ПЕРУН Т. С.,
кандидат юридичних наук,
асистент кафедри адміністративного
та інформаційного права
*(Навчально-науковий інститут права,
психології та інноваційної освіти
Національного університету
«Львівська політехніка»)*

УДК 001.102:34:004
DOI https://doi.org/10.32842/2078-3736/2020.3.25

ОРГАНІЗАЦІЙНО-ПРАВОВІ МОДЕЛІ РЕАЛІЗАЦІЇ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

У контексті визначення інформації як стратегічного ресурсу будь-якої держави, продуктивної сили і цінного майна розглядаються проблеми інформаційної безпеки. Їх вирішення потребує належного правового регулювання і вироблення національної моделі інформаційної безпеки.

Оскільки інформаційна безпека – це невід'ємна частина загальної та національної безпеки, зміст якої базується насамперед на положеннях Конституції України, а також на положеннях основних базових документів, у роботі виділені рівні інформаційної безпеки, дано характеристику принципів інформаційної безпеки.

Формулюються найважливіші завдання забезпечення інформаційної безпеки України. Задаються напрями забезпечення інформаційної безпеки, а також організаційно-технічні заходи щодо захисту інформації в загальнодержавних інформаційних і телекомунікаційних системах.

Пропонується до розгляду розроблена організаційно-правова модель забезпечення інформаційної безпеки України – Модель застосування інформаційних ресурсів для захисту територіальної цілісності держави (модель інформаційного захисту). Виділені об'єкти захисту інформації: персональні дані людини, різні технічні засоби, інформаційно-технічні системи, документи та ін.

Також у роботі досліджено поняття й основні напрями формування інформаційної політики держави. Проведено порівняльний аналіз державної інформаційної політики країн ЄС як основного орієнтира для України у сфері глобалізаційних процесів. Визначено моделі інформаційної безпеки країн ЄС.

У роботі робиться висновок про те, що інформаційна безпека є складовою частиною загальної економічної та національної безпеки й охоплює всі сфери діяльності. Україні потрібна власна модель інформаційної безпеки для захисту законних прав та інтересів громадян, а також територіальної цілісності держави.

Ключові слова: *інформація, інформаційна безпека, захист інформації, інформаційна сфера, організаційно-правова модель.*

Perun T. S. Organizational and legal models of information security policy implementation in Ukraine

In the context of the informational information of a strategic resource of any power, productive strength and valuable mine, problems of informational security are seen. First, I will require proper legal regulation and the first national model of information technology.

So, as the information on the security is completely unimportant, the country is based on the provisions of the Constitution of Ukraine, as well as on the provisions of the basic documents, as well as the operation of the basic principles.

I am formulated to have the best care of the information security of Ukraine. I am asking myself about securing information security, as well as organizational and technical support, go to clean up information in the overseas information and telecommunication systems.

Organizational security has been scrutinized – the legal model of securing information security in Ukraine is a model of information resources for the purpose of clearing territorial power (the information technology model). Views on information technology: personal data, technical information, information and technology systems, documents and information.

Also in the robot, the main understanding of the main form of the information and political policies of the state. The analysis of the sovereign information policy of the Republic of Kazakhstan was conducted, as the main unit for Ukraine in the sphere of globalization processes.

The robots have to worry about those that have information on safety and security є the storage part of the foreign and national safety and security and all areas of the world. Ukrainian government is a model of information security for the purse of legal rights and interests of the population as well as territorial rights of the state.

Key words: *information, information security, information protection, information sphere, organizational-legal model.*

Істинно тотальна війна –
це війна за допомогою інформації.
Маршал Маклюен

Вступ. Початок XXI ст. характеризується активним розвитком інформаційних технологій в усіх сферах суспільного життя. Інформація щодня дедалі більшою мірою стає стратегічним ресурсом, продуктивною силою і цінним товаром у будь-якій державі. Це зумовлює прагнення держав, організацій та окремих громадян одержати дохід за рахунок заволодіння інформацією, нанесення шкоди інформаційним ресурсам опонентів, а також захисту своєї інформації.

У період військової агресії та загрози територіальній цілісності України від правильного вибору організаційно-правової моделі забезпечення інформаційної безпеки залежить безпека держави загалом і кожного громадянина України зокрема.

Питання реалізації політики інформаційної безпеки становлять значний суспільний і науковий інтерес. Детальний аналіз наукових праць вчених економістів, юристів, політологів, психологів дає можливість висвітлити проблему з різних позицій і сформувати дієві рекомендації щодо формування унікальної організаційно-правової моделі інформаційної політики безпеки. Отож, питання формування інформаційного суспільства, аналізуються у працях В. Брижко, Р. Броун, М. Віттман і Н. Маттord, Л. Ірвінг, М. Кастельса, К.Г. Почепцова та ін. Проблеми формування державної політики досліджують С. Арнштейн, А. Таліб, О. Крюков, Р. Калюжний, В. Нікітін, О. Радченко. Питання забезпечення національної безпеки розглядаються у працях Г. Головко, С. Домбровської, В. Косевцова, Ю. Машкарова, Н. Нижник, В. Садкового, В. Стрельцова. Проте наукові дослідження висвітлюють теоретичні проблеми у сфері функціонування інформаційного суспільства або виключно технологічні аспекти впровадження інформаційних технологій. Проте залишається недостатньо дослідженою проблематика інформаційної безпеки держави в умовах військової агресії та загрози територіальній цілісності, що й актуалізує тему статті, визначає її мету та завдання.

Постановка завдання. Метою дослідження є науково-теоретичне обґрунтування та підготовка практичних рекомендацій щодо вдосконалення організаційно-правової моделі реалізації політики у сфері інформаційної безпеки.

Результати дослідження. Сьогодні в Україні активно формується правовий, економічний, фінансовий і політичний базис системи інформаційної безпеки, що визначається, як група однорідних правовідносин суб'єктів інформаційного простору, які за допомогою планових, оперативних, антикризових і комунікаційних заходів здійснюють перманентний вплив на об'єкти інформаційної інфраструктури. Із запропонованого автором визначення можна зробити висновок, що суб'єкти реалізації інформаційної політики є основним системоутворюючим елементом системи національної інформаційної безпеки, і від рівня їх ефективності та професіоналізму залежить стан реалізації інформаційної політики.

А. Таліб інформаційну безпеку визначає як стан інформаційного законодавства та регламентованих ним інститутів безпеки, які гарантують постійну наявність баз даних для реалізації стратегічних рішень і захист інформаційних ресурсів держави [1].

М. Віттман і Н. Маторд зазначають, що інформаційна безпека – це сукупність правових, організаційних і технічних заходів, спрямованих на формування та використання технологічних, інфраструктурних та інформаційних ресурсів для захисту інформації загальнодержавного значення, а також прав і законних інтересів суб'єктів, що беруть участь у інформаційних правовідносинах [2].

На думку Р. Калюжного, інформаційна безпека – це група інформаційних правовідносин щодо формування, підтримки та захисту необхідних для людини, суспільства й держави умов життєдіяльності, спеціалізованих правовідносин щодо створення, зберігання, поширення і використання інформації [3, с. 5].

Вон Солм пропонує таке визначення інформаційної безпеки – це не лише технологічна, а і правова захищеність інформаційної діяльності, що забезпечує її формування та розвиток в інтересах громадян, організацій і держави загалом [4, с. 50].

А. Ахмад вважає, що інформаційна безпека – це захист встановлених законодавством правил, якими регламентуються інформаційні процеси у країні, що забезпечують гарантовані Конституцією умови життєдіяльності людини, держави та суспільства загалом [5].

На основі аналізу зазначених наукових позицій автор доходить висновку, що *система забезпечення інформаційної безпеки* – це комплексна й узгоджена діяльність уповноважених суб'єктів інформаційної безпеки, регламентована нормами міжнародного та національного права, метою якої є запобігання виникненню та реалізації ризиків для безпеки інформаційного простору держави загалом і кожного громадянина зокрема.

Виокремлення ж кібернетичної безпеки зумовлене особливостями середовища функціонування інформаційних систем, у яких здійснюється обіг інформації, реалізація прав і законних інтересів громадян у сфері захисту інформації. А отже, кібернетичний елемент може бути властивим усім складникам інформаційної безпеки, тому ми говоримо не про самостійний інститут інформаційного суспільства, а про забезпечення кібербезпеки безпеки в інформаційній сфері, адже в Законі України «Про основні засади забезпечення кібербезпеки України», прийнятому 5 жовтня 2017 р., *кібербезпека* визначена як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [7].

В.О. Негодченко наводить у своїй науковій праці здійснює порівняльну характеристику суб'єктів забезпечення державної інформаційної безпеки. Особливу роль, на думку автора, відіграють органи Національної поліції України. У дослідженні також обґрунтовано неефективність системи забезпечення державної інформаційної безпеки, що зумовлено наділенням широкого кола суб'єктів дублюючими повноваженнями та відсутністю єдиних стандартів ефективності їх роботи (наприклад, окремі з них наділені повноваженнями щодо формування та реалізації інформаційної політики водночас) [6].

Зазначену проблему законодавець намагається регламентувати шляхом прийняття Стратегії кібербезпеки України від 15 березня 2016 р. № 96/2016, у якій визначено, що наці-

ональна система кібербезпеки має насамперед забезпечити ефективну взаємодію державних органів, органів місцевого самоврядування, військовослужбовців, правоохоронних органів, наукових і навчальних закладів, об'єднань громадян, підприємств, установ та організацій незалежно від форми власності, які працюють у сфері електронних комунікацій, захисту інформації та / або володіють об'єктами критичної інформаційної інфраструктури [8]. Отже, ефективність реалізації інформаційної політики залежить насамперед від злагодженої системи взаємодії органів державної влади та місцевого самоврядування.

До суб'єктів забезпечення інформаційної безпеки належать:

Верховна Рада України	– визначає засади зовнішньої та внутрішньої політики держави в інформаційній сфері; – створює правові засади функціонування системи забезпечення національної безпеки в інформаційній сфері; – затверджує загальнодержавні програми в цій сфері та контролює хід їх виконання; – затверджує бюджетні асигнування для фінансування діяльності із забезпечення національної безпеки в інформаційній сфері; – визначає порядок створення та повноваження Ради національної безпеки й оборони України; – призначає за поданням Президента України, Прем'єр-міністра України, Міністра оборони України, Міністра закордонних справ України, Голови Служби безпеки України, призначення за поданням Прем'єр-міністра України інших членів Кабінету Міністрів України, Голови Антимонопольного комітету України, Голови Державного комітету телебачення та радіомовлення України, звільнення зазначених осіб із посад. Вирішення питання про відставку Прем'єр-міністра України, членів Кабінету Міністрів України, Голови Служби безпеки України; – призначає на посади та звільняє половини складу Національної ради України з питань телебачення і радіомовлення (НРУТР); – надає згоду на призначення на посаду та звільнення з посади Президентом України Генерального прокурора України; може висловлювати недовіру Генеральному прокуророві України, що має наслідком його відставку з посади; – призначає на посаду та звільняє з посади Уповноваженого Верховної Ради України з прав людини; заслуховує його щорічні доповіді про стан дотримання та захисту прав і свобод людини в Україні; – здійснює контроль за діяльністю Кабінету Міністрів України відповідно до цієї Конституції та закону
Президент України	– забезпечує державну незалежність, національну безпеку і правонаступництво держави; – представляє державу в міжнародних відносинах, здійснює керівництво зовнішньополітичною діяльністю держави, веде переговори й укладає міжнародні договори України; – очолює Раду національної безпеки й оборони України; – визначає і затверджує основи політики національної безпеки України; – здійснює керівництво в інформаційній та інших сферах національної безпеки й оборони України; – здійснює контроль і координацію діяльності державних органів у забезпеченні національної безпеки в інформаційній та інших сферах; – вживає оперативні заходи з метою нейтралізації загроз національним інтересам України в межах компетенції, визначеної Конституцією; – здійснює контроль за реалізацією заходів у сфері національної безпеки в межах своїх повноважень

Закінчення табл.

Кабінет Міністрів України	забезпечує здійснення інформаційної політики держави, фінансування програм, пов'язаних з інформаційною безпекою, спрямовуватиме і координуватиме роботу міністерств, інших органів виконавчої влади у цій сфері.
Рада національної безпеки і оборони України	відповідно до Конституції України й у встановленому законом порядку здійснює координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері.
Міністерство інформаційної політики України	– організація та забезпечення: – моніторингу засобів масової інформації та загальнодоступних ресурсів вітчизняного сегмента мережі Інтернет із метою виявлення інформації, поширення якої заборонене в Україні; – моніторингу загроз національним інтересам і національній безпеці в інформаційній сфері; – сприяння Міністерству закордонних справ України щодо донесення офіційної позиції України до іноземних засобів масової інформації; – формування поточних пріоритетів державної інформаційної політики, контролю їх реалізації; – координації діяльності центральних і місцевих органів виконавчої влади у сфері забезпечення інформаційного суверенітету України; – урядових комунікацій; – кризових комунікацій, зокрема під час проведення антитерористичної операції та в особливий період; – вжиття заходів в інформаційній сфері, пов'язаних із запровадженням правових режимів надзвичайного чи воєнного стану; – розроблення стратегічного наративу і його імплементації; – вироблення і впровадження стратегії інформаційного забезпечення процесу звільнення та реінтеграції тимчасово окупованих територій; – розроблення та впровадження єдиних стандартів підготовки фахівців у сфері урядових комунікацій для потреб державних органів.
Міністерство закордонних справ України	– формування та реалізацію стратегії публічної та культурної дипломатії України; – координацію інформаційної діяльності державних органів у зовнішньополітичній сфері; – забезпечення просування інтересів України за кордоном інформаційними засобами; – забезпечення донесення позиції України до керівництва іноземних держав, парламентів та урядів, зовнішньополітичних відомств, представників бізнесу й експертних кіл, широкої громадськості, сприяння просуванню позитивного іміджу України; – сприяння просуванню українських телеканалів у кабельні та супутникові мережі за кордоном; – забезпечення налагодження взаємодії з міжнародними партнерами як на двосторонній, так і на багатосторонній основі з метою застосування міжнародного досвіду та найкращих практик у контексті протидії інформаційним загрозам.
Служба безпеки України	– моніторинг спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та мережі Інтернет із метою виявлення загроз національній безпеці України в інформаційній сфері; – протидію проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуацій.

Проте побудова організаційно-правової моделі забезпечення інформаційної безпеки в Україні потребує детального аналізу міжнародного досвіду у зазначеній сфері. Політика інформаційної безпеки ЄС – це політика взаємодії країн – членів Співтовариства у галузі інформаційних телекомунікацій, узгоджена учасниками міжнародного співтовариства, спрямована на співробітництво в галузі інформації та комунікації [9]. В основу політики інформаційної безпеки ЄС покладено доктрину європейського інформаційного суспільства, Resolution on «Europe and the global information society – Recommendations to the European Council», основна ідея якої полягає у зміні пріоритетів від геополітики до політики вільного інформаційного простору. Політика у зазначеній сфері реалізується шляхом створення міжнародних регіональних організацій, які протистоять загрозам і викликам інформаційного суспільства європейських держав [10].

У рамках забезпечення інформаційної безпеки ЄС реалізується близько п'ятисот грантових програм і проектів, спрямованих на глобальний розвиток інформаційного суспільства, ефективність інформаційної галузі та впровадження новітніх технологій в усі сфери життя громадян країн ЄС. Європейський Союз сприяє активному розвитку наукових досліджень у галузі захисту інформаційних технологій і систем зв'язку за різними стратегічними напрямами європейського розвитку на основі реалізації інтелектуального потенціалу та перманентного об'єднання інформаційних ресурсів. Стратегії глобального телекомунікаційного протистояння покладені в основу аналітичних розробок науковців різних країн, метою яких є саме забезпечення лідерства у сфері міжнародної інформаційної безпеки.

Результатом досліджень стало виділення таких моделей системи глобальної інформаційної безпеки: ***Модель країни-інфолідера*** – створення абсолютної тотальної системи захисту від будь-якого виду наступальної інформаційної зброї, що зумовлює беззаперечні переваги у потенційній інформаційній війні, змушує інші країни вести переговори у з країною-лідером. Застосовують систему жорсткого контролю над інформаційним ресурсами інших країн на підставі положень міжнародно-правових актів з інформаційної безпеки.

Модель держави – ініціатора інформаційної війни – створення шляхом значного бюджетного фінансування значної переваги держави – в наступальних видах озброєнь, у протидії системам інформаційного захисту держави-противника, координація дій із державами-партнерами у застосуванні заборонених засобів інформаційної зброї для встановлення та знешкодження будь-яких джерел і типів інформаційних загроз.

Модель перманентного протистояння країн-інфолідерів передбачає наявність кількох сильних держав із протилежною ідеологією, що стало причиною потенційного протиборства між ними, стримування можливої експансії інформаційних загроз, забезпечення домінантного становища однієї держави у сфері міжнародної інформаційної безпеки, що надає їй інструменти значного впливу на глобальну інформаційну сферу та можливість вирішувати питання глобального світового устрою.

Модель формування ситуативних інформаційних альянсів – всі учасники протистояння використовують транспарентність інформації для формування тимчасових політичних об'єднань, для формування локальних інформаційних рішень, які спроможні заблокувати інформаційне лідерство країн-агресорів, для усунення політичних загроз на окремих територіях, а також із метою запобігання внутрішнім конфліктам опозиції (політичним, соціальним, расовим, сепаратистським, міжнаціональним конфліктам) для проведення міжнародних антитерористичних операцій [11].

Використовуючи запропоновані моделі, а також положення міжнародних і національних актів, пропонуємо сформувати унікальну національну систему інформаційної безпеки.

Закон України «Про інформацію» визначає поняття «державна інформаційна політика» як сукупність основних напрямів і способів діяльності держави по одержанню, використанню, поширенню та зберіганню інформації. Державну інформаційну політику розробляють і здійснюють органи державної влади загальної компетенції, а також відповідні органи спеціальної компетенції [12].

Національна модель інформаційної безпеки України – це ***Модель застосування інформаційних ресурсів для захисту територіальної цілісності держави (модель інформаційного захисту)***. Вона включає: систему міжнародних і національних нормативних актів, визначене законодавством коло суб'єктів забезпечення інформаційної безпеки, цілі, принципи мету і завдання (рис. 1).

Рис. 1. Політика інформаційної безпеки

Зазначена модель ґрунтується на засадах: пріоритетності наукового, технічного та інноваційного розвитку країни; формування сприятливих законодавчих та економічних умов; гармонійного розвитку загальнодоступної інформаційної інфраструктури, інформаційних ресурсів і забезпечення безперешкодного доступу до телекомунікаційних послуг; сприяння збільшенню різноманітності та кількості електронних послуг, створенню загальнодоступних електронних інформаційних ресурсів; посилення мотивації використання усього потенціалу інформаційних ресурсів; широкого впровадження систем захисту інформації в науці, освіті, культурі, охороні здоров'я, охороні навколишнього середовища; захисту інформаційної безпеки.

Висновки. Отже, формування та розвиток інформаційного суспільства в Україні потребує вироблення єдиної моделі реалізації інформаційної політики безпеки для створення цілісної системи національного інформаційного законодавства, яке відповідало би принципам міжнародного права. Головними шляхами реалізації державної політики інформаційної безпеки повинні стати: розвиток збалансованого інформаційного простору України, формування системи державних стратегічних комунікацій, інформаційна реінтеграція непідконтрольних територій Луганської та Донецької областей, а також Криму, популяризація України та її цінностей у світі. Запропонована ***Модель застосування інформаційних ресурсів для захисту територіальної цілісності держави (модель інформаційного захисту)*** дозволить уникнути інформаційних ризиків, невдачі інновацій і втрати репутації, забезпечити прозорість процесу та підвищить продуктивність використання інформаційних технологій.

Список використаних джерел:

1. Abu Talib, M., Khelifi, A., El Barachi, M., Ormandjieva, O. Guide toISO 27001: UAE Case Study. *Issues in Informing Science & Information Technology.* 2012. № 9 (19). P. 331–349.

2. Whitman, M., Mattord, H. Management of information security. Boston : Course Technology Cengage Learning, 2014.

3. Калюжний Р.А., Баєв О.О. Нормативно-правове забезпечення інформаційної безпеки України. *Правова інформатика*. 2009. № 4 (24). С. 5–12.

4. Von Solms, R. Information security management: why standards are important. *Information Management & Computer Security*. 1999. № 7 (1). P. 50–58.

5. Ahmad, A., Maynard, S.B., and Shanks, G. A Case Analysis of Information Systems and Security Incident Responses. *International Journal of Information Management*. 2015.

6. Негодченко В.О. Сучасний підхід до виокремлення функцій органів Національної поліції України у сфері забезпечення державної інформаційної політики. *Вісник Харківського національного університету внутрішніх справ.* 2016. Вип. 4. С. 176–188. URL: http://nbuv.gov.ua/UJRN/VKhnuvs_2016_4_26.

7. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/ show/2163-19 (дата звернення: 18.04. 2020).

8. Про Стратегію кібербезпеки України : Указ Президента України від 15 березня 2016 р. № 96/2016. URL: https://https://zakon.rada.gov.ua/laws/ show/n0003525-16 (дата звернення: 18.04.2020).

9. European Information Policy (based on Fifth Edition) of the conference "Information society – a challenge for Europe" Council of Europe Committee of Ministers Committee on Information. Thessaloniki, Greece, 1997.

10. Resolution on "Europe and the global information society – Recommendations to the European Council" and on a communication from the Commission of the European Communities: "Europe's way to the information society: an action plan" (COM(94)0347 – C4-0093/94)

11. Corpuz M, Barnes P. Integrating information security policy management with corporate risk management for strategic alignment. In: Proceedings of the 14th World Multi-Conference on Systemic, Cybernetics and Informatics (WMSCI). Orlando, Florida, 2010.

12. Про інформацію : Закон України від 2 жовтня 1992 р. № 2657-XII URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 20.04.2020).

СУХАНОВ С. А.,
аспірант кафедри цивільного,
господарського та екологічного права
*(Національний технічний університет
«Дніпровська політехніка»)*

УДК 342.98
DOI https://doi.org/10.32842/2078-3736/2020.3.26

СТВОРЕННЯ ТА ЗАВДАННЯ ДЕРЖАВНОЇ СЛУЖБИ УКРАЇНИ З ПИТАНЬ ПРАЦІ

У статті досліджено створення та завдання Державної служби України з питань праці.

Історія становлення і розвитку державної служби взагалі та державної служби з питань праці, що забезпечують реалізацію функцій держави, пов'язані з розвитком і становленням держави та її органів. Кожен етап історичного розвитку суспільства у різних країнах характеризується особливими підходами до соціуму та конкретно осіб, котрі реалізують державні управлінські функції.

Але ознайомлення із процесом еволюції державної служби в ракурсі історичних етапів має свої особливості з урахуванням національної своєрідно-