованого доступу користувачів до перегляду й аналітичної обробки документів;

– створення єдиного структурованого архіву об'єктів інтересу, досьє на них, а також подій і взаємовідношення між ними з метою моніторингу змін їх стану в процесі діяльності, виконання часових, географічних і тематичних зрізів під час формування різноманітних звітів;

– надання аналітикам засобів швидкого виявлення неявних зв'язків між об'єктами моніторингу і пов'язаними з ними фактами й подіями;

– візуалізацію результатів аналітичних досліджень шляхом генерації дайджестів статей і фактів, формалізованих досьє, семантичних мереж та інших аналітичних звітів;

– визначення рівня інформаційної загрози від негативного ІПВ;

– розроблення варіантів нейтралізації негативного ІПВ;

– можливість вибору оптимального варіанта нейтралізації негативного ІПВ за вибраним критерієм;

– прийняття рішення про нейтралізацію негативного ІПВ;

– підготовку і всебічне забезпечення реалізації рішення;

– нейтралізацію негативного ІПВ;

– створення системи підготовки військовослужбовців, яка дозволить формувати в них навички і вміння обробки й оцінювання інформації, здатності визначати деструктивний інформаційно-психологічний вплив і протистояти йому;

– розроблення моделей елементів підсистем, здатних забезпечити інформаційно-психологічну безпеку як окремих військовослужбовців, так і військових колективів;

– оцінювання рівня інформаційної загрози після впливу на неї заходів елементів

підсистем протидії негативному ІПВ і захисту від нього системи забезпечення інформаційно-психологічної безпеки особового складу НГУ під час виконання СБЗ.

Системі забезпечення ІПБ, як і будь-якій системі, слід мати певні види власного забезпечення, завдяки яким вона виконуватиме свою цільову функцію. З огляду на це система забезпечення ІПБ повинна мати таке.

1. Правове забезпечення. Нормативні документи, положення, інструкції, керівництва, вимоги яких є обов'язковими в рамках сфери їх дії.

2. Організаційне забезпечення. Реалізація забезпечення ІПБ здійснюється певними структурними одиницями: штаб військової частини; відділ по роботі з особовим складом; служба психологічного забезпечення та ін.

3. Технічне забезпечення. Широке використання технічних засобів як для забезпечення інформаційно-психологічної безпеки, так і для забезпечення діяльності власне системи забезпечення ІПБ.

4. Інформаційне забезпечення. Відомості, дані, показники, параметри, покладені в основу вирішення завдань, що забезпечують функціонування системи.

5. Програмне забезпечення. Різні інформаційні, облікові, статистичні й розрахункові програми, що забезпечують оцінювання наявності й небезпеки різних каналів, видів інформаційно-психологічного впливу.

6. Математичне забезпечення. Використання математичних методів для різних розрахунків, пов'язаних із рівнями інформаційно-психологічного впливу й захисту від нього.

7. Лінгвістичне забезпечення. Сукупність спеціальних мовних засобів спілкування фахівців і користувачів у сфері забезпечення ІПБ.

8. Нормативно-методичне забезпечення. Норми й регламенти діяльності органів, служб, засобів, що реалізовують функції забезпечення інформаційно-психологічної безпеки, різного роду методики, які забезпечують діяльність персоналу із забезпечення інформаційно-психологічної безпеки.

Висновки

Таким чином, розгляд вимог до забезпечення інформаційно-психологічної безпеки дає підстави зробити такі висновки.

1. Запобігти можливим негативним наслідкам, спричиненим ІПВ, можливо лише завдяки створенню надійної системи забезпечення інформаційно-психологічної безпеки (ІПБ) особового складу, яка дозволяє: здійснювати моніторинг інформаційного простору, аналізування інформаційно-психологічних впливів і визначення ступеня їх загрози та прогнозування розвитку ситуації; здійснювати заходи протидії щодо нейтралізації загроз; проводити заходи індивідуального і групового захисту свідомості військовослужбовців і групової свідомості військових колективів.

2. Система забезпечення інформаційно-психологічної безпеки особового складу формувань Національної гвардії України, на наш погляд, має складатись із зовнішніх і внутрішніх елементів забезпечення інформаційно-психологічної безпеки особового складу.

3. Внутрішній елемент забезпечення інформаційно-психологічної безпеки особового складу НГУ, який розглядається нами, має три підсистеми: перша – моніторингу, аналізування і прогнозування НІПВ; друга – протидії НІПВ; третя – захисту від НІПВ.

4. Кожна з підсистем поділяється на елементи. Перша підсистема нараховує три елементи: моніторинг, аналізування і прогнозування НІПВ. Друга підсистема також має три елементи: організація запобіжних заходів; зрив і нейтралізація негативного ІПВ противника; здійснення інформаційно-психологічного впливу на свої війська, протидіючі сили і населення. Елементів третьої підсистеми також три: навчання методам і способам обробки й оцінювання інформації; формування колективного соціально-психологічного захисту військових колективів; формування індивідуального психологічного захисту особового складу.

5. Поєднання функцій і завдань трьох підсистем в умовах сучасного інформаційного простору дозволяє визначити вимоги до створення системи забезпечення інформаційно-психологічної безпеки особового складу під час виконання службово-бойових завдань.

6. Система забезпечення інформаційно-психологічної безпеки, як і будь-яка система, потребує певних видів власного забезпечення, завдяки яким вона виконуватиме свою цільову функцію. З огляду на це СЗІПБ може мати: правове забезпечення; організаційне забезпечення; технічне забезпечення; інформаційне забезпечення; програмне забезпечення; математичне забезпечення; лінгвістичне забезпечення; нормативно-методичне забезпечення.

Список використаних джерел

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безреки України". Президент України, Указ від 25 лютого 2017 року № 47/2017. [Електронний ресурс]: Режим доступу: http://zakon3.rada.gov.ua/laws/show/47/2017.
2. Брайант, Д. Основы воздействия СМИ [Текст] / Д. Брайант, С. Томпсон; пер. с англ. – Москва : Изд. дом "Вильямс", 2004. – 432 с.
3. Ліпатов, І. І. Структура та функції системи забезпечення інформаційно-психологічної безпеки військовослужбовців Національної гвардії України [Текст] / І. І. Ліпатов, Г. А. Дробаха, Ю. П. Бабков, М. О. Чепель // Честь і закон. – 2017. – № 2 (61)/. – С. 43–49.
4. Системы мониторинга и анализа СМИ [Электронный ресурс]. – Режим доступа : http://www.newart.ru/oparin/smi_oparin.htm.
5. Michael W. Berry. Survey of Text Mining. Clustering, Classification and Retrieval Michael W. Berry. – Springer-Verlag, 2004. – 244 p.
6. Хан, У. Системы автоматического реферирования [Электронный ресурс] / У. Хан, И. Мани // Открытые системы. – 2000. – № 12. – Режим доступа : http://www.osp.ru.

Стаття надійшла до редакції 12.03.2018 р.

УДК 355.318:355.433.4:316.776.23

И. И. Липатов

ТРЕБОВАНИЯ К СИСТЕМЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ВОЕННОСЛУЖАЩИХ НАЦИОНАЛЬНОЙ ГВАРДИИ УКРАИНЫ

Рассмотрено содержание подсистем и элементов системы обеспечения информационно-психологической безопасности Национальной гвардии Украины, требования к их созданию, а также виды собственного обеспечения системы, опираясь на которые она способна выполнять свою целевую функцию.

Ключевые слова: *информационный простор, информационно-психологическое воздействие, подсистемы и элементы системы обеспечения информационно-психологической безопасности, виды собственного обеспечения системы.*

UDC 355.318:355.433.4:316.776.23

I. Lipatov

SYSTEM REQUIREMENTS FOR OBEZPECHENNJA INFORMATIVE-PSYCHOLOGICAL SECURITY TROOPS OF THE NATIONAL GUARD OF UKRAINE

The Doctrine of Information Security of Ukraine defines the national interests of Ukraine in the information sphere, the actual threats to the national interests and national security of Ukraine in the information sphere, the priorities of the state policy in the information sphere and the mechanism for its implementation. However, in the mechanisms of its implementation, the role and place of the Ministry of Internal Affairs of Ukraine as a body of executive power for ensuring national security in the information sphere, as well as National Guard of Ukraine as a component of the security and defense sector of Ukraine, are not defined, although these structures are the main providers of state and public security.

It was not taken into account that during the execution of the by the formations of the National Guard of Ukraine , there is a need for the internal security of the IPB personnel and population. This requires the establishment of a security system for the personnel of the NSU factions, which will enable the Guards to respond adequately to the emerging information and psychological threats and to effectively implement the. Creation of such a system is impossible without the definition of scientifically substantiated requirements to it.

The purpose of the article is to define the requirements for the system of providing informational and psychological safety of servicemen of the National Guard of Ukraine.

Considered the contents subsystems and safety information-psychological security National Guard, the requirements for their establishment and types of security system on which it is able to fulfil its target function.

Keywords: *informational space, information and psychological impact, subsystems, and components of the system providing information and psychological security, types of security systems.*

Ліпатов Іван Іванович – кандидат психологічних наук, професор, професор кафедри оперативного мистецтва Національної академії Національної гвардії України