УДК 621.263

Антон Миколайович Білан
Олександр Володимирович Зеленко
Олександр Віталійович Шемендюк

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Постановка проблеми. Аналіз останніх досліджень та публікацій

Одним з основних джерел загроз національній безпеці держави є інформаційні війни, які розвиненими країнами розглядаються як один з найбільш ефективних засобів забезпечення національних інтересів. Для їх проведення, в цих країнах і в першу чергу в США, розроблені концепції інформаційної війни. Принципові рішення з цих питань приймає воєнно-політичне керівництво країн. Створені розвинені системи інформаційних і психологічних операцій, основна складова яких розгорнута в збройних силах. Вони оснащені сучасними засобами і технологіями інформаційного впливу, набули значного практичного досвіду під час проведення реальних інформаційних і психологічних операцій та навчань, відпрацьована тісна взаємодія між усіма задіяними відомствами, налагоджена система різнобічної підготовки фахівців.

Концепція інформаційної війни США покладена в основу аналогічної концепції Об'єднаних збройних сил НАТО. Сили психологічних операцій динамічно розвивають суміжні з Україною держави. Велика увага забезпеченню інформаційної безпеки держави приділяється в Росії, де створена чітка вертикальна система державних органів на чолі з Міжвідомчою комісією Ради безпеки РФ [4].

Як свідчить досвід локальних війн і збройних конфліктів, а також події навколо Іраку, Афганістану в сучасній війні неможливо досягти поставлених цілей без постійного здійснення заходів інформаційної боротьби не тільки до початку та в ході війни, але й після її закінчення. Крім того, у мирний час інформаційна боротьба стає важливою складовою потенціалу стримування [2]. Можливість втягнення України в інформаційне протиборство обумовлена її геополітичним положенням, наявністю політичних, економічних та інших інтересів щодо нашої держави з боку провідних та суміжних країн.

Виклад основного матеріалу

Наприкінці двадцятого сторіччя прискорився глобальний світовий процес переходу від "індустріального суспільства" до "суспільства інформаційного". Ця фаза розвитку людства отримала назву інформаційної або третьої хвилі і пов'язана з революційними досягненнями в галузі інформаційних технологій. Відбуваються кардинальні зміни в виробництві, світогляді людей, міждержавних відношеннях. Рівень розвитку інформаційної сфери вирішальним чином впливає на економіку, обороноздатність і політику держави. Від цього значною мірою залежить поведінка людей, соціальна стабільність.

Для реалізації власних національних інтересів провідні держави світу активно розробляють та втілюють у життя концепції інформаційної війни (ІВ) (information warfare), які забезпечують можливість впливу через інформаційну сферу на політичну, економічну, воєнну ситуацію в інших країнах. Саме тому інформаційна безпека починає відігравати одну з ключових ролей у забезпеченні національної безпеки будь-якої країни [3].

Згідно зі ст.17 Конституції України, забезпечення інформаційної безпеки стоїть на одному рівні із захистом суверенітету й територіальної цілісності країни, забезпеченням її економічної безпеки.

На сьогодні основним керівним документом щодо забезпечення інформаційної безпеки є Закон України "Про основи національної безпеки України", який був прийнятий 19 червня 2003 року. Він визначає серед основних сфер національної безпеки й інформаційну сферу.

На рис. 1 показано, що складові інформаційної сфери країни визначені як сукупність інформаційної інфраструктури, інформаційних ресурсів і суб'єктів, які проводять збір, формування, розповсюдження та використання інформації, а також системи регулювання суспільних відносин, що при цьому виникають.

Суб'єктами діяльності в інформаційній сфері виступають: особа, суспільство та держава. Головним об'єктом діяльності (предметом виробництва, продуктом) є інформаційні ресурси – які розглядаються як організована сукупність інформаційних продуктів певного призначення, необхідних для забезпечення інформаційних потреб громадян, суспільства, держави у визначеній сфері життя чи діяльності. Суб'єктами

Рис.1. Складові інформаційної сфери країни

діяльності в інформаційній сфері виступають: особа, суспільство та держава. Головним об'єктом діяльності (предметом виробництва, продуктом) є інформаційні ресурси – які розглядаються як організована сукупність інформаційних продуктів певного призначення, необхідних для забезпечення інформаційних потреб громадян, суспільства, держави у визначеній сфері життя чи діяльності. Перехід світового суспільства до інформаційної цивілізації перетворює інформаційний ресурс на стратегічний чинник розвитку країни.

Засобами діяльності є інформаційна інфраструктура – сукупність систем, що забезпечують, накопичення, зберігання, поширення й виробництво інформаційних продуктів, а також інформаційні технології, сервісне обслуговування інформаційних систем, підготовка кадрів.

Інформаційна інфраструктура України перебуває в процесі становлення і розвивається досить нерівномірно. Окремі її складові (друковані ЗМІ, книговидання, бібліотечний, архівний та кінематографічний комплекси) не відповідають стандартам розвинутих країн, зазнають подальшого скорочення і навіть руйнування; інші (Інтернет, мобільний зв'язок) — хоч і не досягли рівня передових держав, однак виявляють стійку тенденцію до зростання.

Складовими системи регулювання суспільних відносин в інформаційній сфері виступають:

нормативно-правова база – сукупність законів і законодавчих актів в інформаційній сфері;

система забезпечення інформаційної безпеки – організована державою сукупність суб'єктів (державних органів, посадових осіб, громадських організацій, окремих громадян), об'єднаних цілями та завданнями захисту національних інтересів країни в інформаційній сфері;

інформаційний ринок – ринок інформаційних продуктів і послуг, а також інформаційних технологій, засобів зв'язку, інформатизації і телекомунікації.

Безпосередньо середовище, де здійснюється формування, збереження та поширення інформації отримало назву інформаційного простору. Національний інформаційний простір – це вся сукупність інформаційних потоків, що доступні з території держави.

Геополітичні наслідки цифрової революції обумовили можливості глобального впливу на національний інформаційний простір різних країн в тому числі і України. Геополітичними особливостями сучасного національного інформаційного простору є:

- відсутність звичних географічних і державних кордонів;
- зниження значимості фактору відстані в політичних процесах та відношеннях;

- важка національна і державна ідентифікація (належність) його суб'єктів і об'єктів;
- можливість вирішувати задачі протягом усього геополітичного простору у єдиному масштабі часу;
- забезпечення воєнно-політичних комунікацій з будь-якими державами і територіями без посередників;
- можливість здійснення анонімного доступу до інформаційних, в тому числі конфіденційних ресурсів інших держав.

Виділення інформаційної сфери як окремої сфери національної безпеки дозволяє сформувати цілісне уявлення про стан, проблеми, основні тенденції інформаційної безпеки країни. Особливістю є те, що інформаційна складова у вигляді інформаційних ресурсів, елементів інформаційної інфраструктури, індивідуальної та суспільної свідомості також присутня в інших сферах національної безпеки. Інформаційна складова в інших сферах національної безпеки теж впливає на ступінь захищеності та реалізації національних інтересів.

До основних об'єктів інформаційної безпеки у воєнній сфері належать:

- інформаційна інфраструктура центральних органів воєнного управління та органів воєнного управління видів Збройних Сил, об'єднань, з'єднань, військових частин і організацій, які входять до складу Збройних Сил, навчальних закладів, науково-дослідних установ Міністерства оборони;
- інформаційні ресурси підприємств оборонного комплексу і науково-дослідних установ, які займаються оборонною проблематикою;
- програмно-технічні засоби та інформаційні ресурси автоматизованих і автоматичних систем управління військами й зброєю, озброєння і воєнної техніки, оснащених засобами інформатизації;
- керівний і особовий склад Збройних Сил.
- Основними зовнішніми загрозами інформаційній безпеці у воєнній сфері є [1]:
- усі види розвідувальної діяльності закордонних країн, які спрямовані проти інтересів держави у воєнній сфері;
- інформаційно-технічні впливи на інформаційну інфраструктуру й інформаційні ресурси у воєнній сфері з боку інших країн;
- інформаційно-психологічні впливи на особовий і керівний склад Збройних Сил з боку інших країн;
- інформаційна діяльність іноземних політичних, економічних і воєнних структур, спрямована проти національних інтересів у воєнній сфері.
- До основних внутрішніх загроз інформаційної безпеки у воєнній сфері можна віднести:
- порушення встановленого регламенту збору, обробки, збереження і передачі інформації, яка знаходиться в штабах у установах Міністерства оборони, на підприємствах оборонного комплексу;
- навмисні дії, а також помилки персоналу інформаційних і телекомунікаційних систем спеціального призначення;
- ненадійне функціонування інформаційних і телекомунікаційних систем спеціального призначення;
- можлива інформаційно-пропагандистська діяльність, що підриває престиж Збройних Сил та їх боєготовність;
- невирішеність питань захисту інтелектуальної власності підприємств оборонного комплексу, яка призводить до витоку за кордон найцінніших державних інформаційних ресурсів;
- невирішеність питань соціального захисту військовослужбовців і членів їх сімей.

Але складним і небезпечним явищем не тільки для воєнної, а і для інших сфер національної безпеки стала розробка концепцій і підготовка до ведення інформаційних війн. Неминучість інформаційних війн обумовлена насамперед економічною, військовою доцільністю, а висока ймовірність втягнення в неї України - її геополітичним положенням і наявністю політичних, економічних та інших інтересів щодо нашої держави.

Висновки

Таким чином, можна стверджувати, що нові технології кінця двадцятого сторіччя докорінно змінили взаємовідносини між країнами, форми і способи ведення збройної боротьби, а також і саме суспільство. Проведений аналіз переконливо свідчить, що інформаційні війни є реальністю, ігнорування якої у наш час є неприпустимим. Країни, які не мають розробленої стратегії щодо забезпечення власної інформаційної безпеки, ризикують залишитися на узбіччі світової цивілізації. Така перспектива загрожує новим поділом країн світу за ознакою рівня розвитку інформаційної сфери.

Як свідчить досвід локальних війн і збройних конфліктів кінця XX, початку XXI століття, інформаційна боротьба виступає як фактор тиску, так і фактор стратегічного стримування. Створення некерованості державної системи, деморалізація населення країни з одного боку можуть привести до досягнення воєнно-політичних та економічних інтересів без ведення бойових дій або стати вирішальним фактором досягнення успіху в операції, яка готується вже на її початковому етапі, а з іншого – може виступити одним з головних аргументів щодо відмови противника від агресивних планів.

Ефективність інформаційної боротьби залежить від оперативності, цілеспрямованості, безперервності й чіткості в її організації та веденні. Основними завданнями Збройних Сил України щодо підготовки та ведення інформаційної боротьби повинні стати:

– налагодження тісної взаємодії між усіма складовими інформаційної боротьби в інтересах ефективного вирішення її завдань;

– організація операцій щодо деморалізації збройних сил противника і одночасному проведенні заходів по забезпеченню психологічної стійкості своїх військ;

– комплексне проведення заходів інформаційної боротьби з метою випередження противника у кількості, якості, оперативності інформації, необхідної для організації і ведення бойових дій при одночасному захисті інформації про свої війська;

– введення в практику роботи органів військового управління всіх ланок під час операцій (бойових дій) заходів щодо планування і здійснення введення противника в оману;

– формування спеціальних сил ведення програмно-комп'ютерної боротьби, їх всебічне оснащення і якісна підготовка до здійснення спеціальних заходів в комп'ютерних мережах;

– втілення нових, а також удосконалення і ефективне застосування наявних інформаційних технологій;

– постійне вдосконалення прийомів, способів і засобів захисту інформації в інформаційних система всіх типів – соціальних, технічних, соціотехнічних;

– налагодження взаємодії з питань інформаційної боротьби з органами виконавчої влади, іншими міністерствами і відомствами;

– організація і проведення навчань з питань підготовки і ведення інформаційної боротьби в тому числі і на міжвідомчому рівні.

Але ж, проблема розвитку інформаційної боротьби не обмежується лише інтересами Збройних Сил. Як свідчить досвід провідних країн світу вона спрямована на забезпечення інформаційної і національної безпеки країни в цілому і може бути вирішена лише на державному рівні шляхом прийняття відповідних рішень і створення необхідних структур.

Література

1. Лисичкин В.А., Шелепин Л.А. Третья мировая информационно-психологическая война – М.: ИСПИ АСН, 2000. **2. Волковский Н.Л.** История информационных воен. В 2 ч. Ч.2 / СПб.: ООО «Издательство Полигон», 2003. **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. Гриняев С.** Концепция ведения информационной войны в некоторых странах мира // Зарубежное военное обозрение. – 2002. – № 2. С.10-12.

В статье рассмотрена роль информационной безопасности в обеспечении национальной безопасности Украины. Рассмотрены составляющие информационной сферы и основные угрозы информационной безопасности в военной сфере. Определены основные задачи Вооруженных Сил Украины, что касается подготовки и ведения информационной борьбы.

Ключевые слова: информационная война, информационная безопасность.

In the article is considered role to information safety in provision of national safety of the Ukraine. They are considered forming information sphere and the main threats to information safety in military sphere. The certain primary tasks of Armed Forces of the Ukraine as to preparation and conduct of the information fight.

Key words: information war, information safety.