Електронне "**Державне управління: удосконалення та розвиток**"
включено до переліку наукових фахових видань України з питань державного управління
(Наказ Міністерства освіти і науки України від 22.12.2016 № 1604)
www.dy.nayka.com.ua | № 11 2019 р. | 28.11.2019

DOI: 10.32702/2307-2156-2019.11.40

УДК 351:342.57

В. О. Торічний,
кандидат психологічних наук,
старший викладач кафедри психології та морально-психологічного забезпечення,
факультет іноземних мов та гуманітарних дисциплін, Національна академія Державної прикордонної служби України імені Богдана Хмельницького
ORCID ID: 0000-0003-3336-6386

СТРАТЕГІЧНІ ОРІЄНТИРИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ УКРАЇНИ

V. Torichniy
PhD in Psychological Sciences,
Senior Lecturer of the Department of Psychology and Moral and Psychological Support,
Faculty of Foreign Languages and Humanities, National Academy of the State Border Guard Service of Ukraine Named after Bogdan Khmelnitskyi

THE STRATEGIC REFERENCE POINTS OF INFORMATION SUPPORT OF STATE SECURITY OF UKRAINE

У статті виокремлено стратегічні орієнтири інформаційного забезпечення державної безпеки України. Зокрема, проаналізовано сучасний стан інформаційної безпеки в Україні. Показано, що провідною є роль у формуванні національної стратегії інформаційного забезпечення державної безпеки у контексті консолідації всіх верств суспільства для досягнення поставлених цілей інформаційного й інноваційного розвитку, а також координації бізнесу, всіх суспільних інститутів та громадян щодо реалізації цієї Стратегії. Визначено ключові напрями побудови інформаційного суспільства в межах Стратегії інформаційного забезпечення державної безпеки: забезпечення ефективності системи державного управління; забезпечення доступності інформаційно-комунікаційної інфраструктури; створення інформаційного середовища для соціально-економічного і культурного розвитку суспільства; розвиток вітчизняного інформаційного простору. Визначено низку державних заходів мінімізації ризиків інформаційній безпеці: оцінка та вдосконалення засобів контролю за змінами в інформаційних системах; впровадження програми попередження витоку даних. Зазначено, що, спираючись на міжнародний досвід побудови інформаційного суспільства в межах Стратегії інформаційного забезпечення державної безпеки слід визначити чотири ключові напрями: забезпечення ефективності системи державного управління; забезпечення доступності інформаційно-комунікаційної інфраструктури; створення інформаційного середовища для соціально-економічного і культурного розвитку суспільства; розвиток вітчизняного інформаційного простору. Окреслено перспективи впровадження інформаційно-комунікаційних технологій з метою забезпечення державної безпеки: вдосконалення державного управління; створення відкритого і мобільного електронного уряду; розвитку доступності інформаційної інфраструктури.

The strategic reference points of information support of state security of Ukraine are allocated in the article. In particular, the current condition of information security in Ukraine is analyzed. It is shown that the role in formation of national strategy of information support of state security in the context of consolidation of all sectors of society for achievement of goals of information and innovative development and also coordination of business, all public institutes and citizens on realization of this strategy is a leading one. The following key directions of creation of information society within the strategy of information support of state security are defined: ensuring of system effectiveness of public administration; ensuring of availability of information and communication infrastructure; creation of the information environment for social and economic and cultural development of society; development of domestic information space. A number of the following state measures of minimization of risks of information security is defined: assessment and improvement of control devices behind changes in information systems; introduction of the program to prevention of data leakage. It is specified that, relying on the international experience of creation of information society within the strategy of information support of national security it is necessary to define the following key directions: ensuring system effectiveness of public administration; ensuring availability of information and communication infrastructure; creation of the information environment for social and economic and cultural development of society; development of domestic information space. The following prospects of introduction of information and communication technologies for the purpose of ensuring of state security are planned: improvement of public administration; creation of the opened and mobile electronic government; development of availability of information infrastructure.

Ключові слова: *інформаційне забезпечення державної безпеки; інформаційна безпека; інформаційно-комунікаційні технології; стратегічні орієнтири.*

Key words: *information support of state security; information security; information and communication technologies; strategic reference points.*

Постановка наукової проблеми. Сучасний розвиток людської цивілізації характеризується черговим етапом науково-технічної революції − впровадженням у всі сфери життя інформаційно-комунікаційних технологій, які змінюють спосіб життя людей і складають фундамент і матеріальну базу для переходу до інформаційного суспільства − суспільства з високим соціально-економічним, політичним і культурним розвитком. Вищенаведене обумовлює необхідність виокремлення стратегічних орієнтирів інформаційного забезпечення державної безпеки України.

Аналіз останніх досліджень і публікацій, в яких було започатковано розв'язання проблеми. Проблематику інформаційного забезпечення державної безпеки досліджувала велика кількість вітчизняних і зарубіжних учених, зокрема, таких, як: В. П. Горбулін, А. Б. Качинський [1], В. К. Конах [2] та ін.

Однак необхідно зазначити, що стратегічні пріоритети розвитку інформаційного забезпечення державної безпеки в межах державної інформаційної політики все ще потребують конкретизації.

Мета статті. Відповідно, метою даної роботи є виокремлення стратегічних орієнтирів інформаційного забезпечення державної безпеки України.

Необхідність досягнення поставленої мети передбачає постановку та вирішення таких відповідних завдань:

- проаналізувати сучасний стан інформаційної безпеки в Україні;
- визначити чотири ключові напрями побудови інформаційного суспільства в межах Стратегії інформаційного забезпечення державної безпеки слід;
- окреслити перспективи впровадження інформаційно-комунікаційних технологій з метою забезпечення державної безпеки.

Виклад основного матеріалу.

Перш ніж пропонувати інформаційного забезпечення державної безпеки України, доцільно проаналізувати сучасний стан інформаційної безпеки в Україні. Зокрема, доцільно провести опитування серед керівників потужних ІТ-компаній, що функціонують на території України.

У цьому зв'язку керівникам цих компаній було запропоновано відповісти на декілька питань. Перше з яких – «Які механізми повинні використовуватися в державі для підвищення ефективності управління процесами забезпечення інформаційної безпеки?». Результати відповіді на дане запитання наведено у табл. 1.

Таблиця 1.
Розподіл відповідей керівників ІТ-компаній України щодо механізмів підвищення ефективності управління процесами забезпечення інформаційної безпеки

Найменування механізму підвищення ефективності	Відсоток розподілу відповідей, %
Введення засобів безперервного моніторингу контролю доступу	27%
Аутсорсинг окремих заходів у сфері безпеки	4%
Стандартизація на базі єдиної системи контрольних процедур	9%
Уведення системи збалансованих показників	5%
Уведення засобів управління обліковими записами	10%
Впровадження додаткових засобів забезпечення безпеки	45%

З табл. 1 можна побачити, що пріоритетним механізмом підвищення ефективності управління процесами забезпечення інформаційної безпеки 27% респондентів уважають введення засобів безперервного моніторингу контролю доступу. На другому місці знаходиться введення засобів управління обліковими записами – 10%. Однак 45% опитаних пропонує введення альтернативних механізмів підвищення ефективності управління процесами забезпечення інформаційної безпеки в державі.

У табл. 2 наведено результати розподілу відповідей респондентів щодо засобів контролю за витоком конфіденційної інформації на державному та регіональному рівнях.

З табл. 2 можна побачити, що 21% респондентів уважають, що формулювання конкретних вимог до доступу до конфіденційної інформації є ключовим компонентом засобів контролю за витоком конфіденційної інформації на державному та регіональному рівнях.

На другому місці (17%) знаходяться:

- впровадження засобів моніторингу (фільтрації) контенту;
- розробка та впровадження спеціальної політики по відношенню до класифікації конфіденційної інформації.

Таблиця 2.
Розподіл відповідей керівників ІТ-компаній України щодо розподілу відповідей респондентів відносно засобів контролю за витоком конфіденційної інформації на державному та регіональному рівнях

Найменування засобу контролю витоку інформації	Відсоток розподілу відповідей, %
Впровадження засобів моніторингу (фільтрації) контенту	17%
Використання засобів аудиту	6%
Впровадження засобів аналізу журналу подій	5%
Обмеження доступу до конфіденційної інформації визначеними періодами часу	9%
Блокування (обмеження) використання визначених компонентів програмного забезпечення	11%
Заборона використання пристроїв зі вбудованою камерою в зонах обмеженого доступу	3%
Розробка та впровадження спеціальної політики по відношенню до класифікації конфіденційної інформації	17%
Впровадження додаткових механізмів безпеки з метою захисту інформації	
Обмеження (заборона) застосування систем миттєвого обміну повідомленнями при передачі конфіденційної інформації	11%
Формулювання конкретних вимог до доступу до конфіденційної інформації	21%

Третє місце (11%) посідають:

- блокування (обмеження) використання визначених компонентів програмного забезпечення;
- обмеження (заборона) застосування систем миттєвого обміну повідомленнями при передачі конфіденційної інформації.

Третє питання, що підлягало дослідженню – «Які питання повинні розглядатися у державній програмі відносно підвищення обізнаності стосовно безпеки?». Відповідні результати опитування наведено у табл. 3.

Таблиця 3.
Розподіл відповідей керівників ІТ-компаній України щодо питань, які повинні розглядатися у державній програм відносно підвищення обізнаності стосовно безпеки

Зміст питання державної програми	Відсоток розподілу відповідей, %
Підвищення обізнаності з питань забезпечення інформаційної безпеки	33%
Перевірка, узгодження та дотримання діючих політик і стандартів у сфері безпеки	26%
Оцінка ефективності заходів з підвищення рівня обізнаності та вдосконалення існуючої програми на основі такої оцінки	18%
Регулярне сповіщення про загрози інформаційній безпеці	8%
Розповсюдження інформаційних повідомлень з нових актуальних тем	7%
Проведення спеціальних заходів і тренінгів у сфері безпеки	8%

З табл. 3 можна побачити, що підвищення обізнаності з питань забезпечення інформаційної безпеки (33%) знаходиться на першому місці у рейтингу опитаних щодо питань, які повинні розглядатися у державній програмі відносно підвищення обізнаності стосовно безпеки.

На другому місці знаходиться перевірка, узгодження та дотримання діючих політик і стандартів у сфері безпеки (26%). Третє місце посідає оцінка ефективності заходів з підвищення рівня обізнаності та вдосконалення існуючої програми на основі такої оцінки (18%).

Наприкінці доцільно проаналізувати відповіді респондентів щодо заходів, які в нинішніх умовах впроваджуються державою для мінімізації ризиків інформаційній безпеці (табл. 4).

Таблиця 4.
Розподіл відповідей керівників ІТ-компаній України щодо заходів, які в нинішніх умовах впроваджуються державою для мінімізації ризиків інформаційній безпеці

Зміст заходу	Відсоток розподілу відповідей, %
Оцінка та вдосконалення засобів контролю за змінами в інформаційних системах	38%
Оцінка та вдосконалення засобів управління доступом та обліковими записами	16%
Впровадження програми попередження витоку даних	33%
Розробка програми збереження знань	13%

З табл. 4 можна побачити, що переважна більшість респондентів орієнтована на такі державні заходи мінімізації ризиків інформаційній безпеці:

- оцінка та вдосконалення засобів контролю за змінами в інформаційних системах (38%);
- впровадження програми попередження витоку даних (33%).

Вищенаведений аналіз показує, що провідною є роль у формуванні національної стратегії інформаційного забезпечення державної безпеки у контексті консолідації всіх верств суспільства для досягнення поставлених цілей інформаційного й інноваційного розвитку, а також координації бізнесу, всіх суспільних інститутів та громадян щодо реалізації цієї Стратегії.

Спираючись на міжнародний досвід побудови інформаційного суспільства в межах Стратегії інформаційного забезпечення державної безпеки слід визначити чотири ключові напрями:

- забезпечення ефективності системи державного управління;
- забезпечення доступності інформаційно-комунікаційної інфраструктури;
- створення інформаційного середовища для соціально-економічного і культурного розвитку суспільства;
- розвиток вітчизняного інформаційного простору [1; 3].

У рамках даних напрямів за допомогою повсюдного впровадження інформаційно-комунікаційних технологій будуть вирішені завдання:

- вдосконалення державного управління;
- створення відкритого і мобільного електронного уряду;
- розвитку доступності інформаційної інфраструктури [1; 2].

Висновки. Таким чином, у результаті проведення даного дослідження було отримано такі висновки.

1. Проаналізовано сучасний стан інформаційної безпеки в Україні. Показано, що провідною є роль у формуванні національної стратегії інформаційного забезпечення державної безпеки у контексті консолідації всіх верств суспільства для досягнення поставлених цілей інформаційного й інноваційного розвитку, а також координації бізнесу, всіх суспільних інститутів та громадян щодо реалізації цієї Стратегії.

2. Визначено ключові напрями побудови інформаційного суспільства в межах Стратегії інформаційного забезпечення державної безпеки: забезпечення ефективності системи державного управління; забезпечення доступності інформаційно-комунікаційної інфраструктури; створення інформаційного

середовища для соціально-економічного і культурного розвитку суспільства; розвиток вітчизняного інформаційного простору.

3. Окреслено перспективи впровадження інформаційно-комунікаційних технологій з метою забезпечення державної безпеки: вдосконалення державного управління; створення відкритого і мобільного електронного уряду; розвитку доступності інформаційної інфраструктури.

Список використаних джерел.

1. Горбулін В. П., Качинський А. Б. Стратегічне планування : вирішення проблем національної безпеки. Київ : НІСД. 2010. 288 с.

2. Конах В. К. Нормативно-правові засади державної політики України у сфері інформаційно-психологічної безпеки. Стратегічні приоритети. 2012. № 3 (24). С. 152−157.

3. Курас І. Інтеграція інформаційних ресурсів – стратегічний напрям забезпечення інформаційних потреб суспільства. Бібліотечний вісник. 2009. №1. С. 2−6.

References.

1. Gorbulin, V. P. & Kachynskyj, A. B. (2010). *Strategichne planuvannya : vyrishennya problem nacionalnoyi bezpeky* [Strategic Planning : Decision of Problems of National Security]. NISD, Kyiv, Ukraine, P. 288.

2. Konakh, V. K. (2012). "The Standard and Legal Bases of State Policy of Ukraine in the Sphere of Information and Psychological Security", *Strategichni pryorytety*, vol. 3 (24), pp. 152−157.

3. Kuras, I. (2009). Integration of Information Resources − the Strategic Direction of Ensuring of Information Requirements of Society", *Bibliotechnyj visnyk*, vol. 1, pp. 2−6.

Стаття надійшла до редакції 20.11.2019 р.