Formation of an Information Security System in the Field of Storage and Distribution of Food and Energy Resources

UDC: 004.056 DOI: 10.15421/152216

Mordovtsev Oleksandr[1]
Ph.D., Senior Research Scientist, http://orcid.org/0000-0003-1653-5440, acmordov@gmail.com
Avanesova Nina[2]
Dr.Sc., Full Prof., https://orcid.org/0000-0003-3636-9769, Avanesova.science@gmail.com
Lyubushin Roman[2]
Ph.D. Student, https://orcid.org/0000-0001-7896-6524, phd.nauka@gmail.com
[1]The Ukrainian State Scientific Research Institute "Resurs" (Kyiv, Ukraine)
[2]Kharkiv National University of Civil Engineering and Architecture (Kharkiv, Ukraine)

Abstract

The article is devoted to the search for ways to form a real information security system in the field of storage and distribution of food and energy resources of Ukraine, which would respond to external and internal challenges, risks, threats and dangers that our country faces every day. It is found out that the problem of scientific search for a set of measures, means and methods for improving the information security system and increasing managerial potential in this area is an important element for the survival and effective functioning of the entire food and energy complex of the country in war and post-war times. The interaction of the development of information and communication technologies in the food and energy sector with the national security of the country is determined. Threats to information security in the food and energy sectors are systematized. A comprehensive information security system in the field of storage and distribution of food and energy resources has been developed. The subjects and objects of the developed information security system, as well as the goals and priorities of its effective functioning, are clarified. The main components of the system are identified, which include Regulatory Aspects, organizational and technological measures, technical and economic manifestations and social opportunities. It is proved that the exit from the developed system is characterized, on the one hand, by the introduction of methods of effective methods and technologies of Information Protection, which are the "Guardians" of cyberspace of food, energy and other sectors of our country, and on the other – by specific technical and technological features of the sector where they are used. It is concluded that control over the functioning of the developed system and making necessary improvements in response to challenges, threats, risks and dangers that exist in the modern global information space of Ukraine should be carried out on the principles of consistency, complexity and feedback.

Keywords: information security, information and communication technologies, food security, energy security, system, critical infrastructure methods

Citation: Mordovtsev, O., Avanesova, N., & Lyubushin, R. (2022). Formation of an Information Security System in the Field of Storage and Distribution of Food and Energy Resources. *Public Administration Aspects*, 10(3), 21-30. https://doi.org/10.15421/152216

Формування системи інформаційної безпеки у сфері зберігання та розподілу продовольчих та енергетичних ресурсів

Мордовцев Олександр[1], **Аванесова Ніна**[2], **Любушин Роман**[2]
[1]Український державний науково-дослідний інститут «Ресурс» (Київ, Україна)
[2]Харківський національний університет будівництва та архітектури (Харьків, Україна)

Анотація

Статтю присвячено пошуку шляхів формування реально діючої системи інформаційної безпеки у сфері зберігання та розподілу продовольчих та енергетичних ресурсів України, яка б відповідала на зовнішні та внутрішні виклики, ризики, загрози та небезпеки, які постають кожен день перед нашою країною. З'ясовано, що проблема наукового пошуку комплексу заходів, засобів і методів удосконалення системи інформаційної безпеки та підвищення управлінського потенціалу у цій сфері є важливим елементом для виживання та ефективного функціонування усього продовольчо-енергетичного комплексу країни у воєнний та поствоєнний час. Визначено взаємодію розвитку інформаційно-комунікаційних технологій у продовольчій та енергетичній сфері з національною безпекою країни. Систематизовані загрози інформаційній безпеці у продовольчому та енергетичному секторі. Розроблено комплексну систему інформаційної безпеки у сфері зберігання та розподілу продовольчих та енергетичних ресурсів. Уточнені суб'єкти та об'єкти розробленої системи інформаційної безпеки, а також цілі та пріоритети її ефективного функціонування. Визначені основні компоненти системи, які включають в себе нормативно правові аспекти, організаційно-технологічні заходи, техніко-економічні прояви та соціальні можливості. Доведено, що вихід із розробленої системи характеризується, з одного боку, впровадженням методів ефективних методів і технологій захисту інформації, які є «охоронцями» кіберпростору продовольчого, енергетичного та інших секторів нашої країни, а з іншого – конкретними техніко-технологічні особливостями сектору, де вони застосовуються. Зроблено висновок, що контроль за функціонуванням розробленої системи та внесення необхідних удосконалень у відповідь на виклики, загрози, ризики та небезпеки, які існують у сучасному глобальному інформаційному просторі України, повинен здійснюватися на принципах системності, комплексності та зворотного зв'язку.

Ключові слова: інформаційна безпека, інформаційно-комунікаційні технології, продовольча безпека, енергетична безпека, система, критична інфраструктура методи

Цитування: Мордовцев О., Аванесова Н., Любушін Р. Формування системи інформаційної безпеки у сфері зберігання та розподілу продовольчих та енергетичних ресурсів. *Аспекти публічного управління*. 2022. Том 10. №3. С. 21-30. https://doi.org/10.15421/152216

Стаття надійшла / Article arrived: 26.05.2022 Схвалено до друку / Accepted: 30.06.2022

Постановка проблеми.

Проблема динамічного розвитку та зростання обсягів використання інформаційно-комунікаційних технологій у всіх сферах людської діяльності на сьогоднішній день виходить на перший план особливо у воєнних реаліях сьогоднішній України. Нині інформація набуває статусу найважливішого стратегічного ресурсу як держави, так й кожного окремого елемента державної системи, особливо об'єктів продовольчої та енергетичної інфраструктури.

Розвиток нових інформаційно-комунікаційних технологій зумовлює збільшення технологічного розриву між постійно зростаючими вимогами до показників безпеки інформаційних ресурсів суб'єктів продовольчої та енергетичної інфраструктури та можливостями цих технологій і апаратно-програмного забезпечення, що використовуються для забезпечення їх інформаційної безпеки. Тому зростає потреба в науково обґрунтованих методах і технологічних рішеннях для оновлення та вдосконалення системи захисту інформації у сфері зберігання та розподілу продовольчих та енергетичних ресурсів. Таким чином, проблема наукового пошуку комплексу заходів, засобів і методів удосконалення системи інформаційної безпеки та підвищення управлінського потенціалу у цій сфері є важливим елементом для виживання та ефективного функціонування усього продовольчо-енергетичного комплексу країни у воєнний та повоєнний час.

Отже, проблематика забезпечення та зміцнення інформаційної безпеки на об'єктах критичної інфраструктури є гострою темою, яка вирішується на найвищому рівні влади України. На сьогоднішній день для формування ефективної системи безпеки глобального інформаційного простору треба вирішити проблему розвитку вітчизняної індустрії технологій, низької якості підготовки фахівців з протидії інформаційним загрозам і небезпекам, а також активного впровадження практико-орієнтованих підходів щодо забезпечення інформаційної безпеки у продовольчому та енергетичному секторах України.

Аналіз останніх досліджень і публікацій. На цей час, вирішенням проблем щодо формування та сталого функціонування систем та механізмів інформаційної безпеки об'єктів критичної інфраструктури займаються велика кількість вітчизняних та зарубіжних вчених, таких як Нашинець-Наумова А. (2017), Бейкер Дж. (Baker, 2014), Абомхара М., Койен Г. (Abomhara, & Koien, 2015), Сокол К. (Sokol, 2015), Вітко А. (2016), Шолл Е., Вестфал К. (Scholl, & Westphal, 2017), Марутян Р. (2020), Аванесова Н., Мордовцев О. (2020), Бабич М. (2018), Маркевич К., Омельченко В. (2016) та ін. Ці вчені внесли значний вклад до методологічного та практичного вирішення поставлених завдань. Нашинець-Наумова А.Ю. (2017), Baker J. (2014), Abomhara, & Koien (2015) створили актуальну методологічну бази для нашого дослідження щодо забезпечення та зміцнення інформаційної безпеки в контексті її взаємодії за національною безпекою країни. Сокол К. (Sokol, 2015), Вітко А. (2016), Шолл Е. и Вестфал К. (Scholl, & Westphal, 2017) запропонували в своїх наукових працях підгрунтя до формування механізмів забезпечення продовольчої та енергетичної безпеки як на рівні держави, так й на рівні суб'єктів господарювання. Марутян Р. (2020), Аванесова Н., Мордовцев О. (2020), Бабич М. (2018), Маркевич К., Омельченко В. (2016) розглядали окремі елементи і компоненти для створення загальної системи інформаційної безпеки для відповідних суб'єктів.

Однак слід зауважити, що залишаються не вирішеними питання щодо формування єдиної, дієвої та універсальної системи інформаційної безпеки у продовольчій та енергетичній сфері України на довгостроковий період часу.

Мета та завдання дослідження. Метою статті є формування реально діючої системи інформаційної безпеки у сфері зберігання та розподілу продовольчих та енергетичних ресурсів України, яка б відповідала на зовнішні та внутрішні виклики, ризики, загрози та небезпеки, які постають кожен день перед нашою країною.

Виклад основного матеріалу. Як показує теоретичні дослідження та отримані практичні результати, розвиток

інформаційно-комунікаційних технологій генерує нові виклики та загрози національній безпеці, насамперед, тому що інформаційний простір може бути використаний для досягнення військово-політичних, геополітичних та інших цілей (Нашинець-Наумова, 2017). Зростання динаміки та масштабів економічних та інформаційних загроз у сучасному світі зумовлюється невідповідністю між необхідним та існуючим рівнями організації процесів прийняття управлінських рішень та інформаційної взаємодії державних, громадських та приватних структур у продовольчої та енергетичної сферах, що приводить, в свою чергу, до невідповідності між необхідним і наявним рівнями організації процесів зберігання та розподілу продовольчих та енергетичних ресурсів. Недостатнє фінансування цієї сфери також породжує недосконаліть міжвідомчої науково-технічної політики, слабкий рівень розвитку і впровадження інформаційно-комунікаційних технологій, а значить й недостатній захист інформації від навмисного або випадкового втручання, що призводить до витоку важливої політичної, економічної, наукової та військової інформації щодо об'єктів критичної інфраструктури (Baker, 2014; Abomhara, & Koien, 2015).

Таким чином, можна стверджувати, що у системі взаємозв'язків інформаційно-комунікаційних технологій та безпеки зберігання та розподілу продовольчих та енергетичних ресурсів особливе місце посідає проблема інформаційної безпеки, яку породжено значною мірою процесами розвитку цих технологій та становленням інформаційного суспільства в країні. З цього виходить, що інформаційно-комунікаційні технології є «інформаційною зброєю», яка передбачає прагнення окремих суб'єктів (індивідів, груп, держав, коаліцій) до одноосібного володіння інформаційними ресурсами, засобами та технологіями та їх використання для задоволення власних інтересів та протидії інтересам потенційних конкурентів або ворожих держав в економічному, політичному, військовому та іншому протистоянні. Інтеграція інформаційно-комунікаційних технологій також може бути використана для формування та реалізації відповідних загроз ворожих держав продовольчо-енергетичному комплексу нашої країни (Sokol, 2015). Теоретико-методологічних висновком наведених тез є представлена схема взаємодії розвитку інформаційно-комунікаційних технологій продовольчої та енергетичної сфери з національною безпекою країни (рис. 1).

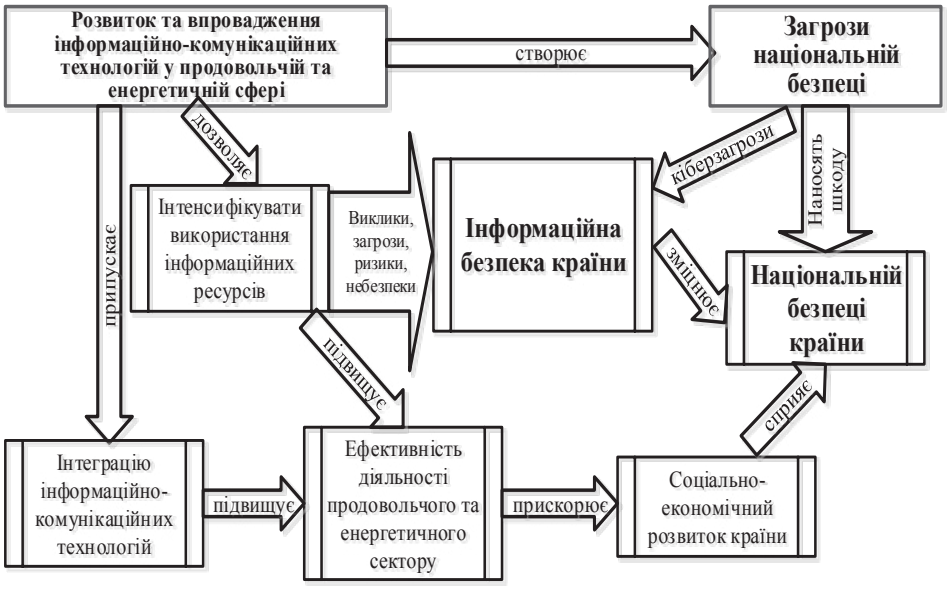

Рис. 1. Взаємодія розвитку інформаційно-комунікаційних технологій у продовольчій та енергетичній сфері з національною безпекою країни

Джерело: розроблено з використанням (Вітко, 2016; Scholl, & Westphal, 2017; Марутян, 2020),

З рис. 1 видно, що інформаційна безпека у сфері зберігання та розподілу продовольчих та енергетичних ресурсів як складова частина загальної системи національної безпеки займає істотне місце у виді системоутворюючої основи забезпечення інших складових національної безпеки. Це визначає необхідність протидії інформаційним, а ширше – кіберзагрозам, а також необхідність забезпечення можливості ефективного функціонування найважливіших інфраструктурних об'єктів держави в умовах інформаційної війни в кіберпросторі.

Слід зазначити, що загрози інформаційній безпеці у продовольчому та енергетичному секторі, які представлені на рис. 1 можна поділити на внутрішні та зовнішні загрози (табл. 1).

Таблиця 1

Загрози інформаційній безпеці у продовольчому та енергетичному секторі

№ з/п	Основні складові загроз інформаційній безпеці у продовольчому та енергетичному секторі
	Внутрішні загрози
1.	Низькі темпи інформатизації та розвитку нових сучасних видів засобів обробки та вилучення інформації (технологічна залежність вітчизняних інформаційних технологій від іноземних виробників)
2.	Навмисні дії, помилки спеціалістів, відповідальних за забезпечення захисту інформації
3.	Недостатня координація та фінансування роботи об'єктів критичної інфраструктури
4.	Недостатній розвиток законодавчої бази країни, особливо в сферах впровадження інноваційних інформаційно-комунікаційних технологій
	Зовнішні загрози
1.	Цілеспрямована політика ворожих іноземних держав щодо витіснення України з глобального інформаційного простору
2.	Втручання ззовні в інформаційне забезпечення державної політики України
3.	Проникнення ворожих суб'єктів в діяльність та інформаційно-комунікаційні технології об'єктів критичної інфраструктури
4.	Технічні впливи ззовні шляхом проникнення в будь-які функціонуючі мережі, системи зв'язку, інформаційні системи тощо
5.	Розробка низкою країн концепцій інформаційних війн, створення інформаційної зброї як одного з головних елементів ведення загальних бойових дій на території та інформаційному просторі країни
6.	Посилення технологічної відокремленості провідних держав світу
7.	Інформаційно-пропагандистська діяльність іноземних ворожих держав, яка може спричиняти диверсії в продовольчо-енергетичному секторі країни
8.	Діяльність міжнародних терористичних організацій, кількість яких збільшилася з початком бойових дій в Україні

Джерело: систематизовано на основі (Аванесова, Мордовцев, & Сергієнко, 2020; Бабич, 2018)

Таким чином, виходячи з наведених в табл. 1 загроз інформаційній безпеці у продовольчому та енергетичному секторі України, з урахуванням розвиненості технічних засобів розвідки та можливості їх офіційного застосування, низька якість розроблених вітчизняних засобів захисту інформації призводить до появи нових різноманітних технічних можливостей витоку інформації, а значить й загрози втрати продовольчих та енергетичних ресурсів країни. Тому для теоретико-практичної цінності нашого наукового дослідження доцільно розробити комплексну систему інформаційної безпеки у сфері зберігання та розподілу продовольчих та енергетичних ресурсів (рис. 2).

Треба відзначити, що суб'єктами системи інформаційної безпеки у сфері зберігання та розподілу продовольчих та енергетичних ресурсів (рис. 2) є держава, державні та приватні продовольчо-енергетичні суб'єкти господарювання, науково-дослідні інститути і лабораторії, а

Рис. 2. Система інформаційної безпеки у сфері зберігання та розподілу продовольчих та енергетичних ресурсів

Джерело: розроблено з використанням (Аванесова, Мордовцев, 2020; Бабич, 2018; Маркевич, & Омельченко, 2016)

також інформаційне суспільство в цілому. Об'єктами цієї системи виступають як інформаційно-комунікаційні технології, так й окремі методи захисту важливої (конфіденційної) інформації суб'єктів наведеної на рис. 1 системи.

Також треба звернути увагу, що без комплексного аналізу вхідної (ретроспективної) інформації щодо стану та розвитку системи інформаційної безпеки як досліджуваних секторів, так й в цілому за об'єктами критичної інфраструктури неможлива ефективна робота усієї розробленої системи та її постійний розвиток для подолання викликів, загроз, ризиків та небезпек, які постійно виникають під час функціонування цих об'єктів.

Основною метою розробленої на рис. 2 системи є стале функціонування продовольчого та енергетичного комплексу країни у складних умовах венного та поствоєного часу на засадах інформаційної захищеності об'єктів критичної інфраструктури цього комплексу з

використанням інноваційних вітчизняних та зарубіжних інформаційно-комунікаційних технологій.

Основні компоненти, які представлені на рис. 2 є «ядром» розробленої системи, тому доцільно розглянути кожен з них більш детально.

І. Нормативно-правовий компонент.

Для здійснення і проведення ефективної державної політики в сфері зберігання та розподілу продовольчих та енергетичних ресурсів, яку повинно бути спрямовано на реалізацію національних інтересів України в інформаційній сфері, державною владою формуються наступні нормативно-правові акти, зокрема:

– концептуальні документи, які визначають пріоритетні напрями розвитку інформаційно-комунікаційних технологій в Україні для забезпечення інформаційної безпеки основних об’єктів критичної інфраструктури;

– законодавчо-нормативні акти в інформаційній сфері, що визначають правила і обмеження в галузі регулювання глобального інформаційного простору для забезпечення та зміцнення інформаційної безпеки;

– організація державного контролю над об’єктами продовольчого на енергетичного сектору у інформаційній сфері.

Отже, забезпечення інформаційної безпеки здійснюється регламентуючими документами і нормативно-правовими актами, що визначають вимоги і критерії, загальну організацію робіт із забезпечення інформаційної безпеки, а також з виробництва та експлуатації систем захисту інформації; порядок виробництва, зберігання, продаж, передача, поширення і споживання інформації в продовольчому та енергетичному секторах країни.

Але треба зазначити, що в умовах сучасногомінливогосередовищатазовнішніх викликів, з якими кожен день стикається наша країна, з'являються нові загрози та небезпеки, зокрема: інформаційний тероризм (кібертероризм); дестабілізація інформаційного поля об’єктів критичної інфраструктури; комп'ютерні атаки; атаки на віртуальні системи; психологічні операції; різні типи інформаційних війн (кібервійна, мережева війна, сетецентрична війна тощо); застосування інформаційної зброї; розробка високотехнологічних засобів розвідки тощо. Це обумовлює необхідність постійного розвитку, вдосконалення та оновлення нормативно-правової бази в інформаційній сфері, а також регулювання та комплексного контролю кіберпростору.

ІІ. Організаційно-технологічний компонент.

Інформаційна діяльність держави визначається діяльністю органів державної влади, з одного боку, в рамках розвитку інформаційної інфраструктури, створення умов для її ефективного функціонування, для вільного доступу громадян до джерел інформації, а з іншого – створенням законодавчих перешкод для доступу громадян до певного виду інформації, розголошення якої може завдати істотної шкоди об'єктам критичної інфраструктури.

В даний час об’єкти продовольчої та енергетичної інфраструктури часто піддаються кібератакам як внутрішнім, так й зовнішнім, що може призвести або призводить до серйозних наслідків, зокрема: видалення файлів із системи, яка відповідає за моніторинг важливих вузлів системи енергетичного забезпечення об’єктів критичної інфраструктури; отримання повного (часткового доступу) до систем розподілу газу та інших енергоносіїв; збоїв у громадянської та воєнної продовольчої логістиці; не дотримання умов зберігання продуктів харчування, що є прямою загрозою продовольчій безпеці тощо.

Для забезпечення зміцнення інформаційної безпеки критичної інфраструктури державна інформаційна політика України реалізується шляхом формування органами державної влади необхідних правових, економічних, організаційних та інших умов, що сприяють зміцненню захисту інформаційного поля та подальшому сталому функціонування в мінливих умовах сьогодення.

ІІІ. Техніко-економічний компонент.

Пріоритетним напрямком державної політики забезпечення інформаційної безпеки в продовольчому та енергетичному секторі України є підвищення конкурентоспроможності вітчизняних виробників і компаній, які спеціалізуються в галузі інформаційних технологій, що

займаються виробництвом і експлуатацією засобів захисту інформації.

Така політика набуває особливої актуальності у зв'язку з повільними процесами інформатизації в нашій країні, застарілим вітчизняним програмним забезпеченням, засобами інформатизації, засобами захисту безпеки критичної інфраструктури. Тому суб'єкти системи інформаційної безпеки у сфері зберігання та розподілу продовольчих та енергетичних ресурсів при розробці та експлуатації систем захисту інформації використовують обладнання та програмне забезпечення здебільшого іноземного виробництва, при цьому не завжди проводячи спеціальні перевірки і сертифікація цих технічних засобів обробки інформації, а також автоматизованих робочих місць для таких технічних засобів, що підвищує ризики несанкціонованого доступу до інформації, яка зберігається та обробляється.

IV. Соціальний компонент.

Цей компонент системи передбачає підготовку фахівців у сфері інформаційної безпеки, а також забезпечення раціонального та ефективного використання технічних засобів та інформаційних систем, що є найважливішим елементом сталого функціонування суб'єктів системи у глобальному інформаційному просторі.

Проблема недостатнього кадрового забезпечення у сфері інформаційної безпеки об'єктів критичної інфраструктури загострюється кожен рік та є одним із головних недоліків у системі інформаційної безпеки будь-якого суб'єкта системи та основною причиною успіху кібератак, які здійснюються внутрішніми та зовнішніми кіберзлодіями. Зростаюча координація і масштабність інформаційних атак на критично важливі об'єкти інформаційно-комунікаційної інфраструктури продовольчого та енергетичного секторів України вимагає забезпечення високого рівня готовності сил і засобів попередження та виявлення комп'ютерних атак, з наступною ліквідацією наслідків їх проведення.

Треба відзначити, що порушення правил експлуатації інформаційно-комунікаційних технологій, зокрема, відбувається через слабкий контроль керівництва та низький рівень відповідальності за порушення у сфері захисту інформації. Нині це завдання вирішується в рамках діючої системи підготовки, перепідготовки та підвищення кваліфікації кадрів у цій сфері. Водночас зростання нових викликів і загроз в інформаційному просторі зумовлює необхідність вжиття додаткових заходів щодо вдосконалення цієї системи.

Для вирішення цих проблем необхідно забезпечити цільову підтримку та підготовку фахівців з інформаційної безпеки в рамках окремої групи спеціальностей і напрямів підготовки (при цьому повинен бути дотримуватися принцип рівної участі технічної та економічної складової під час навчання), підвищити ефективність функціонування спеціалізованих навчальних закладів, у тому числі за рахунок розвитку їх матеріально-технічної бази.

Таким чином, складність і взаємопов'язаність завдань підвищення кадрової безпеки в інформаційній сфері зумовлює необхідність вжиття додаткових заходів нормативно-правового, організаційного та матеріально-технічного характеру.

Вихід із розробленої системи на рис. 2 характеризується, насамперед, впровадженням методів ефективних методів і технологій захисту інформації, які є «охоронцями» кіберпростору продовольчого, енергетичного та інших секторів нашої країни.

Запропоновано використовувати наступні методи для сталого функціонування системи інформаційної безпеки у сфері зберігання та розподілу продовольчих та енергетичних ресурсів (табл. 2).

Пошук та реалізація оптимальних рішень щодо забезпечення та зміцнення інформаційної безпеки у сфері зберігання та розподілу продовольчих та енергетичних ресурсів повинні спиратися не тільки за представлені в табл. 2 методи та технології захисту інформації, а й конкретні техніко-технологічні особливості сектору, де вони застосовуються. Прикладом такого підходу може слугувати наступні системні функції операторів підприємств енергетики, які закладають основу для створення кібербезпеки у глобальному інформаційному просторі, а саме:

– управління технологічними режимами роботи об'єктів електроенергетики в порядку,

Таблиця 2

Методи і засоби захисту інформації

№ з/п	Методи (технологія) захисту інформації	Складові та характеристика методу (технології) захисту інформації
I.	Організаційні	До них відносяться заходи, що регламентуються внутрішніми положеннями та інструкціями суб'єктів системи. Вони здійснюють підтримку технологічних методів і засобів та є невід'ємною частиною політики інформаційної безпеки суб'єктів, яка здійснюється за допомогою: – визначення повноважень і посадових обов'язків, контроль за порядком доступу співробітників до важливої (конфіденційної) інформації; – навчання та інформування співробітників, регулярне проведення семінарів та тренінгів з питань інформаційної безпеки; – присвоєння грифів секретності і міток конфіденційності документам і матеріалам; – визначення порядку зберігання та знищення носіїв інформації; – визначення порядку реєстрації користувачів інформаційної системи, видачі, зберігання та відкликання паролів, секретних ключів тощо.
II.	Технологічні	До них відноситься наступні елементи, зокрема: – програмно-технічні модулі захисту, а саме: програмні та антивірусні системи; системи ідентифікації та аутентифікації, контролю доступу, реєстрації та аудиту подій; системи резервного копіювання та відновлення інформації; міжмережеві екрани тощо; – апаратні засоби, а саме: шифрувальне обладнання; джерела безперебійного живлення; спеціальні системи вентиляції та кондиціонування. планування тощо; – технічні системи контролю фізичного доступу, охоронно-пожежної сигналізації, системи відеоспостереження тощо. – криптографічні методи захисту інформації (тобто шифрування та електронного підпису даних)
III.	Правові	Передбачають механізми розвитку та вдосконалення нормативно-правової бази, що регулює захист інформації; заходи контролю за виконанням нормативно-правових актів загальнодержавного значення; розроблення в організації нормативних та нормативно-методичних актів (інструкцій, положень) з питань інформаційної безпеки та захисту інформації.

встановленому основними положеннями про функціонування ринку;

– дотримання встановлених параметрів надійності та якості електричної енергії;

– регулювання частоти електричного струму, забезпечення функціонування системи автоматичного регулювання частоти електричного струму та потужності, системи та протиаварійної автоматики;

– участь в організації діяльності з прогнозування обсягів виробництва і споживання в електроенергетиці, прогнозування обсягів виробництва і споживання в електроенергетиці та участь у процесі формування резерву виробничих енергетичних потужностей;

– координація введення в експлуатацію та виведення з експлуатації об'єктів електромереж та енергетики з виробництва електричної та теплової енергії, а також введення їх в експлуатацію після ремонту;

– видача обов'язкових для виконання функцій суб'єктам електроенергетики та споживачам електричної енергії з регульованим навантаженням оперативно-диспетчерські команди та розпорядження;

– розробка оптимальних добових графіків роботи електростанцій і електричних мереж;

– організація та управління режимами паралельної роботи електроенергетичної системи України та електроенергетичних систем країн Європи;

– моніторинг фактичного технічного стану та рівня експлуатації об'єктів електроенергетики.

Контроль за функціонуванням розробленої системи та внесення необхідних удосконалень у відповідь на виклики, загрози, ризики та небезпеки, які існують у сучасному глобальному інформаційному просторі України (рис. 2), повинен здійснюватися на принципах системності, комплексності та зворотного зв'язку.

Таким чином, стале функціонування розробленої на рис. 2 системи забезпечить приведення інформаційно-комунікаційних систем продовольчих та енергетичних суб'єктів господарювання у відповідність до вимог нормативно-методичних документів у сфері інформаційної безпеки, підвищить ефективність прийнятих управлінських рішень, а також забезпечить раціональний баланс між принципом відкритості діяльності суб'єктів системи для інформаційного суспільства та принципом захисту інформації від витоку, негативного впливу та несанкціонованого доступу.

Висновки та перспективи подальших досліджень.

У статті були проведенні дослідження теоретико-методологічної та практичної складової загальної системи національної безпеки України, а саме – інформаційної безпеки об'єктів продовольчої та енергетичної інфраструктури та отримані наступні результати.

1. Визначено взаємодію розвитку інформаційно-комунікаційних технологій у продовольчій та енергетичній сфері з національною безпекою країни та виявлено, що інформаційна безпека у сфері зберігання та розподілу продовольчих та енергетичних ресурсів як складова частина загальної системи національної безпеки займає істотне місце у виді системоутворюючої основи забезпечення інших складових національної безпеки.

2. Систематизовані загрози інформаційній безпеці у продовольчому та енергетичному секторі, які поділяються на загрози, які породжує внутрішнє середовище країни (державні органи влади усіх рівнів, суб'єкти господарювання, інформаційне суспільство) та загрози, що виникають на тлі мінливості зовнішнього середовища, в якому так чи інакше присутня наша країна.

3. Сформовано універсальну, дієву та комплексу систему інформаційної безпеки у сфері зберігання та розподілу продовольчих та енергетичних ресурсів, яка має наступні елементи, зокрема:

– вхід у систему, що характеризується визначенням суб'єктів та об'єктів, які функціонують та взаємодіють в рамках системного підходу; наявністю ретроспективної інформації щодо поточного стану інформаційної безпеки на об'єктах продовольчої та енергетичної інфраструктури; постоновкою цілей та пріоритетів подальшого розвитку системи;

– компоненти системи, які поділяються на нормативно-правові, організаційно-технологічні, матеріально-технічні та соціальні;

– вихід із системи, де доведено, що пошук та реалізація оптимальних рішень щодо забезпечення та зміцнення інформаційної безпеки у сфері зберігання та розподілу продовольчих та енергетичних ресурсів повинні спиратися не тільки за представлені в дослідженні методи та технології захисту інформації, а й конкретні техніко-технологічні особливості сектору, де вони застосовуються.

Зроблено узагальнюючий висновок, що стале функціонування розробленої на рис. 2 системи забезпечить приведення інформаційно-комунікаційних систем продовольчих та енергетичних суб'єктів господарювання у відповідність до вимог нормативно-методичних документів у сфері інформаційної безпеки, підвищить ефективність прийнятих управлінських рішень, а також забезпечить раціональний баланс між принципом відкритості діяльності суб'єктів системи для інформаційного суспільства та принципом захисту інформації від витоку, негативного впливу та несанкціонованого доступу.

БІБЛІОГРАФІЧНІ ПОСИЛАННЯ

Аванесова, Н. Е., Мордовцев, О. С., & Сергієнко, Ю. І. (2020). Теоретико-методичні засади ідентифікації та взаємозв'язку впливу дестабілізуючих факторів на економічну безпеку промислового підприємства. *Бізнес Інформ*, 9, 20-28. Відновлено з https://doi.org/10.32983/2222-4459-2020-9-20-28

Бабич, М. М. (2018). *Формування системи продовольчої безпеки: теорія, методологія, практика*. (Монографія). Миколаїв: вид. відділ МНАУ.

Вітко, А. Л. (2016). Сфера забезпечення енергетичної безпеки держави як об'єкт публічного адміністрування. *Вісник Харківського національного університету внутрішніх справ*, 3 (66), 144-152.

Маркевич, К., & Омельченко, В. (2016). *Глобальні енергетичні тренди крізь призму національних інтересів України: Аналітична доповідь*. Київ: Заповіт.

Марутян, Р. Р. (2020). Механізми інтелектуального забезпечення політики національної безпеки України: зміст та структура. *Web of Scholar: international academy journal*, 1(43), 26-31.

Нашинець-Наумова, А. Ю. (2017). *Інформаційна безпека: питання правового регулювання*. (Монографія). Київ: Видавничий дім «Гельветика».

Abomhara, M., & Koien, G. (2015). Cyber Security and the Internet Of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security,* 4, 65-88.

Baker, J. (2014). Process, Practice and Principle: Teaching National Security Law and the Knowledge that Matters Most. *The Georgetown Journal of Legal Ethics*, 27, 163-189.

Scholl, E., & Westphal, K. (2017). *European Energy Security Reimagined. Berlin: Stiftung Wissenschaft und Politic*.

Sokol, K. (2015). Assessing the Scale and Readiness of Companies to Enter the World Market of Informational Technologies. *Journal L'Association 1901 "SEPIKE"*, 9, 182-186.

REFERENCES

Abomhara, M., & Koien, G. (2015). Cyber Security and the Internet Of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security*, 4, 65-88.

Avanesova, N., Mordovcev, O., & Serghijenko, Ju. (2020). Theoretical and Methodological Foundations of Identification and Interrelation of the Influence of Destabilizing Factors on the Economic Security of an Industrial Enterprise. *Biznes Inform*, 9, 20-28. Retrieved from https://doi.org/10.32983/2222-4459-2020-9-20-28

Babych, M. M. (2018). *Formation of Food Security System: Theory, Methodology, Practice*. (Monograph). Mykolaiv: MNAU.

Baker, J. (2014). Process, Practice and Principle: Teaching National Security Law and the Knowledge that Matters Most. *The Georgetown Journal of Legal Ethics*, 27, 163-189.

Markevych, K., & Omeljchenko, V. (2016). *Global Energy Trends through the Prism of National Interests of Ukraine: Analytical Report*. Kyjiv: Zapovit.

Marutjan, R. (2020). Mechanisms of Intellectual Support of the National Security Policy of Ukraine: Content and Structure. *Web of Scholar : international academy journal*, 1(43), 26-31.

Nashynecj-Naumova, A. (2017). *Information Security: Issues of Legal Regulation*. Kyjiv: Vydavnychyj dim «Gheljvetyka».

Scholl, E., & Westphal, K. (2017). *European Energy Security Reimagined*. Berlin: Stiftung Wissenschaft und Politic.

Sokol, K. (2015). Assessing the Scale and Readiness of Companies to Enter the World Market of Informational Technologies. *Journal L'Association 1901 "SEPIKE"*, 9, 182-186.

Vitko, A. (2016). Sphere of Ensuring Energy Security of the State as an Object of Public Administration. *Visnyk Kharkivsjkogho nacionaljnogho universytetu vnutrishnikh sprav*, 3(66), 144-152.