Розвиток та застосування Повітряних Сил, інших видів Збройних Сил України, удосконалення їх системи управління

УДК 354.42 DOI: 10.30748/nitps.2018.30.01

О.В. Левченко

Житомирський військовий інститут ім. С.П. Корольова, Житомир

КОНЦЕПТУАЛЬНІ ОСНОВИ ФОРМУВАННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті обґрунтовано концептуальний підхід до формування системи забезпечення інформаційної безпеки як складової загальнодержавної системи забезпечення воєнної безпеки. Визначено мету, завдання і функції та розроблено принципи побудови даної системи. З позицій системного підходу запропоновано її базову структуру, що складається з функціональних підсистем. Окреслено призначення і завдання кожної підсистеми.

Ключові слова: *мета, завдання, функції, принципи побудови, система забезпечення інформаційної безпеки.*

Вступ

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими та практичними завданнями. Вивчення досвіду підготовки та ведення Російською Федерацією гібридної агресії проти України показує, що інформаційна складова на всіх етапах конфлікту є визначальною [1]. Завдяки потужним антиукраїнським інформаційним операціям Росії значною мірою вдалося досягти своїх цілей. Результативно протидіяти ворожим інформаційним операціям, спрямованим проти об'єктів держави та її Збройних Сил, і проводити власні активні заходи впливу можливо, створивши ефективну систему забезпечення інформаційної безпеки (СЗІБ) у складі системи забезпечення воєнної безпеки держави (СЗВБД).

Отже, проблема наукового супроводження формування СЗІБ у воєнній сфері є важливим науковим та прикладним завданням.

Аналіз останніх досліджень і публікацій за визначеною темою [2–7] показав, що проблемі наукового супроводження СЗІБ у воєнній сфері приділяється значна увага. Вітчизняні дослідження стосуються всіх без винятку аспектів функціонування системи: від питань виявлення деструктивного інформаційно-психологічного впливу до рекомендацій щодо організації та проведення заходів протидії інформаційним загрозам (ІЗ). Проте в них означені проблеми, як правило, розглядаються в цілому без достатньої деталізації. Найбільш ґрунтовні розробки щодо концептуальних основ побудови СЗІБ у воєнній сфері містяться в роботах [6–7], але на сьогодні в нових умовах функціонування сектора безпеки й оборони держави вони потребують коригування і конкретизації.

Таким чином, незважаючи на значну увагу наукової спільноти до питань забезпечення інформаційної безпеки держави та її Збройних Сил, на цей час продовжують залишатися недостатньо глибоко дослідженими питання обґрунтування напрямів формування СЗІБ у загальній СЗВБД.

Метою статті є обґрунтування мети, завдань, функцій і принципів побудови СЗІБ як складової загальнодержавної системи забезпечення воєнної безпеки.

Виклад основного матеріалу

Аналіз іноземного досвіду щодо захисту інформаційної інфраструктури держави від зовнішнього інформаційного впливу на власне населення і особовий склад збройних сил свідчить, що багатьма країнами світу створені національні системи інформаційної безпеки, причому в провідних державах, які розглядають інформаційну безпеку виключно з позицій системного підходу, такі системи мають загальні ключові ознаки:

ієрархічність побудови;

управління та координація діяльності структурних підрозділів системи на найвищому державному рівні;

наявність спеціально створеного керівного органу системи;

чітка організація взаємодії між складовими.

Найбільш досконалі та потужні системи інформаційної безпеки побудовані й успішно функціонують у США, Росії, Великобританії, Ізраїлі, Китаї та деяких інших державах, які є об'єктами постійного потужного зовнішнього інформаційного впливу. Слід зауважити, що зазначені системи цих країн мають і достатню активну складову, завдяки чому мають можливість проведення інформаційно-психологічних операцій та кібернетичного впливу на противників.

Вбачається, що саме такий підхід потрібно застосовувати для побудови загальнодержавної системи інформаційної безпеки. У складі СЗВБД необхідно мати як підсистему СЗІБ, яка одночасно має також бути частиною системи інформаційної безпеки України, причому однією з найбільш вагомих її складових, а тому повинна будуватися з урахуванням наведеного іноземного досвіду.

Разом з тим, базовими чинниками побудови СЗІБ є визначені в державних керівних документах існуючі актуальні й потенційні ІЗ національній і воєнній безпеці [8–10], напрями державної політики з питань інформаційної безпеки [11–12], функції та завдання, визначені для виконання суб'єктами забезпечення інформаційної безпеки держави [13].

Отже, формування СЗІБ у складі СЗВБД має відбуватися згідно з принципами реалізації стратегії національної, воєнної та інформаційної безпеки з урахуванням закордонного та власного досвіду захисту інформаційного простору і протидії деструктивному іноземному впливу, а також наявних і прогнозованих інформаційних загроз державі та її Збройним Силам.

Головною метою створення СЗІБ як складової загальнодержавної системи забезпечення воєнної безпеки вважаємо попередження та нейтралізацію ІЗ, що надходять від іноземних держав, створення умов для гарантованого виконання Міністерством оборони України та Збройними Силами України, іншими суб'єктами сектора безпеки й оборони України своїх завдань за призначенням.

Частковими цілями створення СЗІБ слід вважати:

забезпечення реалізації державної інформаційної політики у воєнній сфері;

організацію управління суб'єктами інформаційної безпеки у воєнній сфері;

забезпечення своєчасного виявлення та ефективної протидії ІЗ;

організацію і ведення інформаційної боротьби;

створення необхідних умов для ефективного використання інформаційних ресурсів у воєнній сфері та їх розвитку.

Виходячи з усіх наведених підходів до побудови, чинників впливу, мети і завдань СЗІБ, на неї доцільно покласти такі функції:

управління системою, а саме:

формування інформаційної політики щодо забезпечення інформаційної безпеки у воєнній сфері;

формування нормативно-правової бази з питань забезпечення інформаційної безпеки у воєнній сфері та вдосконалення механізмів реалізації правових норм чинного законодавства;

організація управління системою та її структурними елементами, визначення їх повноважень;

координація діяльності всіх органів сектора безпеки й оборони, що вирішують завдання забезпечення інформаційної безпеки, щодо виявлення та нейтралізації інформаційних загроз у воєнній сфері;

виявлення ІЗ, а саме:

організація моніторингу іноземного інформаційного впливу та виявлення ознак ІЗ;

аналізу та прогнозування розвитку ІЗ, а саме:

проведення аналізу ІЗ, визначення їх рівня;

оцінювання стану інформаційної безпеки у воєнній сфері, прогнозування та виявлення джерел зовнішніх і внутрішніх загроз інформаційній безпеці, визначення пріоритетних напрямів запобігання, відбиття та нейтралізації цих загроз;

протидія ІЗ, а саме:

підготовка і проведення заходів захисту від виявлених ІЗ;

ведення інформаційної боротьби;

контроль та оцінювання ефективності функціонування системи, а саме:

контроль виконання завдань за призначенням складовими елементами системи;

оцінювання ефективності заходів щодо забезпечення інформаційної безпеки та протидії ІЗ;

всебічне забезпечення функціонування системи, а саме:

забезпечення необхідних умов функціонування всіх складових елементів системи матеріальними, фінансовими та іншими ресурсами;

підготовка кадрів та наукового супроводження, а саме:

удосконалення і розвиток системи підготовки кадрів за напрямом забезпечення інформаційної безпеки;

організація фундаментальних та прикладних наукових досліджень за напрямом забезпечення інформаційної безпеки.

Відповідно до визначеної мети та функцій СЗІБ основними її завданнями слід вважати:

створення нормативно-правової бази щодо забезпечення інформаційної безпеки у воєнній сфері;

створення і підтримання сил і засобів забезпечення інформаційної безпеки у воєнній сфері в готовності до застосування;

прогнозування потенційних загроз інформаційній безпеці і на цій основі передбачення змін в інформаційній безпеці у воєнній сфері;

організацію діяльності щодо усунення передумов і попередження загроз інформаційній безпеці;

виявлення, оцінювання та нейтралізацію загроз інформаційній безпеці у воєнній сфері та ліквідацію (участь у ліквідації) їх наслідків;

організацію і керівництво проведенням активних заходів у ході інформаційної боротьби;

організацію узгодженої діяльності складових СЗІБ, СЗВБД і взаємодіючих державних структур, що вирішують завдання забезпечення інформаційної безпеки, щодо виявлення та нейтралізації ІЗ у воєнній сфері;

оцінювання ефективності заходів щодо забезпечення інформаційної безпеки та протидії ІЗ;

попередження, виявлення та припинення правопорушень щодо забезпечення інформаційної безпеки;

участь у розвитку вітчизняної інформаційної інфраструктури;

участь у забезпеченні захисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури від ІЗ;

здійснення єдиної технічної політики у сфері забезпечення інформаційної безпеки України;

забезпечення необхідних умов функціонування всіх елементів системи матеріальних, фінансових та інших ресурсів;

організацію фундаментальних і прикладних наукових досліджень у сфері забезпечення інформаційної безпеки;

удосконалення та розвиток єдиної системи підготовки кадрів у сфері інформаційної безпеки України;

здійснення міжнародного співробітництва з питань інформаційної безпеки.

Важливою особливістю СЗІБ є те, що вона, з одного боку, є елементом системи більш високого рівня – СЗВБД, а з іншого – частиною системи забезпечення національної безпеки в інформаційній сфері. Ця особливість також має бути врахована при побудові СЗІБ, зокрема щодо розмежування повноважень органів законодавчої та виконавчої влади в даній сфері, а також поєднання зусиль зазначених органів з метою підвищення рівня інформаційної безпеки держави.

Виходячи з наведених вище умов, автором розроблено принципи побудови СЗІБ, які, на відміну від відомих, враховують особливості, притаманні саме цій системі.

Системність підходу до формування СЗІБ передбачає врахування усіх взаємопов'язаних, взаємодіючих і змінних у часі елементів, умов і факторів, важливих для розуміння і вирішення проблеми забезпечення інформаційної безпеки.

Структура СЗІБ має включати підсистеми і складові відповідно до розподілу її функцій і завдань. З позицій системного підходу повинна бути побудована не лише система, але й організовані зв'язок і взаємодія із СЗВБД і загальнодержавною системою інформаційної безпеки.

Розподіл і розмежування функцій. Цей принцип передбачає розподіл усіх функцій системи між усіма її складовими відповідно до їх призначення і завдань, а також їх чітке розмежування для виключення дублювання відповідальності за їх виконання.

Простота структури системи передбачає мінімізацію зв'язків між підсистемами й елементами та їх спрощення. Система повинна містити лише ті компоненти і зв'язки, які потрібні для її функціонування (з урахуванням вимог надійності та перспективного розвитку).

Гнучкість централізованого управління. Принцип передбачає жорстке централізоване управління силами і засобами щодо планування та протидії інформаційним загрозам, зокрема проведення активних заходів у рамках інформаційної боротьби. При цьому можливе поєднання централізованого управління з передачею частини повноважень підлеглим та взаємодіючим структурам з окремих питань контролю інформаційного простору і моніторингу негативного інформаційного впливу, а в питаннях технічного захисту інформації та деяких інших – перехід до децентралізованого управління. Передача частини повноважень і децентралізація управління дозволять значно спростити і прискорити роботу тих структур, які не вимагають постійного контролю вищою інстанцією. Натомість надзвичайно чутливі питання здійснення різнопланових заходів інформаційного впливу на противника повинні бути максимально скоординованими та проводитися під єдиним керівництвом навіть при залученні до них сил і засобів вищої інстанції. Цей принцип забезпечується чіткою вертикаллю управління системою з охопленням по каналам взаємодії залучених до протидії інформаційним загрозам структур вищих інстанцій.

Адаптивність системи полягає в можливості її пристосуванні без порушення роботи і зниження ефективності до змін зовнішніх і внутрішніх факторів, які впливають на безпеку інформаційного середовища та функціонування системи, а також до зміни умов життєдіяльності об'єктів інформаційної безпеки.

Стійкість до зовнішніх впливів полягає в забезпеченні спроможності СЗІБ функціонувати без погіршення своїх характеристик і результатів роботи в умовах проведення проти неї та її складових цілеспрямованих інформаційно-психологічних та інформаційно-технічних атак.

Безперервність функціонування полягає в організації системою такого режиму роботи всіх складових і підсистем, за якого не допускаються перерви як суб'єктивного, так і об'єктивного характеру. При цьому має бути забезпечена постійна керованість

процесами, які циркулюють у системі, та організаційно-адміністративна і ресурсна підтримка роботи складових структур.

Превентивність реагування на загрози в інформаційній сфері полягає у наданні пріоритету щодо аналізу ознак виявлених загроз та прийняття управлінських рішень по ним інформаційним загрозам по відношенню до загроз, які надходять з інших сфер воєнної безпеки держави. Цей принцип обумовлюється тим, що ознаки загроз в різних сферах воєнної безпеки, як правило, починають спочатку проявлятися в інформаційній сфері, а вже згодом надходять на «свої» сфери. Тому своєчасне їх виявлення в інформаційній сфері надасть змогу превентивно на них зреагувати. Принцип забезпечується створенням необхідних умов для надійного виявлення ознак інформаційних загроз ще на ранній стадії їх прояву та якісного аналізу, оцінювання і прогнозування розвитку.

Безпосередньо для побудови СЗІБ скористаємося методикою, викладеною в [13]. Виходячи з того, що система утворюється сукупністю суб'єктів, які повинні виконувати наведені вище різні функції та завдання за напрямами своєї діяльності, її структура може бути утворена за рахунок об'єднання суб'єктів у функціональні підсистеми за обраним показником. Таким показником може бути близькість функцій, що виконуються цими об'єктами. Визначення об'єктів з близькими функціями та їх групування в підсистеми здійснюється за допомогою методу кластерного аналізу.

Отже, відповідно до визначених вище основних функцій, які має виконувати СЗІБ в інтересах своєчасного виявлення інформаційних загроз державі та її Збройним Силам, а також для ефективної протидії їм, з урахуванням принципу системного підходу до побудови СЗІБ, її структуру доцільно подати у вигляді складної системи, яка складається з функціональних підсистем:

управління;

моніторингу зовнішнього інформаційного впливу;

аналізу, оцінювання рівня та прогнозування ІЗ;

протидії ІЗ;

контролю та оцінювання ефективності функціонування СЗІБ;

всебічного забезпечення її функціонування;

підготовки кадрів та наукового супроводження.

У свою чергу, кожна з підсистем складається з функціональних елементів у вигляді змістовних блоків, що виконують певну окрему функцію і завдання.

Застосування зазначених вище підходів до побудови СЗІБ, а також наведені її функції і призначення дозволяють визначити завдання її підсистем.

На *підсистему управління* доцільно покласти такі завдання:

безпосереднє управління діяльністю суб'єктів забезпечення інформаційної безпеки;

координацію та контроль виконання заходів щодо забезпечення інформаційної безпеки;

планування заходів протидії ІЗ;

оцінювання ефективності функціонування підсистем та заходів протидії ІЗ;

організацію взаємодії з іншими суб'єктами забезпечення інформаційної безпеки сектора безпеки й оборони держави.

На *підсистему моніторингу зовнішнього інформаційного впливу* доцільно покласти такі завдання:

постійний моніторинг зовнішнього інформаційного потоку;

виявлення заходів інформаційно-психологічного впливу на воєнно-політичне керівництво і населення держави, особовий склад Збройних Сил України;

виявлення ознак ІЗ.

На *підсистему аналізу, оцінювання рівня та прогнозування ІЗ* доцільно покласти такі завдання:

аналіз виявлених загроз, оцінювання їх рівня;

прогнозування розвитку ІЗ та їх впливу на воєнну безпеку держави;

збір, узагальнення та систематизацію даних про факти реалізації ІЗ.

На *підсистему протидії ІЗ* доцільно покласти такі завдання:

безпосередню підготовку і проведення заходів відповідно до плану протидії ІЗ;

захист об'єктів державної та військової інформаційної інфраструктури, органів державної влади, органів військового управління, населення та особового складу Збройних Сил України та інших визначених законом військових формувань від деструктивного інформаційно-психологічного впливу;

ведення інформаційної боротьби у формі інформаційних операцій, акцій та окремих спеціальних заходів.

На *підсистему контролю та оцінювання ефективності функціонування СЗІБ* доцільно покласти такі завдання:

контроль роботи всіх підсистем і елементів СЗІБ та оцінювання ефективності їх функціонування;

постійний моніторинг результатів реалізації пасивних і активних заходів з протидії ІЗ та оцінювання їх ефективності;

вироблення необхідних поправок для корегування плану протидії ІЗ у разі невідповідності реальних результатів протидії запланованим.

На *підсистему всебічного забезпечення функціонування СЗІБ* доцільно покласти такі завдання:

забезпечення необхідних умов функціонування всіх складових системи матеріальними, фінансовими та іншими ресурсами.

На *підсистему підготовки кадрів та наукового супроводження* доцільно покласти такі завдання:

удосконалення і розвиток системи підготовки кадрів за напрямом забезпечення інформаційної безпеки;

організацію фундаментальних та прикладних наукових досліджень за напрямом забезпечення інформаційної безпеки.

Висновки та перспективи подальших досліджень

Формування ефективної СЗІБ у складі СЗВБД та її удосконалення є надзвичайно актуальним завданням в умовах гібридного й, у першу чергу, інформаційного впливу країни-агресора.

СЗІБ необхідно створювати, виходячи з функцій і завдань, які вона повинна виконувати, та базуючись на визначених принципах побудови і функціонування складної системи, з урахуванням підпорядкованості СЗВБД та прогнозованого розвитку інформаційного середовища і можливих ІЗ у майбутньому.

Визначені в статті мета, завдання, функції і принципи побудови СЗІБ та її концептуальна структура є основою для подальших досліджень ефективності функціонування цієї системи.

Список літератури

1. Радковець Ю.І. Ознаки технологій "гібридної війни" в агресивних діях Росії проти України / Ю.І. Радковець // Наука і оборона. – 2014. – № 3. – С. 36–42.

2. Горбулін В.П. Проблеми захисту інформаційного простору України: монографія / В.П. Горбулін, М.М. Биченок. Ін-т пробл. нац. безпеки. – К.: Інтертехнологія, 2009. – 136 с.

3. Толубко В.Б. Концептуальні основи інформаційної безпеки України / В.Б. Толубко, С.Я. Жук, В.О. Косевцов // Наука і оборона. – 2004. – № 2. – С. 19-25.

4. Пєвцов Г.В. Концептуальні підходи щодо забезпечення інформаційної безпеки / Г.В. Пєвцов, С.В. Залкин, А.О. Феклістов // Інформаційна безпека. – 2011. – № 2. – С. 57-59.

5. Теоретико-методологічні засади забезпечення національної безпеки держави у її визначальних сферах: монографія / В.Ю. Богданович, А.І. Семенченко, Ю.В. Єгоров та ін. – К.: Кий, 2007. – 370 с.

6. Рось А.О. Щодо удосконалення системи інформаційної безпеки держави / А.О. Рось // Матер. міжвуз. наук.-практ. конф. – Житомир: ЖВІ НАУ. – 2009. – С. 14-19.

7. Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення : монографія / Г.В. Пєвцов, С.В. Залкін, С.О. Сідченко, К.І. Хударковський. – Х.: Цифрова друкарня № 1, 2013. – 270 с.

8. Воєнна доктрина України, затв. Указом Президента України від 24 вересня 2015 р. № 555/2015 [Електронний ресурс]. – Режим доступу до ресурсу: http://www.president.gov.ua/documents/5552015-19443.

9. Доктрина інформаційної безпеки України, затв. Указом Президента України від 25 лютого 2017 р. № 47/2017 [Електронний ресурс]. – Режим доступу до ресурсу: http://www.president.gov.ua/documents/472017-21374.

10. Стратегія національної безпеки України, затв. Указом Президента України від 26 травня 2015 р. № 287/2015 [Електронний ресурс]. – Режим доступу до ресурсу: http://zakon3.rada.gov.ua/laws/show/287/2015.

11. Концепція розвитку сектору безпеки і оборони України, затв. Указом Президента України від 14 березня 2016 р. № 92/2016 [Електронний ресурс]. – Режим доступу до ресурсу: http://www.president.gov.ua/documents/922016-19832.

12. Про основи національної безпеки України: Закон України від 15 грудня 2005 р. № 3200-IV [Електронний ресурс]. – Режим доступу до ресурсу: http://zakon3.rada.gov.ua/laws/show/964-15.

13. Косогов О.М. Методика визначення структури системи інформаційної безпеки Міністерства оборони та Збройних Сил України / О.М. Косогов, А.О. Сірик // Зб. наук. праць Харк. нац. ун-ту Повітряних Сил. – Х.: ХНУПС, 2017. – Вип. 3 (52). – С. 30-34.

Reference

1. Radkovecj, Ju.I. (2014), “Oznaky tekhnologhij "ghibrydnoji vijny" v aghresyvnykh dijakh Rosiji proty Ukrajiny” [Symptoms of "hybrid war" technology in Russia's aggressive actions against Ukraine], *Science and defense*, No. 2, pp. 36-42.

2. Ghorbulin, V.P. and Bychenok, M.M. (2009), “*Problemy zakhystu informacijnogho prostoru Ukrajiny*” [*Problems of protecting the informational space of Ukraine*], Intertekhnologhija, Kyiv, 136 p.

3. Tolubko, V.B., Zhuk, S.Ja. and Kosevcov, V.O. (2004), “Konceptualjni osnovy informacijnoji bezpeky Ukrajiny” [Conceptual foundations of Ukraine's information security], *Science and defense*, No. 2, pp. 19-25.

4. Pjevcov, Gh.V., Zalkyn, S.V. and Feklistov, A.O. (2011), “Konceptualjni pidkhody shhodo zabezpechennja informacijnoji bezpeky” [Conceptual approaches to information security], *Informational security*, No. 2, pp. 57-59.

5. Boghdanovych, V.Ju., Semenchenko, A.I., Jeghorov, Ju.V., Bortnyk, O.O. and Mukha, V.A. (2007), “Teoretyko-metodologhichni zasady zabezpechennja nacionaljnoji bezpeky derzhavy u jiji vyznachaljnykh sferakh” [Theoretical and methodological principles of ensuring the national security of the state in its defining spheres], Kyj, Kyiv, 370 p.

6. Ros, A.O. (2009), “Shchodo udoskonalennia systemy informatsiinoi bezpeky derzhavy” [Concerning the improvement of the state information security system], *Materials of the inter-university scientific-practical conference*, Zhytomyr, pp. 14-19.

7. Pievtsov, H.V., Zalkin, S.V., Sidchenko, S.O. and Khudarkovskyi, K.I. (2013), “*Informatsiina bezpeka u voiennii sferi: problemy, metodolohiia, systema zabezpechennia*” [*Information security in the military sphere: problems, methodology, security system*], Tsyfrova drukarnia No. 1, Kharkiv, 270 p.

8. The decree of the President of Ukraine (2015), "*Voienna doktryna Ukrainy, zatv. Ukazom Prezydenta Ukrainy vid 24 veresnia 2015 r. No. 555/2015*" [*Military Doctrine of Ukraine, approved by the Decree of the President of Ukraine dated September 24, 2015, No. 555/2015*], www.president.gov.ua/documents/5552015-19443.

9. The decree of the President of Ukraine (2017), "*Doktryna informatsiinoi bezpeky Ukrainy, zatv. Ukazom Prezydenta Ukrainy vid 25 liutoho 2017 r. No. 47/2017*" [*Doctrine of Information Security of Ukraine, approved by the Decree of the President of Ukraine dated February 25, 2017 No. 47/2017*], www.president.gov.ua/documents/472017-21374.

10. The decree of the President of Ukraine (2015), "*Stratehiia natsionalnoi bezpeky Ukrainy, zatv. Ukazom Prezydenta Ukrainy vid 26 travnia 2015 r. No. 287/2015*" [*National Security Strategy of Ukraine, approved by the Decree of the President of Ukraine dated May 26, 2015, No. 287/2015*], zakon3.rada.gov.ua/laws/show/287/2015.

11. The decree of the President of Ukraine (2016), "*Kontseptsiia rozvytku sektoru bezpeky i oborony Ukrainy, zatv. Ukazom Prezydenta Ukrainy vid 14 bereznia 2016 r. No. 92/2016*" [*Concept of development of the security and defense sector of Ukraine, approved by a Decree of the President of Ukraine dated March 14, 2016, No. 92/2016*], www.president.gov.ua/documents/922016-19832.

12. Law of Ukraine (2005), "*Pro osnovy natsionalnoi bezpeky Ukrainy: Zakon Ukrainy vid 15 hrudnia 2005 r. No. 3200-IV*" [*On the Fundamentals of National Security of Ukraine: Law of Ukraine dated December 15, 2005 No. 3200-IV*], zakon3.rada.gov.ua/laws/show/964-15.

13. Kosogov, O.M. and Siryk, A.O. (2017), "Metodyka vyznachennia struktury systemy informatsiinoi bezpeky Ministerstva oborony ta Zbroinykh Syl Ukrainy" [Methodology for determining the structure of the information security system of the Ministry of Defense and Armed Forces of Ukraine], *Scientific works of Kharkiv National Air Force University*, No. 3 (52), pp. 30-34.

Надійшла до редколегії 12.11.2017
Схвалена до друку 1.02.2018

Відомості про автора:
Левченко Олександр Віталійович
кандидат військових наук професор
начальник Житомирського військового інституту
ім. С.П. Корольова
Житомир, Україна
e-mail: levch@i.ua

Information about the author:
Oleksandr Levchenko
Candidate of Science of Military Science Professor
Chef of S. Korolov Zhytomyr Military Institute,
Zhytomyr, Ukraine
e-mail: levch@i.ua

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ФОРМИРОВАНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.В. Левченко

В статье обоснован концептуальный подход к формированию системы обеспечения информационной безопасности как составляющей общегосударственной системы обеспечения военной безопасности. Определены цель, задачи, функции и разработаны принципы построения системы. С позиций системного подхода предложена базовая структура системы, которая состоит из функциональных подсистем. Очерчены назначение и задачи каждой подсистемы.

Ключевые слова: *цель, задача, функции, принципы построения, система обеспечения информационной безопасности.*

THE CONCEPTUAL PRINCIPLES OF FORMING THE SYSTEM OF ENSURING THE INFORMATION SECURITY

O. Levchenko

Forming the information security system as part of the national system of ensuring military security must be accomplished in accordance with the principles of implementing the national, military and information security strategy, taking into account foreign and national experience in protecting the information space and counteracting destructive foreign influence, as well as existing and predicted information threats to the state and its armed forces.

The main objective of creating the information security system as a component of the national system of ensuring military security is preventing and neutralizing information threats from foreign states, creating the conditions for ensuring the performance of designated tasks by the Ministry of Defense of Ukraine, the Armed Forces of Ukraine, and other subjects of Ukraine's security and defense sector.

The formation of an effective information security system as part of the national system of ensuring military security and its improvement are extremely important under the conditions of the hybrid and, above all, informational influence of the aggressor country.

The information security system needs to be formed proceeding from the functions and tasks that it must perform and based on the specified principles of the construction and operation of a complex system, taking into account the subordination to the national system of ensuring military security, as well as the predicted development of the information environment and possible future information threats.

The author develops the structural principles of the information security system, which, unlike the known ones, take into account the peculiarities inherent to this system.

Keywords: *aim, task, functions, principles of formation, system of ensuring information security.*