УДК 338.1:355.3

DOI: <https://doi.org/10.32840/2522-4263/2020-6-7>**Поліщук А.С.***викладач кафедри оборонного менеджменту
Навчально-наукового центру оборонного менеджменту
Національного університету оборони України***Ткаченко О.В.***магістрант
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»***Polishchuk Anatoliy***Lecturer at the Department of Defense Management
Training and Research Center of Defense Management
National Defense University of Ukraine***Tkachenko Oleksandr***Master
National Technical University of Ukraine
“Igor Sikorsky Kyiv Polytechnic Institute”*

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВ ЯК СКЛАДОВА ЧАСТИНА НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

INFORMATION SECURITY OF ENTERPRISES AS A COMPONENT OF THE NATIONAL SECURITY OF THE STATE

АНОТАЦІЯ

У статті проаналізовано інформаційну безпеку підприємств як складову частину національної безпеки держави. Державна інформаційна політика України є складовою частиною соціально-економічної політики. Вона ґрунтується на національних доктринах, стратегіях, концепціях згідно з чинним законодавством. Інформаційна безпека є однією із суттєвих складових частин національної безпеки країни. Доведено, що відставання в галузі інформаційних технологій оборонно-промислового комплексу у сфері цифрової економіки несе стратегічно значущу загрозу втрати технологічного, економічного суверенітету. Нейтралізація цієї загрози значною мірою пов'язана з подоланням критичної залежності підприємств оборонного комплексу від імпортованих поставок електронної компонентної бази, програмно-апаратних засобів обчислювальної техніки, побудовою та розвитком єдиного цифрового простору підприємств. Стабільність і безпека функціонування таких систем є важливими для нормального функціонування держави.

Ключові слова: інформація, безпека, національна безпека, цифрова економіка, автоматизовані системи управління.

АННОТАЦИЯ

В статье проанализирована информационная безопасность предприятий как составляющая национальной безопасности государства. Государственная информационная политика Украины является составляющей социально-экономической политики. Она основывается на национальных доктринах, стратегиях, концепциях в соответствии с действующим законодательством. Информационная безопасность является одной из существенных частей национальной безопасности страны. Доказано, что отставание в области информационных технологий предприятий оборонно-промышленного комплекса в сфере цифровой экономики несет стратегическую угрозу потери технологического, экономического суверенитета. Нейтрализация этой угрозы в значительной степени связана с преодолением критической зависимости предприятий оборонного комплекса от импортных поставок электронной компонентной базы, программно-аппаратных средств вычислительной техники, построением и развитием единого цифрового пространства предприятий. Стабильность и безопасность функциони-

рования таких систем являются важными для нормального функционирования государства.

Ключевые слова: информация, безопасность, национальная безопасность, цифровая экономика, автоматизированные системы управления.

ANNOTATION

An important part of national security is economic information security. The article analyzes the information security of enterprises as a component of national security. State information policy of Ukraine is a component of socio-economic policy. It is based on national doctrines, strategies, concepts in accordance with current legislation. Information security is one of the essential components of a country's national security. It is proved that the lag in the field of information technologies of the defense-industrial complex in the digital economy carries a strategically significant threat of loss of technological and economic sovereignty. Neutralization of this threat is largely related to overcoming the dependence of defense companies on imported supplies of electronic components of the database, computer software and hardware, construction and development of a single digital space of enterprises. The study developed ideas about the relationship between information and national security of the state. When developing the information environment of the functioning of objects (subjects) of management, it is necessary to take into account the system of criteria for ensuring the effective integration of Ukraine into the world space: availability of information; cost minimization; relevance, completeness and analytical information. Consideration of economic, legal, psychological and technical methods of information protection and their use in enterprises will develop an improved structure of information protection methods in enterprises through a combination of passive-preventive, active-preventive and reactive approaches and identify shortcomings of information protection. The need to regulate the exchange of information between the subjects of the information space has been established. Proved the need to create a body within the executive branch, which will formulate policy on public information resources and take care of information and telecommunications, government intervention requires the problem of lack of access to public information on the Internet.

Key words: information, security, national security, digital economy, automated control systems.

Постановка проблеми. Четверта промислова революція, відома як «Індустрія 4.0», сприяє розвитку нових форм і способів досягнення країнами політичних, соціально-економічних, екологічних та інших цілей на інформаційному рівні. Захищаючи свої національні інтереси, держава має дбати про свою інформаційну безпеку, яка є основою зміцнення української державності. Державна інформаційна політика України є складовою частиною соціально-економічної політики. Вона ґрунтується на національних доктринах, стратегіях, концепціях згідно з чинним законодавством. Інформаційна безпека є однією із суттєвих складових частин національної безпеки країни.

Аналіз останніх досліджень і публікацій. Проблемам інформаційної безпеки, захисту інформаційного простору присвячені наукові праці А. Марущака, В. Петрика, В. Ліпкана, Б. Кормича, В. Почепцова, І. Седікової та інших учених.

Виділення не вирішених раніше частин загальної проблеми. Однак у працях вищезазначених фахівців інформаційна безпека досліджувалась, скоріше, як складова частина національної безпеки, її невід'ємний компонент. Поза увагою науковців залишились проблеми чіткого окреслення інформаційних загроз, вивчення їхніх джерел.

Формулювання цілей статті (постановка завдання). Метою статті є дослідження проблеми інформаційної безпеки підприємств оборонного комплексу та методів захисту від несанкціонованого доступу.

Виклад основного матеріалу дослідження. У Законі України «Про основи національної безпеки України» визначено, що «національна безпека – захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам» [1].

В сучасних умовах національна безпека залежить не тільки від збройних сил, але й від низки таких факторів, як економіка, конкурентоспроможність, добробут громадян. Серед джерел реальної загрози для багатьох країн можна назвати тероризм, поширення зброї масового знищення, спад економічного зростання, забруднення довкілля, чисельність населення, енергоресурси. Важливою складовою частиною національної безпеки є економічна інформаційна безпека. Інформаційна безпека, з одного боку, передбачає забезпечення якісного всебічного інформування громадян та вільного доступу до різних джерел інформації, а з іншого боку, є контролем за поширенням дезінформації, сприянням цілісності суспільства, збереженням інформаційного суверенітету, протидією негативним інформаційно-психологічним пропагандистським впливам та захистом національного інформаційного простору від маніпуляцій, інформаційних війн

та операцій [2]. Існує два аспекти трактування інформаційної безпеки у контексті національної безпеки. З одного боку, інформаційну безпеку розглянуто як самостійний елемент національної безпеки будь-якої країни, а з іншого боку, вона є інтегрованою складовою частиною будь-якої іншої безпеки, зокрема військової, економічної, політичної.

У 2017 р. цифрова революція увійшла у вирішальну фазу: до Інтернету підключився кожен другий житель Землі. За оцінкою Глобального інституту McKinsey (MGI), у найближчі 20 років до 50% робочих операцій у світі можуть бути автоматизовані. Дослідження свідчать про те, що в Китаї до 22% збільшення ВВП до 2025 р. можуть відбутися за рахунок інтернет-технологій. У США очікуваний приріст вартості, що створюється цифровими технологіями, до 2025 р. може скласти 1,6–2,2 трлн. дол. США. Такі економічні прогнози пов'язані не тільки з ефектом від автоматизації наявних процесів, але й з упровадженням принципово нових, проливних бізнес-моделей і технологій. Серед них слід назвати цифрові платформи, цифрові екосистеми, поглиблену аналітику великих масивів даних, технології «Індустрії 4.0» (3D-друк, роботизація, Інтернет речей) [3; 4].

Відставання в галузі інформаційних технологій оборонно-промислового комплексу (ОПК) у сфері цифрової економіки несе стратегічно значущу загрозу втрати технологічного, економічного суверенітету та закріплення за Україною довгострокового статусу «технологічної периферії» [5].

Нейтралізація цієї загрози національній безпеці значною мірою пов'язана з подоланням критичної залежності ОПК від імпорتنих поставок електронною компонентою бази (ЕКБ), програмно-апаратних засобів обчислювальної техніки, побудовою та розвитком єдиного цифрового простору підприємств ОПК, поетапним переведенням (функціонуючих та проєктованих) систем інформаційної інфраструктури на типові вітчизняне програмно-апаратне середовище. Стабільність і безпека функціонування таких систем є важливими для нормального функціонування держави [6]. Слід констатувати, що основним напрямом розвитку автоматизованих систем управління (АСУ) підприємств ОПК на найближчу та середньострокову перспективу можна вважати досягнення технологічної незалежності галузі, яка дасть їй змогу динамічно розвиватися в умовах дестабілізуючих зовнішньополітичних тенденцій, бути стійкою до негативних змін світової політичної та економічної ситуації [7].

Досі більшість фахівців підприємств, організацій ОПК та компаній-розробників поділяє думку про те, що щодо досягнення технологічної незалежності галузі інформаційних технологій ОПК намітилися позитивні тенденції: процес заміщення імпорту запущений, проте поки що частка українських продуктів не дуже велика, а саме 10%. Проблема, на наш погляд,

вирішується повільно, що змушує сумніватися в ефективності наявного розподілу обмежених фінансово-матеріальних ресурсів між галузевими програмами заміщення імпорту. Масштаб впливу інформаційної сфери перевершує галузеві ефекти, а індекс конкурентоспроможності економіки держав пов'язаний з показником розвитку ІКТ.

Програмно-апаратне середовище АСУ підприємств ОПК включає взаємопов'язані апаратну платформу, операційне середовище, пакети прикладних програм та засоби захисту інформації. Апаратна платформа – це ключова й слаборозвинена ланка в цій проблемі. Причина цього полягає у відсутності високотехнологічної вітчизняної ЕКБ, промислового виробництва виробів електроніки і, як наслідок, виробництва якісного системного програмного забезпечення (ПЗ) [7].

Надалі існує проблема невизначеності національної стратегії заміщення імпорту. Невирішеність проблеми викликає істотну невизначеність під час формулювання цілей та постановки завдань заміщення імпорту як в ОПК, так і в соціально-економічних галузях. Високий пріоритет науково-технологічного напрямку розвитку ІКТ та електроніки, заміщення імпорту треба розглядати як особливий тип державної та економічної стратегії, інструмент досягнення головної мети, якою є забезпечення достатнього рівня технологічної незалежності України від зарубіжних країн у найважливіших соціально-економічних галузях та ОПК з пріоритетом системоутворюючого науково-технологічного напрямку розвитку передових ІКТ та електроніки [6].

Невирішеною є проблема недостатності нормативно-правової бази. Проведений аналіз законодавчих і нормативно-правових актів державного регулювання інформаційних процесів свідчить про його недосконалість. Встановлено, що не врегульовано на законодавчому рівні право на інформацію, охорону персональних даних, немає документів, які регламентують порядок формування й підтримки відомчих інформаційних ресурсів, доступ до них, не встановлено правила придбання та експлуатації інформаційних телекомунікаційних технологій, що приводить до безконтрольної витрати значних коштів, до того, що інформаційні системи не дають очікуваної віддачі у підвищенні ефективності діяльності суб'єктів господарювання. Визначено, що наявні документи, які регламентують цю діяльність, мають характер технічного завдання, вирішують питання організації, фінансування та безпеки. Проте відсутні правові акти, які зобов'язують міністерства та відомства оприлюднювати визначений набір інформації у відкритому доступі в Інтернеті. У рамках загальної стратегії переходу до інформаційного суспільства пропонується приділити більше уваги побудові державної політики щодо розвитку української частини Інтернету.

Можливість доступу до інформації, як правило, обмежується її відомчою належністю та обумовлена найчастіше посадовим становищем і соціальним статусом споживача. Не вирішена проблема доступу та отримання інформації від низки територіально віддалених інформаційних ресурсів. Ці проблеми можна вирішити шляхом формування єдиного інформаційного простору України.

Для вирішення проблем створення єдиної інформаційної системи запропоновано розробити законодавчі й нормативні акти, що визначають права та обов'язки юридичних і фізичних осіб щодо формування та використання інформаційних ресурсів, засобів їх оброблення й доставки; економічні регулятори, які забезпечать стимулювання активного формування й використання інформаційних ресурсів. Функціонування інформаційного простору України на законодавчій основі забезпечує оперативний доступ органів державної влади, суб'єктів підприємницької діяльності до наявних інформаційних ресурсів з постійним поповненням єдиної інформаційної системи новими інформаційними ресурсами [8].

Концептуальна нормативно-правова база повинна містити поняття, визначення, показники та методики оцінювання результатів заміщення імпорту у сфері ІКТ, служити основою для створення вітчизняних програмно-апаратних середовищ, що відповідають світовому рівню. Відсутня стандартизація технологій безпечного розроблення ПЗ задля створення системи аудиту та виправлення вихідних кодів в продуктах компаній, що є розробниками ПЗ, спрямованої на запобігання небезпечних уразливостей у розроблюваних продуктах. Забезпечення інформаційної безпеки технології «Інтернет речей» ускладнено відсутністю єдиного стандарту їх взаємодії.

Тенденція до зростання цінності інформації як бізнес-ресурсу разом із підвищенням рівня інформаційних загроз призводить до неефективності наявних систем інформаційної безпеки більшої підприємств, специфіка діяльності яких передбачає необхідність захисту не тільки власної інформації та інших відомостей з обмеженим доступом, які отримують співробітники.

Далі проаналізуємо внутрішні причини інформаційних загроз підприємств (табл. 1).

І. Седікова [8] джерела інформаційних загроз об'єднує у такі три групи: природні – вплив факторів навколишнього середовища; антропогенні – дії чи бездіяльність людини (групи людей); технічні – результати використання апаратного та/або програмного забезпечення. Визначені такі суб'єкти антропогенних загроз: наймані працівники підприємства, зокрема звільнені з роботи; пов'язані з підприємством особи; державні службовці, які проводять адміністративний контроль за діяльністю підприємства; особи, які не мають прямого відношення до діяльності підприємства [8].

Таблиця 1

Внутрішні причини виникнення інформаційних загроз підприємств

Причини	Частка респондентів, %
Нерозуміння зв'язку між інформаційною безпекою та проблемами господарської діяльності	19
Ігнорування проблем інформаційної безпеки	17
Делегування повноважень щодо забезпечення інформацією співробітників, які не мають відповідної кваліфікації	15
Недооцінка вартості інформації	13
Вжиття реактивних короткострокових заходів, які не вирішують проблему остаточно	11
Використання поодиноких засобів безпеки без забезпечення їхньої комплексності	8
Відсутність належного контролю за виконанням рішень з інформаційної безпеки	7
Інші причини	2

Вивчення процесу формування та функціонування системи інформаційної безпеки підприємства дало змогу вдосконалити загальну структуру системи інформаційної безпеки підприємства через поєднання основних елементів (суб'єктів та об'єктів), рівнів (оперативного, тактичного, стратегічного) та функцій (управління, ресурсного забезпечення, вжиття заходів) системи інформаційної безпеки підприємства.

Побудована загальна структура системи інформаційної безпеки підприємства дала змогу визначити такі основні групи заходів із забезпечення функціонування системи інформаційної безпеки підприємства: управління системою інформаційної безпеки, ресурсне забезпечення системи інформаційної безпеки та забезпечення інформаційної безпеки. Виходячи з визначення інформаційної ефективності, пропонуємо розглядати ефективність системи інформаційної безпеки як відношення приросту рівня інформаційної безпеки до приросту витрат на систему інформаційної безпеки підприємства.

Серед загроз, які можуть привести до розголошення інформації, за своїми небезпечними наслідками особливе місце посідають несанкціонований доступ до інформації, яка обробляється та циркулює на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, витік інформації технічними каналами [8].

Обґрунтовано, що необхідною умовою отримання позитивного ефекту від вжиття комплексу організаційних заходів є формування директив контролю інформаційної безпеки на основі інформаційного аудиту, який дає змогу оцінити відповідність системи інформаційної безпеки підприємств зберігання та переробки зерна стандартам інформаційної безпеки, які розподіляються на такі дві групи:

- корпоративні (розробляються великими підприємствами, які виробляють інформаційну техніку та програмне забезпечення (IBM, Microsoft, Cisco));
- інституціональні (розробляються всесвітньо відомими організаціями у сфері стандартизації).

Висновки. В результаті дослідження розвинені уявлення щодо взаємозв'язку інформаційної та національної безпеки держави. Під час розбудови інформаційного середовища функціо-

нування об'єктів (суб'єктів) господарювання необхідно враховувати систему таких критеріїв щодо забезпечення ефективної інтеграції України у світовий простір: доступність інформації, мінімізація вартості, актуальність, повнота та аналітичність інформації. Розгляд економічних, правових, психологічних та технічних методів інформаційного захисту та їх використання на підприємствах дадуть змогу розробити удосконалену структуру методів інформаційного захисту на підприємствах за допомогою поєднання пасивно-превентивного, активно-превентивного та реактивного підходів, а також виявити недоліки інформаційного захисту.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Про національну безпеку України: Закон України. Київ, 2014. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#n355> (дата звернення: 28.11.2020).
2. Концепція створення державної системи захисту критичної інфраструктури. Київ, 2017. URL: <https://www.kmu.gov.ua/ua/npas/pro-shvalennya-koncepciyi-stvorenniya-derzhavnoyi-sistemi-zahistu-kritichnoyi-infrastrukturi> (дата звернення: 30.11.2020).
3. Наумова А. Інформаційна безпека: питання правового регулювання: монографія. Київ: Гельветика, 2017. 168 с.
4. Біленчук П. Правові засади інформаційної безпеки України: монографія. Харків, 2018. 289 с.
5. Про критичну інфраструктуру та її захист. Київ, 2018. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996 (дата звернення: 28.11.2020).
6. Стратегія кібербезпеки України. Київ, 2015. URL: <https://zakon5.rada.gov.ua/laws/show/96/2016> (дата звернення: 28.11.2020).
7. Фролова О. Роль ООН в системі міжнародної інформаційної безпеки. Київ, 2016. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/3468/3140 (дата звернення: 25.11.2020).
8. Седікова І. Роль інформаційної складової у системі зберігання та переробки зерна. *Проблеми економіки*. 2016. № 3. С. 143–149.

REFERENCES:

1. Zakon Ukrayiny' "Pro nacional'nu bezpeku Ukrayiny". Ky'yiv, 2014. Available at: <https://zakon.rada.gov.ua/laws/show/2469-19#n355> (accessed 28 November 2020).

2. Koncepciya stvorenniya derzhavnoyi sy'stemy' zaxy'stu kry'ty'-chnoyi infrastruktury. Ky'yiv. 2017. URL: <https://www.kmu.gov.ua/ua/npas/pro-shvalennya-koncepciyi-stvorenniya-derzhavnoyi-sistemi-zahistu-kritichnoyi-infrastrukturi> (accessed 30 November 2020).
3. Naumova A. (2017) *Informacijna bezpeka: py'tannya pravovogo reguluvannya : monografiya* [Information security: issues of legal regulation: monograph]. Kiev: Helvetica, pp. 168. (in Ukrainian)
4. Bilenchuk P. (2018) *Pravovi zasady' informacijnoyi bezpeky' Ukrayiny': monografiya* [Legal bases of information security of Ukraine: monograph]. Xarkiv, pp. 289. (in Ukrainian)
5. Pro kry'ty'chnu infrastrukturu ta yiyi zaxy'st. Ky'yiv, 2018. Available at: http://w1.c1.rada.gov.ua/pls/zweb2/web-proc4_1?pf3511=65996 (accessed 28 November 2020). (in Ukrainian)
6. Strategiya kiberbezpeky' Ukrayiny'. Ky'yiv, 2015. Available at: <https://zakon5.rada.gov.ua/laws/show/96/2016> (accessed 28 November 2020).
7. Frolova O. (2016) *Rol' OON v sy'stemi mizhnarodnoyi informacijnoyi bezpeky* [The role of the UN in the system of international information security]. Available at: http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/3468/3140 (accessed 25 November 2020). (in Ukrainian)
8. Sedikova I. (2016) *Rol' informacijnoyi skladovoyi u sy'stemi zberigannya ta pererobky' zerna* [The role of the information component in the system of storage and processing of grain]. *Problems of the economy*, vol. 3, pp. 143–149. (in Ukrainian)