Юрій Радковець,
Олександр Левченко,
Олександр Косогов

Погляди на створення системи інформаційної безпеки України та її Збройних Сил

На основі аналізу досвіду іноземних держав з формування системи підтримання інформаційної безпеки у сфері оборони запропоновано підхід до створення такої системи в Україні як сукупності взаємопов'язаних функціональних підсистем з визначенням функцій кожної з них.

Бурхливий розвиток інформаційних технологій і їх проникнення у всі сфери людської діяльності призвів на рубежі нового тисячоліття до нової трансформації в розвитку людства: світова спільнота рішуче перейшла від постіндустріальної ери до інформаційної. Однак нова ера разом з величезними перевагами принесла людству й нові загрози – фактично розпочалася ера інформаційного протиборства.

На сьогодні інформаційна боротьба стає однією з важливих, а не рідко й основних форм вирішення суперечностей між державами, і в цій боротьбі шляхом проведення інформаційних операцій досягаються стратегічні цілі [1–4].

В умовах перманентного інформаційного протиборства у світі стрімко зростає рівень та значно розширюється спектр інформаційних загроз. Така ситуація становить серйозну небезпеку національній і міжнародній безпеці та призводить до важкопрогнозованих і часом непередбачуваних наслідків у воєнно-політичній, економічній, військово-технічній, екологічній та інформаційній сферах.

Не залишається осторонь світових тенденцій і Україна, яка, з огляду на своє геополітичне положення, існуючу навколо неї воєнно-політичну обстановку та наявність досить розвиненої інформаційної інфраструктури, перебуває під потужним іноземним інформаційним впливом. Маючи системний і цілеспрямований характер, зовнішній негативний інформаційний вплив призводить у підсумку до появи загроз національній безпеці України в інформаційній сфері, які завдають державі відчутних збитків. Особливо це стосується виконання завдань оборони країни, оскільки ця діяльність безпосередньо спрямована на захист національних інтересів держави від зовнішніх загроз і пов'язана з підготовкою та веденням війни з можливим агресором.

На заваді цим загрозам може стати лише ефективна система протидії інформаційному впливу, яка забезпечуватиме прийнятний рівень інформаційної безпеки в Україні.

На сьогодні в нашій державі та її Збройних Силах ще не до кінця створено цілісну систему інформаційної безпеки, яка б у повному обсязі забезпечувала гарантований захист і надійну протидію інформаційним загрозам. Разом з тим, триває інтенсивний процес її формування, зокрема в Міністерстві оборони України розроблені концептуальні документи і плани щодо розгортання такої системи, у Збройних Силах України створюються відповідні підрозділи.

Однак відсутність власного досвіду формування зазначеної системи та різноплановість поглядів на шляхи підтримання інформаційної безпеки у сфері оборони держави, складність вивчення питань інформаційної безпеки у воєнній сфері, котра полягає в слабко виявлених зв'язках між елементами всієї системи, не дає змоги повною мірою визначити структуру системи інформаційної безпеки цієї сфери, її завдання та функції. Тому розробка

науково обґрунтованих підходів до створення дієвої системи гарантування інформаційної безпеки держави у сфері оборони з урахуванням досвіду іноземних держав є актуальним науково-практичним завданням.

Інформаційними загрозами стосовно нашої держави, як визначено в Законі України «Про основи національної безпеки України» [5], можуть бути:

- прояви обмеження свободи слова та доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації;
- 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;
- комп'ютерна злочинність та комп'ютерний тероризм.

У затвердженій 8 липня 2009 р. відповідним указом Президента держави Доктрині інформаційної безпеки України [6] ці загрози деталізуються й водночас систематизуються за сферами, у яких вони можуть реалізовуватися: зовнішньополітичній, воєнній, внутрішньополітичній, економічній, соціальній, гуманітарній, науково-технологічній та інших.

Разом з тим, за оцінками вітчизняних експертів з проблем інформаційної безпеки [7–9], сформованими на основі аналізу іноземного впливу на інформаційний медіа- та кіберпростір України, існують ознаки реальних загроз для нашої держави. Про це свідчать такі основні тенденції:

- цілеспрямоване формування окремими іноземними державами негативного міжнародного іміджу України;
- активізація критики вищого державного керівництва України;
- здійснення низкою зарубіжних країн потужного інформаційного тиску на Україну з метою спонукання українського керівництва до прийняття вигідних для цих країн рішень у внутрішньо- та зовнішньополітичній сферах;
- посилення інформаційних заходів з перешкоджання реалізації Україною її зовнішньополітичного курсу та спонукання її до участі в проектах, які в сучасних умовах не вигідні нашій державі;
- дискредитація нашої держави як конкурента у сфері міжнародного військово-технічного співробітництва;
- зростання для України загроз кібернетичних атак, що зумовлено появою нових, більш досконалих зразків кібернетичної зброї.

Крім того, новим джерелом загроз інформаційній безпеці України слід вважати соціальні мережі, які можуть використовуватись окремими країнами для просування власної ідеології у світі та впливу на ситуацію в нашій країні.

Реалізація зазначених інформаційних загроз може завдати суттєвих збитків нашій державі та її Збройним Силам, що в підсумку призводитиме до зниження обороноздатності України [10, 11].

Аналіз іноземного досвіду захисту інформаційної інфраструктури держави від кіберзагроз та протидії зовнішньому інформаційному впливу на власне населення та особовий склад збройних сил свідчить [12–13], що багатьма країнами світу створені національні системи інформаційної безпеки. Причому в провідних державах світу, котрі розглядають **інформаційну безпеку виключно з позицій системного підходу**, такі системи мають загальні ключові ознаки:

- ієрархічність побудови системи;
- управління та координація діяльності структурних підрозділів системи на найвищому державному рівні;
- наявність спеціально створеного не дорадчого, а керівного органу системи;
- чітка організація взаємодії між складовими системи.

Загальне керівництво системою здійснюється, як правило, головою виконавчої влади через відповідний робочий орган, який розробляє державну інформаційну політику й координує діяльність її складових елементів, якими є підсистеми інформаційної безпеки визначених державних структур (наприклад Міністерства оборони, Міністерства внутрішніх справ, інших відомств), котрі, у свою чергу, мають у своєму складі підрозділи виявлення, аналізу та протидії інформаційним загрозам як інформаційно-психологічної, так і кібернетичної спрямованості.

Найдосконаліші та найпотужніші системи інформаційної безпеки побудовані й успішно функціонують у США, Великій Британії, Ізраїлі, Китаї та деяких інших державах, які є об'єктами постійного потужного зовнішнього інформаційного впливу. Причому зазначені системи цих країн мають і достатню активну складову, завдяки чому існує можливість проведення інформаційно-психологічних заходів та кібернетичних атак проти країн – супротивників.

У деяких країнах (Туреччині, Ірані, Іспанії) процес створення системи інформаційної безпеки триває, в інших цей процес лише започаткований. Разом з тим, низка європейських країн, зокрема Польща, Болгарія, Румунія, Словаччина, Угорщина, Чехія та інші, не створюють цілісних систем інформаційної безпеки, а зосереджуються на побудові окремих її елементів, зокрема кібернетичної безпеки, але в усіх випадках створення системи інформаційної безпеки пов'язане передусім з наявністю реальних кібернетичних загроз для об'єктів критичної інфраструктури цих країн.

У збройних силах іноземних держав системи інформаційної безпеки загалом побудовані за подібними підходами, але з урахуванням національних особливостей (*рис. 1*). При цьому країни, які входять до певних воєнно-політичних блоків, будують відомчі системи інформаційної

Рис. 1. Узагальнена схема побудови системи інформаційної безпеки іноземних держав у сфері оборони

безпеки відповідно до принципу розподіленості зусиль у рамках колективних систем безпеки.

Цей досвід може застосовуватися для побудови системи інформаційної безпеки як нашої держави, так і її Збройних Сил. Але при формуванні системи інформаційної безпеки держави у сфері оборони обов'язково слід ураховувати геополітичне положення нашої країни, її позаблоковий стан та національні особливості.

Основною метою створення системи гарантування інформаційної безпеки держави у сфері оборони (далі – Системи) є запобігання та нейтралізація інформаційних загроз їх функціонуванню; створення умов для сталого й гарантованого виконання Міністерством оборони України та Збройними Силами України завдань, визначених Конституцією та законами України.

Відповідно до зазначеної мети, основними функціями такої Системи доцільно визначити:

1. Створення й забезпечення діяльності організаційних структур та елементів Системи, зокрема:

• розроблення адміністративно-правових засад для побудови та функціонування Системи;

• усебічне забезпечення діяльності елементів Системи.

2. Управління Системою, зокрема:

• розроблення та введення в дію Керівництва із підтримання інформаційної безпеки в Міністерстві оборони та Збройних Силах України, у якому визначаються єдині підходи до запобігання та нейтралізації інформаційних загроз;

• прогнозування, планування, організація, координація та контроль у межах Системи та окремих її елементів;

• оцінювання результативності заходів протидії інформаційним загрозам, витрат на їх підготовку та проведення.

3. Проведення планової та оперативної діяльності з підтримання інформаційної безпеки та протидії інформаційним загрозам, зокрема:

• визначення та формування моделі потенційних і реальних інформаційних загроз;

• визначення об'єктів критичної інфраструктури, які мають важливе значення для національної безпеки та оборони;

• виявлення інформаційних загроз, джерел їх виникнення, а також прогнозування можливих наслідків у разі їх реалізації з відпрацюванням відповідних превентивних заходів;

• удосконалення форм, методів і засобів запобігання загрозам інформаційній безпеці та ліквідація наслідків її порушення.

З метою визначення елементів Системи та їх завдань, доцільно розглянути її як організовану сукупність взаємопов'язаних функціональних підсистем:

• виявлення інформаційних загроз;

• аналізу і прогнозування загроз та планування заходів інформаційної безпеки;

• протидії інформаційним загрозам;

• захисту від інформаційних загроз;

• наукових досліджень та підготовки спеціалістів з питань інформаційної безпеки.

На ці підсистеми можуть бути покладені такі завдання.

На **підсистему виявлення інформаційних загроз:**

• виявлення загроз національній безпеці України в інформаційній сфері;

• виявлення ознак інформаційно-психологічного впливу на особовий склад Збройних Сил України;

• виявлення джерел, які можуть спричинити витік інформації з обмеженим доступом;

• виявлення кібернетичних загроз функціонуванню інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем;

• виявлення невідповідностей стану та можливостей інформаційно-телекомунікаційних систем та інших інформаційних систем військового призначення сучасним вимогам;

• виявлення апаратних та програмних закладок на об'єктах інформаційної діяльності Збройних Сил України.

На **підсистему аналізу і прогнозування загроз та планування заходів інформаційної безпеки:**

• збирання, узагальнення та систематизація даних про інформаційні загрози, їх оцінювання та прогнозування їх розвитку;

• збирання, узагальнення та систематизація даних про факти інформаційно-психологічного впливу на керівництво та населення держави, особовий склад Збройних Сил України;

• оцінювання джерел інформаційно-психологічного та інформаційно-технічного впливу;

• визначення об'єктів критичної інфраструктури;

• планування заходів інформаційної боротьби.

На **підсистему протидії інформаційним загрозам:**

• адекватне реагування на кризові ситуації в інформаційному просторі;

• підготовка та ведення інформаційно-психологічних операцій (заходів);

• інформаційно-аналітичне забезпечення заходів реагування на кризові ситуації, що спричинюються інформаційними загрозами;

• комплектування, забезпечення, підготовка та управління застосуванням сил і засобів захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах.

На **підсистему захисту від інформаційних загроз:**

• захист інформаційного простору від кібератак у мирний час та в особливий період;

• проведення заходів захисту об'єктів критичної інфраструктури;

• контроль використання інформації з обмеженим доступом;

• захист особового складу Збройних Сил України від негативного інформаційно-психологічного впливу.

На **підсистему наукових досліджень та підготовки спеціалістів з питань інформаційної безпеки:**

• замовлення проведення науково-дослідних та дослідно-конструкторських робіт за напрямами інформаційної безпеки;

• формування державного замовлення й підготовка спеціалістів тактичного, оперативно-тактичного та оперативно-стратегічного рівнів з питань захисту інформації, інформаційної безпеки держави у воєнній сфері, інформаційної боротьби, інформаційно-аналітичного забезпечення органів військового управління.

Висновок

Досвід іноземних країн свідчить, що забезпечення надійної протидії сучасним викликам і загрозам національній безпеці України в інформаційній сфері можливе лише за умови формування та проведення єдиної державної інформаційної політики та системного підходу до організації захисту національного інформаційного простору. Виходячи із цього, для гарантування інформаційної безпеки Збройних Сил України доцільно формувати відомчу систему підтримання інформаційної безпеки як складову загальнодержавної системи, яка структурно має складатися із взаємопов'язаних функціональних підсистем: виявлення інформаційних загроз; аналізу і прогнозування загроз та планування заходів інформаційної безпеки; протидії інформаційним загрозам; захисту від інформаційних загроз; наукових досліджень; підготовки спеціалістів з питань інформаційної безпеки.

Такий підхід дасть змогу побудувати раціональну систему інформаційної безпеки держави у сфері оборони та забезпечити підвищення загальної ефективності протидії загрозам у інформаційному просторі України.

Перелік літератури

1. *Горбулін В. П.* Проблеми захисту інформаційного простору України: монографія / В. П. Горбулін, М. М. Биченок. – К. : Інтертехнологія, 2009. – 136 с.

2. *Толубко В. Б.* Складові інформаційної боротьби / В. Б. Толубко, А. О. Рось // Наука і оборона. – 2002. – № 2. – С. 23–28.

3. *Богуш В. М.* Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. – К. : МК-Прес, 2005. – 432 с.

4. *Галушко С. О.* Протиборство в інформаційному просторі / С. О. Галушко // Оборонний вісник. – 2011. – № 11. – С. 16–19.

5. Закон України № 964-IV «Про основи національної безпеки України» від 19 червня 2003 р.

6. Доктрина інформаційної безпеки України [затверджена указом Президента України від 8 липня 2009 року № 514/2009]. – К. : Офіційний вісник України, 2009. – № 52.

7. *Жарков Я. М.* Напрями зовнішнього інформаційно-психологічного впливу на Україну / Я. М. Жарков // Сучасні інформаційні технології у сфері безпеки та оборони. – 2009. – № 1 (4). – С. 42–46.

8. *Жук С. Я.* Тенденції та перспективи розвитку інформаційної боротьби й інформаційної зброї / С. Я. Жук, В. О. Чмельов, Т. М. Дзюба // Наука і оборона. – 2006. – № 2. – С. 35–41.

9. *Рось А. О.* Щодо удосконалення системи інформаційної безпеки держави / А. О. Рось // Матеріали міжвузівської науково-практичної конференції. – Житомир : ЖВІ НАУ, 2009. – С. 14–19.

10. *Богданович В. Ю., Семенченко А. І., Єгоров Ю. В., Бортник О. О., Муха В. А.* Теоретико-методологічні засади забезпечення національної безпеки держави у її визначальних сферах : монографія / В. Ю. Богданович, А. І. Семенченко, Ю. В. Єгоров, О. О. Бортник, В. А. Муха. – К. : Кий, 2007. – 370 с.

11. *Ожеван М. А.* Основні напрями зовнішніх інформаційно-маніпулятивних впливів на суспільні трансформації в Україні: засоби протидії / М. А. Ожеван // Стратегічні пріоритети. – 2011. – № 3. – С. 118–126.

12. *Ноговицын А. А.* В центре внимания – информационная безопасность / А. А. Ноговицын // Красная звезда. – 2009. – 27 февр.

13. Война в киберпространстве: уроки и выводы для России // Независимое военное обозрение. – 2013. – № 46 (787). – С. 1–4.

Надійшла до редакції 15 січня 2014 р.