PUBLIC ADMINISTRATION

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЗАБЕЗПЕЧЕННІ ДЕРЖАВНОЇ БЕЗПЕКИ

Панченко Олег Анатолійович,
доктор медичних наук, професор, Заслужений лікар України, директор, ДЗ «Науково-практичний медичний реабілітаційно-діагностичний центр МОЗ України», президент Всеукраїнської професійної психіатричної ліги, м. Київ, Україна,
ORCID ID: https://orcid.org/0000-0001-9673-6685

DOI: https://doi.org/10.31435/rsglobal_sr/30062020/7141

ARTICLE INFO

Received 24 April 2020
Accepted 10 June 2020
Published 30 June 2020

KEYWORDS

information technologies,
national security,
information security,
information space,
information,
information society,
information supply.

ABSTRACT

The items of information technologies and their role in the protection and maintenance of national security, as well as key problems related to strengthening their influence in the world are considered in this article. The modern world is a complex system, a space of global information technologies. Modern information is the main determinant of society, and the rapid development of information technologies, which penetrate into all spheres of our lives, opens up completely new opportunities for social progress, as well as certain problems and challenges.

Information technologies, which are used in almost all spheres of human life and society, have become an attribute of modernity and directly influence national security and mechanisms for its provision.

The introduction of information technology in all spheres of human life due to the vulnerability and imperfection of computer programs and information technology, as well as their availability, creates serious risks and threats, both for ordinary citizens and for entire states.

The role of information and information technology in the modern world is extremely great. Together with the rapid development of information technology, new and already known information risks to the national security of the state to society as a whole and to each individual citizen are emerging.

On the basis of the national interests of Ukraine in the information sphere, strategic and current tasks of domestic and foreign policy of public administration dealing with the ensuring of information security as a component of the state security sector are formed.

Citation: Panchenko O. A. (2020) Information Technologies in Ensuring of the State Security. *Science Review*. 5(32). doi: 10.31435/rsglobal_sr/30062020/7141

Постановка проблеми. В умовах інформатизації суспільства проблема забезпечення державної безпеки не тільки зберігається, але й набуває ряд нових особливостей, пов'язаних зі зростанням ролі інформації в суспільстві. Інформаційні технології можуть, як забезпечувати стабільність і безпеку, так і загрожувати цим двом компонентам. З одного боку, інформаційні технології можна використовувати для поширення та обміну ідеями та стратегіями в області безпеки, для організації допомоги в миротворчих місіях, а також для здійснення і координації планів та операцій щодо забезпечення безпеки. Вони є важливою складовою всіх державних операцій по забезпеченню безпеки, від збору розвідувальної інформації до командування і контролю. Однак, з іншого боку, інформаційні технології можуть бути використані таким чином, щоб загрожувати стабільності і безпеки держави. Противник може знищити комунікаційні системи

за допомогою фізичної зброї (бомби, ракети) і електромагнітної зброї; використовувати засоби масової інформації (ЗМІ) для поширення брехні по всьому світу; а також проникнути або атакувати комп'ютерні мережі з метою отримання секретної інформації або пошкодження даних і систем.

Аналіз останніх досліджень і публікацій. Питання пов'язані з інформаційною безпекою, проблемами інформаційного суспільства та інформаційних війн досліджували такі науковці, як В.Б. Бритков, С.В. Дубовський [1], В.В. Гафнер [2], М.В. Гуцалюк [3], О.В. Казарін, В.Ю. Скиба, Р.А. Шаряпов [4], С.І. Кузіна, Д.О. Мякінченко [5], В.Ф. Шаньгін [6] та інші. 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 дослідження. Визначити принципи забезпечення державної безпеки з застосуванням інформаційних технологій.

Зв'язок публікації з плановими науково-дослідними роботами. Стаття написана в рамках НДР «Розробка системи реабілітації медико-психологічного спрямування особам в умовах інформаційно-психологічної війни» (термін виконання 2020-2022 рр., номер держреєстрації - 0120U101304).

Виклад основного матеріалу.

На сьогодні основним змістом розвитку людства вважається перехід від індустріального суспільства до постіндустріальної стадії розвитку в формі інформаційного суспільства.

В інформаційному суспільстві виробництво і споживання інформації є найважливішим видом діяльності, а інформація визнається найбільш значущим ресурсом, нові інформаційні та телекомунікаційні технології стають базовими технологіями, а інформаційне середовище поряд із соціальною та екологічною – новим середовищем проживання людини.

Інформаційне суспільство формується в процесі інформатизації, що має на увазі процес впровадження інформаційних технологій в усі сфери людської діяльності. Інформаційні технології використовуються сьогодні практично у всіх сферах життєдіяльності людини і суспільства і безпосередньо впливають на національну безпеку, пов'язану з захистом життєво важливих інтересів особистості, суспільства і держави від внутрішніх і зовнішніх загроз, а також механізми її забезпечення[7].

Глобальне використання інформаційних технологій, з одного боку, призводить до залежності національної безпеки держави від захищеності інформаційної інфраструктури. З іншого боку, рівень розвитку інформаційної інфраструктури повинен забезпечувати ефективність проведення державної політики (забезпечення органів державної влади повною і достовірною інформацією, забезпечення сучасних інформаційних відносин в сфері бізнесу; реалізація ефективного механізму включення інформаційного ресурсу в господарський оборот; забезпечення прав громадян на інформацію та ін.).

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.

Національна інформаційна безпека є комплексним поняттям, яке по-різному розкривається в різних публічних документах, навчальних посібниках, статтях. Вона не обмежується тільки інформаційною безпекою держави, його органів, сфер оборони та внутрішньої політики.

Доктрина інформаційної безпеки розглядає в якості об'єкта захисту збалансовані інтереси особистості, суспільства і держави. Без охорони інформаційних інтересів особистості і громадянина неможливо сприйняття держави як суб'єкта суспільного договору і носія суверенітету, без якого неможливий захист громадян. Також всередині поняття знаходиться і захист інформаційної інфраструктури, який здійснюється програмними, фізичними і технічними засобами, забезпечення безпеки наукових розробок і ноу-хау.

Під національною безпекою в цифровому просторі, що включає забезпечення інформаційної безпеки особистості, суспільства, держави та інфраструктури, розуміється стан захищеності інформаційного середовища, що гарантує, в першу чергу дотримання прав і законних інтересів особистості в інформаційній сфері, коли повністю забезпечуються їх захист, реалізація та можливості розвитку незалежно від кількості та якості внутрішніх і зовнішніх загроз.

Законодавство України щодо національної безпеки визначає інформаційну безпеку важливою складовою національної безпеки. Значимість інформаційної безпеки пояснюється тим, що, по-перше, національні інтереси, ризики, 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.

Важливим кроком у захисті національних інтересів України в інформаційній сфері стало затвердження Указом Президента України від 25 лютого 2017 р. № 47/2017 Доктрини інформаційної безпеки України (Доктрина–2017) [8]. У Доктрині–2017 визначено її мету та принципи, національні інтереси та актуальні загрози національним інтересам і національній безпеці України та пріоритети державної політики в інформаційній сфері, а також механізм реалізації Доктрини. Як особливий інструментарій досягнення мети Доктрина–2017 визначає систему комунікацій – стратегічних, урядових та кризових – як спеціалізованих (різнорівневих, різнопредметних та різносуб'єктних) комплексів заходів з реалізації державної політики в забезпеченні інформаційної безпеки України.

Значення Доктрини–2017 як у площині протидії загрозам інформаційній та національній безпеці України, осучаснення векторності діяльності держави у захисті інформаційного простору країни від зовнішньої інформаційної агресії, так і з точки зору вдосконалення нормативно-правового регулювання інформаційної сфери є безперечним.

В основі національної інформаційної безпеки знаходяться технічні, програмні та наукові ресурси, які, з одного боку, самі є об'єктом захисту, з іншого боку, забезпечують безпеку. Збільшення потужності цього ресурсу стає одним з основних завдань держави в цифрову еру.

За останні кілька десятиліть світ повністю змінився, і більшість комунікацій, фінансових трансакцій, інформаційних архівів потрапили в Інтернет. Це збільшило їх доступність для третіх осіб в порівнянні з епохою тільки матеріальних носіїв, і, відповідно, разом з доступністю підвищилася і вразливість.

Інтереси особистості і суспільства, що виражаються у збереженні інформації або в захисті від деструктивного інформаційного впливу, постійно піддаються загрозам, в основі яких полягає не тільки комерційний, а й психологічний або ідеологічний інтерес.

Інтереси держав в області інформаційної безпеки, в свою чергу, також знаходяться під ударом не тільки хакерських угруповань, а й окремих держав. У числі загроз прагнення окремих держав домінувати в міжнародному інформаційному полі. Це виражається не тільки в систематичному зниженні значення міжнародних організацій, в тому числі в невизнанні значимості прийнятих ними документів міжнародного права в галузі інформаційної безпеки, але і в конкретних діях.

Інформаційні технології сьогодні набули глобальний транскордонний характер, що створює неможливість як їх регулювання на національному рівні, так і безпомилкового виявлення джерел загроз [9].

Система інформаційних загроз істотно змінилася за останні роки. Крім хакерських угруповань і терористичних організацій, а також традиційно протиборчих іноземних розвідувальних організацій, генерувати загрози почали екстремістські організації і деструктивні секти, які часто направляються службами розвідки. Загрози посилилися, почастішали спроби перехоплення управління об'єктами критичної інфраструктури, посягання на державні інформаційні ресурси і мережі.

Забезпечення національної інформаційної безпеки покладається на наступні служби і організації: Рада національної безпеки і оборони України; органи внутрішньої безпеки; державні органи, які встановлюють стандарти в області захисту інформації, безпеки інформаційних потоків; наукові установи; інститути громадянського суспільства та інші.

Всі учасники процесів забезпечення інформаційної національної безпеки в цифровому світі повинні працювати у взаємодії, відчуваючи потреби один одного і зміну кон'юнктури.

Єдиний процес забезпечення інформаційної безпеки є безперервне і взаємопов'язане застосування превентивних, захисних і спрямованих на посилення позиції заходів наступного характеру: технічних; організаційних; аналітичних; пропагандистських; міжнародно-правових; кадрових; фінансово-економічних; розвідувальних.

Всі заходи повинні бути спрямовані на зниження рівня загроз, прогнозування нових ризиків, відбиття нападів, ліквідацію їх наслідків, нарощування технічного, ідеологічного та інформаційного потенціалу, забезпечення інформаційної безпеки держави, громадян і суспільства.

Інформаційні технології істотно впливають і на характер загроз національній безпеці. Останнім часом почав широко використовуватися термін кібертероризм, тобто терористичні дії в віртуальному просторі. Кібертероризм включає в себе операції, які компрометують, завдають шкоди і знищують інформацію, що зберігається в комп'ютерних мережах; комп'ютерні вторгнення і застосування мережевих «сніфферов» (Sniffers) для прослуховування телефонів; використання шкідливого програмного забезпечення, а саме комп'ютерних вірусів, хробаків і троянських коней. До них відносяться атаки типу «відмова в обслуговуванні» (DoS), які зупиняють або порушують роботу мережевих комп'ютерів, і «дефейс» (Deface), при якій сторінка веб-сайту замінюється на іншу (як правило, зухвалого виду: реклама, попередження, загроза і т.д.).

Зростаюча загроза кібератак може бути пов'язана з тенденціями і розвитком інформаційних технологій. Основними тенденціями є: поширеність, мобільність, інструменти взлому, вразливість і безпека.

Інформаційні технології стають все більш всеосяжними і взаємопов'язаними. Вони поширюються по всьому світу і інтегруються у все можливе: від приладів і транспортних засобів до процесів і інфраструктур. Автоматизація та підключення зростають стрімкими темпами, чому сприяють досягнення в області обчислювальної техніки і телекомунікаційних технологій. Дана тенденція посилює проблеми інформаційної безпеки. Збільшується число злочинців, цілей, а також можливостей використовувати, руйнувати і саботувати системи.

Інформація та інформаційні технології стають все більш мобільними. Люди і пристрої можуть перебувати де завгодно, програмне забезпечення та дані можуть зберігатися і передаватися в будь-якому місці і в будь-який час через електронну пошту, Інтернет і однорангові мережі.

Інструменти і методи, що використовуються для атаки на комп'ютерні мережі, стають все більш численними. Вони доступні на різних веб-сайтах. За деякими оцінками, в даний час існує більше 60 000 комп'ютерних вірусів.

Основна технологія завжди буде мати уразливості. Крім того, інсайдери, що мають доступ до інформації, будуть здійснювати навмисні дії шпигунства і саботажу. Таким чином, важливим компонентом будь-якої програми безпеки є здатність виявляти і реагувати на виникаючі проломи в безпеці.

Комплексний захист комп'ютерної мережі сучасного рівня вимагає використання різних засобів безпеки, таких як системи виявлення мережевих атак, системи захисту від спаму, антивіруси, брандмауери (firewall), сканери безпеки і т.д. Для виявлення загроз на практиці використовується великий асортимент спеціалізованих систем: аналізатори мережевих протоколів, системи моніторингу мережі, як активний компонент - системи тестування навантаження. Також широко використовуються антивіруси, міжмережеві екрани, криптографічні засоби захисту інформації, систем виявлення атак (IDS) та ін. Однак всі ці засоби захисту застосовуються періодично, виходячи з суб'єктивних рішень адміністраторів мережі, як інструмент для вирішення вже виниклої проблеми і лише зрідка – для профілактики. Методи аналізу спрямовані на виявлення заздалегідь відомих і описаних в літературі загроз, отже – далеко не завжди мають можливість виявити нові види загроз або модифікації вже відомих, що значно знижує безпеку мережі.

Для здійснення моніторингу потрібна наявність в комп'ютерній мережі єдиної системи управління всіма вузлами і сегментами мережі, яка буде служити базою для розгортання системи моніторингу, що дозволить здійснювати динамічний контроль стану всіх важливих вузлів і елементів мережі в реальному часі, а також накопичувати відповідну статистику для подальшого використання в прогнозуванні ситуацій порушення функціональності мережі.

У загальному вигляді система моніторингу повинна складатися з наступних компонентів:

- підсистема збору інформації, що надходить від усіх наявних засобів захисту;
- сервер подій, призначений для централізованої обробки інформації, що надходить про події, що мають відношення до безпеки мережі, відповідно до правил, заданих адміністратором мережі;
- сервер зберігання даних - як первинної інформації (подій), так і результатів аналізу;
- призначений для користувача інтерфейс управління системою моніторингу, що дозволяє здійснювати контроль і управління в реальному масштабі часу.

Технології забезпечення безпеки значно просунулися в таких областях, як криптографія, біометрія, виявлення вторгнень, антивірусний захист, сканування вразливостей та ін. Крім того, багато компаній сьогодні пропонують послуги з управління інформаційною безпекою, включаючи віддалений моніторинг вразливостей і вторгнень. Хоч ці досягнення, безсумнівно, допомогли запобігти численним атакам, в цілому вони не впоралися зі зростаючою загрозою як безпосередньо конкретної організації, так і національної безпеки держави.

Таким чином, 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.

Висновки та перспективи подальших досліджень.

1. Особливістю сучасного суспільства є зростання впливу інформації та інформаційних технологій на всі сфери життя, а також переміщення центру боротьби в інформаційну область. Інформація та інформаційні технології стають все більш поширеними, мобільними і вразливими.

2. Інформаційна безпека займає одну 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.

3. У сучасному інформаційному суспільстві, в умовах зростання загальних та інформаційних загроз, зростання комп'ютерної злочинності, повсюдного поширення штучного інтелекту, застосування інформаційних технологій у всіх сферах правоохоронної, економічної, регулятивної діяльності є необхідним, неминучим і найперспективнішим напрямом діяльності для забезпечення безпеки особистості, суспільства і держави.

Тому проблема забезпечення національної безпеки в умовах інформатизації суспільства стає ще більш актуальною.

REFERENCES

1. Britkov, V.B. and Dubovskoy, S.V. (2000). *Informatsionnyye tekhnologii v natsionalnom i mirovom razvitii* [Information Technologies in National and World Development], journal *Obshchestvennyye nauki i sovremennost* [Social Sciences and the Present], vol. 1, pp. 146-150 [Russia]
2. Gafner V.V. (2010). *Informatsionnaya bezopasnost* [Information Security], Tutorial, Press Phoenix, Rostov-on-Don, 324 p. [Russia]
3. Hutsalyuk M.V. (2012). *Orhanizatsiya zakhystu informatsiyi* [Organization of information protection], Tutorial, Press Alterpres, Kyiv, 224 p. [Ukraine]
4. Kazarin O.V., Skiba V.YU. and Sharyapov R.A. (2016). *Novyye raznovidnosti ugroz mezhdunarodnoy informatsionnoy bezopasnosti* [New varieties of threats to international information security], journal *Vestnik RGGU. Seriya* "*Dokumentovedeniye i arkhivovedeniye. Informatika. Zashchita informatsii i informatsionnaya bezopasnost*" [Bulletin of the Russian State Humanitarian University. Series "Documentation and Archival Studies. Computer science. Information Protection and Information Security"], vol.1(3), pp.54-72 [Russia]

5. Kuzina S.I. and Myakinchenko D.A. (2015). *Informatsionnoye nasiliye: aspekty natsional'noy bezopasnosti* [Information violence: aspects of national security], journal *Gosudarstvennoye i munitsipal'noye upravleniye. Uchenyye zapiski SKAGS.*[State and municipal government. Scholarly notes of SKAGS], vol. 3, pp.205-209 [Russia]
6. Shangin V.F. (2017). *Informatsionnaya bezopasnost i zashchita informatsii* [Information Security and Information Protection], Tutorial, Press DMK Press Moscow, 195 p. [Russia]
7. Panchenko O. A. and Banchuk N. V. (2011). *Informatsionnaya bezopasnost' lichnosti* [Information security of a person], Tutorial, Press KIT. Kyiv, 672 p. [Ukraine]
8. Administration of the President of Ukraine (2017), *Pro rishennya Rady natsionalnoyi bezpeky i oborony Ukrayiny vid 29 hrudnya 2016 roku "Pro Doktrynu informatsiynoyi bezpeky Ukrayiny"* [On the decision of the National Security and Defense Council of Ukraine of December 29, 2016 "On the Doctrine of Information Security of Ukraine"], Decree of the President of Ukraine dated February 25, 2017 № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (related to 17.06.2020) [Ukraine]
9. Panchenko O.A., Antonov V.G. and Humeniuk V.V. (2016), "Informatsionnaya bezopasnost lichnosti v usloviyakh izmenyayushchikhsya sotsiokulturnykh tsennostey" ["Information security of an individual in the context of changing sociocultural values"], journal Visnyk Odeskoho natsionalnoho universytetu. Psykholohiya [Bulletin of Odessa National University. Psychology], vol. 21, issue 2(40), pp. 140-148. DOI: https://doi.org/10.18524/2304-1609.2016.2 (40).134504. [Ukraine].