УДК004.738:351.852

Олег ПАНЧЕНКО
доктор медичних наук, професор, заслужений лікар України,
президент Громадської організації «Всеукраїнська професійна психіатрична ліга» директор ДЗ «Науково-практичний медичний реабілітаційно-діагностичний центр МОЗ України»
ORCID ID:0000-0001-9673-6685
oap@ukr.net

ІНФОРМАЦІЙНА СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Стаття присвячена інформаційній безпеці як складової національної безпеки. Представлено визначення поняття інформаційна безпека та національна безпека. Розглянуті питання інформаційної безпеки в умовах розвитку інформаційного суспільства та інформатизації. Проаналізовано вплив інформаційної безпеки на національну безпеку держави.

Інформаційна безпека суспільства держави визначається ступенем їх захищеності і стійкістю основних сфер життєдіяльності по відношенню до небезпечних, дестабілізуючих, деструктивних, що зачіпають інтереси країни інформаційних впливів на рівні як впровадження, так і вилучення інформації.

Рольінформації та інформаційнихтехнологій у сучасномусвіті є надзвичайно великою.Разом зі швидким розвитком сфери інформаційних технологій виникають нові та вдосконалюються уже відомі інформаційні ризики національній безпеці держави перед суспільством в цілому та кожного окремого громадянина.

У сучасних умовах інформаційна складова національної безпеки держави відіграє надзвичайно важливу роль через наявні в ній ризики та загрози, до яких доцільно відносити кібертероризм, кіберзлочинність, агресивну пропаганду, поширення антиконституційних та антидержавних гасел, обмеження доступу населення до публічної інформації тощо .

Суспільні інститути є повноцінними учасниками процесу забезпечення інформаційної безпеки держави. Як показує суспільно-політична практика, зусиль державних, як правило, не вистачає для ефективної протидії інформаційним загрозам, обумовлює потребу побудови діалогу з соціумом.

Базовими елементами механізму взаємодії між владою і суспільством у даній сфері є інституційна, нормативно-правова та практична складові. Від повноцінного використання всіх можливостей і ресурсів, наявних у суспільстві залежить ефективність функціонування всієї системи інформаційної безпеки держави.

Політика інформаційної безпеки повинна бути орієнтована на забезпечення гарантій інформаційного суверенітету України та інформаційної безпеки всіх суб'єктів сфери інформатизації, бо інформаційне забезпечення національної безпеки являє собою процес задоволення інформаційних потреб суб'єктів національної безпеки.

Характер інформаційних потреб суб'єктів національної безпеки визначає зміст інформаційного забезпечення національної безпеки.

Інформаційне забезпечення національної безпеки виконує важливу багатопланову роль у визначенні національних інтересів і пріоритетів національної безпеки. Для

забезпечення інформаційної безпеки держави необхідно всебічне задоволення потреб громадян, підприємств, установ і організацій всіх форм власності в доступі до достовірної та об'єктивної інформації; збереження і примноження духовних, культурних і моральних цінностей Українського народу; розвиток медіа-культури суспільства і соціально відповідальної медіа-середовища; формування ефективної правової системи захисту особистості, суспільства і держави від деструктивних пропагандистських впливів; створення на базі норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, перш за все, пропаганди; розвиток інформаційного суспільства.
Ключові слова: інформаційна безпека, національна безпека, інформація,інформаційний простір,ризики інформаційної безпеки,інформаційні технології, інформаційна війна.

1. ВСТУП

Постановка проблеми. Інформаційна безпека займає особливе місце взагальній системі національної безпеки держави, оскільки є елементом усіх складових системи безпеки, внаслідок чого одночасно набуває й автономного значення. Будь-які виклики чи загрози власне національній безпеці країни безпосередньо стосуються її інформаційного чинника. Сучасна українська соціально-економічна ситуація, недосконаліть організації державної влади та громадянського суспільства створюють широкий спектр внутрішніх загроз інформаційній безпеці країни. Актуальною є проблема створення і підтримки захищеного середовища інформаційного обміну, що реалізує правила і політику безпеки держави, тому що інформація давно перестала грати допоміжну роль, перетворившись на важливий і вагомий фактор зі своїми характеристиками, обумовленим прибутком, який можна отримати від її використання. Але можливий і варіант збитку, що наноситься власнику інформації шляхом несанкціонованого проникнення в інформаційну структуру і впливу на її компоненти.

Аналіз останніх досліджень і публікацій. Питання пов’язані з інформаційною безпекою, проблемами інформаційного суспільства та інформаційних війн досліджували такі науковці, якГ.М. Сащук, В. А. Ліпкан, М. В. Гуцалюк, О. Г. Данільян, О. П. Дзьобань, М. І. Пановта ін.

Дослідники відзначають існуючі та потенційні ризики у вітчизняній інформаційній сфері: незбалансованість політико-правової бази, відсутність необхідної інформаційної інфраструктури, проблеми входження української держави у світовий інформаційний простір тощо.

Мета статті. Дослідити теоретико-методологічні основи інформаційної безпеки як складової національної безпеки, що відіграє одну з ключових ролей у забезпеченні життєво важливих інтересів держави.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Безпека завжди була найважливішою метою і фундаментальною потребою як окремої людини, так і суспільства в цілому, так як становлення і розвиток людського суспільства завжди було пов'язано з подоланням різних загроз, які виходили від природи, ворогів, технічних об'єктів та інші. Отже, найважливішою умовою функціонування і розвитку людського суспільства є забезпечення безпеки. Високоякісна національна безпека потребує врахування соціально-політичних, економічних, правових, геополітичних, екологічних, техногенних та цілого ряду інших аспектів. Особливу роль у цьому відіграє інформаційне забезпечення національної безпеки.

Інформаційна безпека, як складова національної безпеки – стан захищеності життєво важливих інтересів людини, суспільства і держави, коли запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [1].

Інформаційна безпека регулюється рядом міжнародних стандартів та норм: CoBiT (Control Objectives for Information and Related Technology), ITIL (Information Technology Infrastructure Library), ISO/IEC 27001:2005, ISO/IEC 17799, ISO/IES 15408.

В Україні регулювання інформаційної безпеки здійснюється за допомогою таких нормативно-правових актів: Конституція України, Закон України «Про інформацію», Закон України «Про Національну програму інформатизації», Указ Президента України «Про Доктрину інформаційної безпеки України», Концепція національної безпеки України.

Закон України «Про основи національної безпеки України» визначає інформаційну безпеку важливою складовою національної безпеки. Значимість інформаційної безпеки пояснюється тим, що, по-перше, національні інтереси, загрози їм, управління цими ризиками реалізуються тільки через інформаційну сферу; по-друге, людина та її права, інформація та інформаційні системи та права на них – це основні об'єкти не тільки національної безпеки в інформаційній сфері, але й основні елементи всіх об'єктів безпеки в усіх галузях; по-третє, інформаційна складова є притаманною будь-якій сфері життєдіяльності суспільства. Об'єктами інформаційної безпеки є людина, суспільство та держава, забезпечення їхніх інтересів є завданням інформаційної безпеки.

Варто зазначити, що механізми управління інформаційною безпекою суттєво відстають у розвитку від сучасного рівня інформатизації, що сприяє зростанню рівня кіберзлочинності, яка у свою чергу спричиняє важкі, а іноді й незворотні наслідки для держави, підприємства, суспільства, особи. У глобальному плані спостерігається широкий діапазон кіберзлочинів, які включають злочини, що здійснюються в цілях отримання фінансової вигоди, злочини, пов'язані з використанням інформації, яка міститься в комп'ютерах,планшетах, мобільних телефонах, а також злочини, спрямовані проти конфіденційності, цілісності та доступності комп'ютерних систем [2, с.8].

Закон України «Про основи національної безпеки» стосовно загроз національній безпеці зазначає: на сучасному етапі найбільш важливими

потенційними та реальними ризиками стабільності в суспільстві та національній безпеці України в інформаційній сфері є:

1) розголошення конфіденційної інформації, що є власністю держави та спрямована на забезпечення національних інтересів та потреб держави та суспільства;

2) прояви обмеження доступу громадян до інформації та свободи слова;

3) поширення через засоби масової інформації культу та ідеології насильства, жорстокості тощо;

4) комп'ютерна злочинність та комп'ютерний тероризм;

5) розголошення інформації, що становить як державну, так і іншу таємницю, що передбачена Законом;

6) намагання маніпулювання суспільною свідомістю, зокрема, шляхом поширення упередженої, неповної чи недостовірної інформації [3].

Інформаційна безпека останнім часом займає одне з провідних позицій в системі національної безпеки. У сучасному світі будь-яка держава може розраховувати на свою перевагу над іншими державами у військово-технічній, економічній сферах, володіти стратегічною і тактичною перевагою, успішно прогнозувати розвиток нових технологій, військової техніки і сучасного озброєння, лише за умови лідерства у володінні розвиненими засобами інформації, організації ефективної системи інформаційної боротьби, в тому числі і в успішному протистоянню інформаційній війні.

Інформація є основною зброєю у протидії провідних світових держав у боротьбі за світове панування на глобальному інформаційному просторі.

Від інтенсивності, повноти, якості та своєчасності інформаційного обміну залежить рівень розвитку таких галузей, як оборонна промисловість, енергетика, зв'язок, наука і медицина, транспорт і виробництво в цілому.

Поява та активізація ризиків інформаційної сфери, насамперед від ведення інформаційних війн, суттєво підвищують роль та значення інформаційної безпеки в системі національної безпеки України та обумовлює розширення її

змісту. Втрата контролю над національними інформаційними комунікаціями в XXI столітті може призвести до втрати національної незалежності. Майбутні війни – війни без застосування безпосереднього насильства, засобами якого є не безпосередні дії, одним із методів яких є інформаційні війни [4, с.160].

Ризики пов'язані з загрозою інформаційної безпеки – це явище, дії негативних чинників або процеси, через які соціальні об'єкти інформаційної безпеки частково або цілком втрачають можливість реалізувати свої інтереси в інформаційній сфері; порушується нормальне функціонування, здійснюється руйнація або стримується розвиток технічних об'єктів інформаційної безпеки [5, с.16].

Отже, державна політика щодо забезпечення інформаційної безпеки є важливою складовою національної безпеки. В її основі повинна бути системна превентивна діяльність органів державного управління щодо надання гарантій інформаційної безпеки особистості, соціальним групам, суспільству і державі в цілому. Аналіз свідчить про існування реальних загроз інформаційній безпеці України [6, с.158]. Поряд з цим, проблема інформаційної безпеки держави є досить складною і багатогранною і тому її слід розглядати лише у взаємозв'язку з іншими проблемами, які мають більш високий або такий же порядок важливості. Перш за все, до таких проблем відноситься проблема національної безпеки.

Загальна система національної безпеки містить у собі кілька підсистем: державно-політичну, екологічну, економічну, соціальну та інформаційну. Підсистема інформаційної безпеки посідає особливе місце, тому що:

- По-перше, інформаційні відносини і процеси пронизують всі інші відносини і процеси, що мають місце в суспільстві, тому інформаційна безпека, як складова, входить в усі інші підсистеми національної безпеки;
- по-друге, в сучасних умовах, коли різноманітні інформаційні технології та процеси, засоби обчислювальної техніки інтенсивно і в масовому порядку

впроваджуються в багатьох галузях діяльності людини, питання інформаційної безпеки набувають самостійне суспільне значення;

- по-третє, система зовнішніх і внутрішніх ризиків інформаційної безпеки має комплексний характер.

До основних джерел зовнішніх ризиків можна віднести:

- введення іноземними державами обмежень Україні на поширення інформації і нових інформаційних технологій;
- розвідувальна діяльність іноземних державних органів і спеціальних служб;
- протиправна діяльність різних іноземних формувань і окремих особистостей в сфері інтересів України;
- стихійні катаклізми і катастрофи.

До основних джерел внутрішніх ризиків можна віднести:

- відсутність науково обґрунтованої політики інформаційної безпеки держави;
- недосконаліть законодавчої бази в галузі інформаційних відносин та інформаційної безпеки;
- недосконаліть державної структури забезпечення інформаційної безпеки;
- протиправні дії державних органів, політичних і економічних структур, окремих громадян в інформаційній сфері;
- виникнення позаштатних, непередбачених ситуацій в системах, процесах, які базуються на використанні інформаційних технологій, в результаті чого зростає ступінь ризику нанесення шкоди, а також його розмір;
- недосконаліть або відсутність засобів забезпечення інформаційної безпеки.

Реалізація наведених ризиків може завдати конкретну реальну шкоду як державі, так і окремій особистості. У загальнодержавній сфері Україна може придбати такі негативні тенденції, як: втрата пріоритету при вирішенні

міжнародних проблем, зниження темпів формування рівноправних і взаємовигідних відносин з іноземними державами, поглиблення економічної кризи, зниження військового і науково-технічного потенціалу, розвиток внутрішньополітичної дестабілізації тощо.

Без сумніву, шкода, що завдана державі внаслідок реалізації ризиків, так чи інакше проектується на всіх або багатьох суб'єктах суспільства. Але існує ряд загроз, реалізація яких може завдати шкоди конкретному громадянинові - матеріальний, моральний, або навіть фізичний.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

1. У сучасних умовах інформаційна складова національної безпеки держави відіграє надзвичайно важливу роль через наявні в ній ризики та загрози, до яких доцільно відносити кібертероризм, кіберзлочинність, агресивну пропаганду, поширення антиконституційних та антидержавних гасел, обмеження доступу населення до публічної інформації тощо .

2. Суспільні інститути є повноцінними учасниками процесу забезпечення інформаційної безпеки держави. Як показує суспільно-політична практика, зусиль державних, як правило, не вистачає для ефективної протидії інформаційним загрозам, обумовлює потребу побудови діалогу з соціумом.

3. Базовими елементами механізму взаємодії між владою і суспільством у даній сфері є інституційна, нормативно-правова та практична складові. Від повноцінного використання всіх можливостей і ресурсів, наявних у суспільстві залежить ефективність функціонування всієї системи інформаційної безпеки держави.

4. Політика інформаційної безпеки повинна бути орієнтована на забезпечення гарантій інформаційного суверенітету України та інформаційної безпеки всіх суб'єктів сфери інформатизації, бо інформаційне забезпечення національної безпеки являє собою процес задоволення інформаційних потреб суб'єктів національної безпеки.

5. Характер інформаційних потреб суб'єктів національної безпеки визначає зміст інформаційного забезпечення національної безпеки.

Інформаційне забезпечення національної безпеки виконує важливу багатопланову роль у визначенні національних інтересів і пріоритетів національної безпеки. Для забезпечення інформаційної безпеки держави необхідно всебічне задоволення потреб громадян, підприємств, установ і організацій всіх форм власності в доступі до достовірної та об'єктивної інформації; збереження і примноження духовних, культурних і моральних цінностей Українського народу; розвиток медіа-культури суспільства і соціально відповідальної медіа-середовища; формування ефективної правової системи захисту особистості, суспільства і держави від деструктивних пропагандистських впливів; створення на базі норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, перш за все, пропаганди; розвиток інформаційного суспільства.

Список використаних джерел

1. Сащук Г. Інформаційна безпека в системі забезпечення національної безпекиURL: http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php.

2. Державна служба фінансового моніторингу України. *Кіберзлочинність та відмивання коштів* URL: http://www.sdfm.gov.ua/content/file/Site_docs/2013/20131230/tipolog2013.pdf

3. Про основи національної безпеки України: Закон України. *Офіційний Вісник України.* 2003. № 29. Ст. 1433.

4. Ліпкан В. А. Теоретичні основи та елементи національної безпеки України. К.: Текст, 2003. 600 с.

5. Гуцалюк М. В. Організація захисту інформації : [навч. посібн.]. К. : Альтерпрес, 2012. 224 с.

6. Данільян О. Г., Дзьобань О. П., Панов М. І. Національна безпека України: структура та напрямки реалізації: навч. посіб. Х. : Фоліо, 2002. 285 с.

Panchenko Oleksandr. The Information Component of the National Security

The article is devoted to information security as a component of national security. The definition of the concept of information security and national security is presented. The issues of information security in the development of the information society and computerization are considered. The influence of security on the national security of the state is analyzed.

The information security of the state's society is determined by the degree of their security and the stability of the main spheres of life in relation to dangerous, destabilizing, destructive, affecting the interests of the country information impacts at the level of both introduction and extraction of information.
The role of information and information technology in the modern world is extremely large. Along with the rapid development of the sphere of information technology, new and emerging information risks of the national security of the state in front of society as a whole and each individual citizen are improved.
The information component of the national security of the state plays an extremely important role because of the risks and threats in it that are appropriate to include cyberterrorism, cybercrime, aggressive propaganda, dissemination of anti-constitutional and anti-state slogans, limitation of public access to public information, etc.
Public institutions are full participants in the process of ensuring information security of the state. As the socio-political practice shows, the efforts of the state, as a rule, are not sufficient for effective counteraction to information threats, necessitates the need for dialogue with the society.
Institutional, regulatory and practical components are the basic elements of the mechanism of interaction between government and society in this field. The effective functioning of the entire information security system of the state depends on the full utilization of all opportunities and resources available in the society.
Information security policy should be focused on providing guarantees of information sovereignty of Ukraine and information security of all subjects of information sphere, since information security of national security is a process of meeting the information needs of national security subjects. The nature of the information needs of national security entities determines the content of the national security information support.
National security information plays an important multifaceted role in defining national interests and national security priorities. To ensure the information security of the state it is necessary to fully meet the needs of citizens, enterprises, institutions and organizations of all forms of ownership in access to reliable and objective information; preserving and enhancing the spiritual, cultural and moral values of the Ukrainian people; development of media culture of society and socially responsible media environment; formation of an effective legal system to protect the individual, society and the state from destructive propaganda influences; creation, on the basis of the norms of international law, of a system and mechanisms of protection against negative external information and psychological influences, above all, propaganda; development of the information society.
Key words: information security, national security, information, information space, information security risks, information technology, information war.

References

1. Sashuk G.(2013). *Informatsiyna bezpeka v systemi zabezpechennya natsionalnoyi bezpeky* [Information security in the national security system]. Retrieved from http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php [in Ukrainian].

2. *Derzhavna sluzhba finansovoho monitorynhu Ukrayiny. Kiberzlochynnist ta vidmyvannya koshtiv* [State Financial Monitoring Service of Ukraine. Cybercrime and money laundering] Retrieved from http://www.sdfm.gov.ua/content/file/Site_docs/2013/20131230/tipolog2013.pdf [in Ukrainian].

3. *Pro osnovy natsionalnoyi bezpeky Ukrayiny: Zakon Ukrayiny* [On the basics of national security of Ukraine: Law of Ukraine]. (2003). *OfitsiynyyVisnykUkrayiny – Official Bulletin of Ukraine*, 29 [in Ukrainian].

4. Lipkan, V.A. (2003). *Teoretychni osnovy ta element natsionalnoyi bezpeky Ukrayiny* [Theoretical bases and elements of national security of Ukraine]. Kyiv: Tekst [in Ukrainian].

5. Gutsalyuk, M.V. (2012). *Orhanizatsiya zakhystu informatsiyi* [Organization of information security]. Kyiv: Alterpres [in Ukrainian].

6. Danilyan, O. G., Djoban, O.P., Panov, M.I. (2002). *Natsional'na bezpeka Ukrayiny: struktura ta napryamky realizatsiyi* [National security of Ukraine: structure and directions of implementation]. Kharkiv: Folio [in Ukrainian].