DOI: 10.33766/2524-0323.88.67-80
УДК 340; 342; 324

В. В. Шемчук,
кандидат юридичних наук,
Заслужений юрист України,
доцент кафедри конституційного та міжнародного
права Таврійського національного
університету імені В. І. Вернадського
(м. Київ, Україна)
e-mail: vvshem.chuk@gmail.com
https://orcid.org/0000-0001-7969-6589

АЗІАТСЬКА МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУЧАСНИХ ДЕРЖАВ

У статті досліджується досвід забезпечення інформаційної безпеки деяких зарубіжних держав. На прикладі вивчення законодавства і практики його реалізації в даній сфері охарактеризовано азіатську модель забезпечення інформаційної безпеки. Аналіз конституцій і спеціальних законів Китайської Народної Республіки, Російської Федерації дозволив виокремити їх особливості, порівняно з американською та європейською моделями забезпечення інформаційної безпеки. На цій основі зроблено висновки щодо доцільності запозичення такого досвіду в Україні.

Ключові слова: інформаційна безпека, законодавство, кібербезпека, азіатська модель, кіберпростір.

Постановка проблеми. Останнім часом активізувалась діяльність державних і недержавних суб'єктів у сфері інформаційної безпеки. Ідеться як про мирний час, так і період збройних конфліктів. Спостерігається зростання кількості загроз територіальній цілісності України, її державному суверенітету, безпеці особи й держави. Відзначається іноді їх прихований характер, різноманітність засобів і методів ведення конфліктів тощо. Це зумовлює вивчення зарубіжного досвіду попередження й протидії таким загрозам, механізмів гарантування інформаційної безпеки. Виходячи з цього, вважаємо актуальним і необхідним вивчення досвіду інших країн забезпечення інформаційної безпеки, зокрема законодавчого регулювання та реалізації. Оскільки в попередніх статтях ми проаналізували європейську й американську моделі інформаційної безпеки [1], доцільно продовжити вивчення такого досвіду інших країн.

Сусідня держава – Російська Федерація – за допомогою технологій гібридної війни проти України перетворила інформаційну сферу на ключову арену протиборства. Використовуючи нові інформаційні технології впливу на свідомість громадян, певних органів місцевої влади, іноді розпалюється етнічна, релігійна ворожнечі, пропагується зміна конституційного ладу насильницьким шляхом, державного устрою України тощо. Наочним прикладом цьому є події на Сході України, де «наша держава стикнулася з особливим, «гібридним»

різновидом війни з боку Російської Федерації, коли головним полем бою стала свідомість людей, а найефективнішою зброєю – викривлена інформація» [2, с. 14].

Аналіз останніх досліджень і публікацій демонструє відсутність значної кількості наукових праць, присвячених вивченню зарубіжної практики інформаційної безпеки. Разом із тим, згадаємо наукові здобутки А. Пазюка, О. Бусол, О. Березі, О. Баранова, М. Желіховського, В. Картера, М. Карчевського, В. Ліпкана, О. Кирилюк, Н. Камінської, Я. Малика та інших.

Формування цілей. Мета статті полягає в дослідженні особливостей деяких азіатських держав у сфері забезпечення інформаційної безпеки (на прикладі Китайської Народної Республіки (КНР) і Російської Федерації (РФ), щоб запропонувати шляхи удосконалення механізмів забезпечення інформаційної безпеки України.

Виклад основного матеріалу. Китайська модель інформаційної безпеки заснована на тотальному контролі державою її інформаційного простору, що суперечить європейській практиці в цій сфері. У Конституції КНР 1982 р. (редакція 2018 р.) відсутнє поняття інформаційної безпеки та інформації, але декларується свобода слова, право на таємницю листування. Зокрема, за ст. 40 свобода і таємниця листування громадян КНР захищається законом. Жодна організація або приватна особа не може вчиняти замах на таємницю листування громадян, за винятком випадків, коли в інтересах державної безпеки чи кримінального розслідування, органам громадської безпеки або прокуратури дозволяється перегляд кореспонденції при дотриманні передбачених законом процедур [3].

Головним актом у сфері інформаційної безпеки КНР є Закон про кібербезпеку 2016 р. Це вершина законодавства про кібербезпеку, результат еволюції правил із різних рівнів. Закон містить основні норми з певних невідкладних питань, які мають довгострокове значення, як-от: 1) вимоги безпеки інтернет-провайдерів, продуктів і послуг; 2) правила захисту персональної інформації; 3) принцип суверенітету кіберпростору; 4) правила транснаціональної передачі даних у критично важливій інформаційній інфраструктурі; 5) систему безпеки ключової інформаційної інфраструктури. Сфера дії цього закону поширена на операторів мереж і підприємства в «критичних секторах». У Китаї до підприємств, що працюють у цих секторах, відносять вітчизняні мережеві підприємства, які займаються телекомунікаціями, транспортом, енергією, водними ресурсами, надають інформаційні, фінансові, громадські послуги і забезпечують електронні урядові сервіси. Це підприємства критично важливої інфраструктури, яка в разі її руйнування, втрати функції або витоку даних може серйозно поставити під загрозу національну безпеку, національний добробут, засоби до існування людей або громадські інтереси. Тому до операторів такої інфраструктури висуваються суворі вимоги щодо безпеки, закупівлі мережевих продуктів і послуг, зберігання даних і їх передачі. При цьому, якщо їм необхідно передати дані за кордон, слід спочатку пройти оцінку безпеки урядом Китаю.

Закон про кібербезпеку КНР визначає «мережевих операторів» як власників мереж, менеджерів і постачальників мережевих послуг. Підприємства

або установи, які надають послуги через мережі, також можуть бути визнані операторами мереж. Вони, з-поміж іншого, повинні таке: уточнити обов'язки своєї організації у сфері кібербезпеки , прийняти технічні заходи для забезпечення безпеки роботи мережі й запобігання витоків і крадіжки даних; повідомляти про будь-які інциденти кібербезпеки як користувачам мережі, так і відповідному відділу реалізації політики безпеки для цього сектора [4]. Згідно зі ст. 9 згаданого закону, оператори мереж повинні дотримуватися соціальних норм і комерційної етики, бути чесними, заслуговувати на довіру і виконувати зобов'язання щодо захисту мережевої безпеки, відповідати перед урядом і громадськістю [5-6]. Водночас ст. 41 Закону встановлено обов'язок мережевих операторів збирати й зберігати особисту інформацію відповідно до закону, адміністративних регламентів, їх угод з користувачами.

Таким чином, усі підприємства, які збирають і генерують персональні дані китайських громадян, згідно із законом, зобов'язані зберігати ці дані в межах Китаю. Такі законодавчі вимоги ускладнили роботу в КНР іноземних компаній, а також склалося декілька варіантів виконання вимог закону про кібербезпеку КНР в частині зберігання даних.

Послуги центрів обробки даних у Китаї швидко ростуть. Huawei, Tencent й Alibaba розширюють й інвестують у центри обробки даних як локально, так і за кордоном, кидаючи виклик таким компаніям, як Microsoft, Google і Amazon. Інші міжнародні компанії побудували свої власні дата-центри в Китаї або орендують центри для даних, де розміщують свої сервери, обладнання (колокейшн). Так компанія Apple передала свої китайські операції з iCloud південно-китайської компанії «Guizhou-Cloud Big Data». Згодом вони оголосили, що інвестують в будівництво в 2020 р. 2 нових центрів обробки даних у Китаї, щоб зберігати свої китайські дані iCloud згідно із Законом про кібербезпеку КНР. Останній передбачає вибіркові перевірки, сертифікацію та обов'язок співпраці з китайськими органами безпеки. Тобто на запит правоохоронних органів компанії зобов'язані надати вихідний код, шифрування, іншу важливу інформацію, що збільшує ризик її втрати, передачі конкуренти чи використання владою КНР. Закон про кібербезпеку КНР передбачає юридичну відповідальність за його невиконання. Так за порушення правил локалізації даних на території Китаю компанія може отримати штраф, буде призупинено її діяльність, відкликано ліцензію чи дозвіл на ведення бізнесу.

Державний контроль і цензура запроваджені і в китайському онлайн-просторі; це зумовлено у першу чергу тим, що в Китаї найбільша кількість інтернет-користувачів у світі (802 млн. користувачів і 42 % світових транзакцій електронної торгівлі надходять з цієї країни). Тому в КНР реалізується проект «Золотий щит» (The Golden Shield Project), який ще називають Великий китайський фаєрвол, програма фільтрації інтернет-контенту в КНР. Даний проект запущено 2003 р.; він охоплює такі напрями: управління трафіком; інформування про правопорушення; управління безпекою; інформаційна система моніторингу, контролю виходу і введення. «Золотий Щит» є одним з 12 ключових проектів КНР у сфері електронного уряду, іменованих «золотими», поряд із іншими: «Золота митниця» (іноземні торги), «Золоті мости» (загальноекономічна інформація), «Золоті фінанси» (управління фінансами),

«Золота картка» (електронні валюти), «Золота вода» (інформація про водні ресурси), «Золоте сільське господарство» (сільськогосподарська інформація) «Золота якість» (контроль якості), «Золоте оподаткування» (оподаткування) тощо. Так «Золотий Щит» передбачає обмеження доступу до іноземних сайтів; вебсторінки фільтруються за кодовими словами, пов'язаними з національною безпекою і чорним списком сайтів. Сайти, які розміщені в Китаї, повинні проходити реєстрацію в Міністерстві промисловості та інформаційних технологій. Крім того, у Китаї діють блогери, які за винагороду висловлюються про державну політику Китаю в чатах, блогах і на форумах.

Прикметно, що досвід КНР щодо інтернет-цензури вивчає та імплементує у своє законодавство РФ, що дозволяє віднести російську модель забезпечення інформаційної безпеки до азіатської. Підтвердженням цього є форум з кібербезпеки (2016), спільне комюніке про кіберпростір [7].

Отже, проаналізуємо особливості забезпечення інформаційної безпеки в РФ. Російська модель інформаційної безпеки заснована на засадах інформаційного суспільства, цифрової трансформації, захисту інформаційної інфраструктури, інтересів держави в інформаційному просторі. Правові засади цієї моделі закріплені в Конституції РФ, федеральному законодавстві, міжнародних актах. Контент-аналіз Конституції РФ свідчить про відсутність у її тексті поняття інформаційної безпеки, є лише термін «державна безпека». Положення про право на інформацію, заборону цензури мають засадниче значення для інформаційної безпеки особи. Так, відповідно до ст. 24 Конституції РФ, збір, зберігання, використання та поширення інформації про приватне життя особи без її згоди не допускаються [8]. Ст. 29 Конституції РФ гарантує свободу вираження поглядів, право на вільний доступ до інформації, свободу масової інформації.

Важливе місце посідає Федеральний Закон РФ «Про інформацію, інформаційні технології та про захист інформації» 2006 р., що визначає засади правового регулювання у трьох напрямах: реалізації права на інформацію, застосування інформаційних технологій та захисту інформації. У першому випадку вказаний закон визначає основні поняття в цій сфері, закріплює статус інформації як об'єкта правовідносин, встановлює критерії її класифікації, визначає суб'єктів інформації та їх компетенцію. Забороняється розповсюдження повідомлень і матеріалів іноземного ЗМІ, що виконує функції іноземного агента, визначеного Законом «Про засоби масової інформації» 1991р. (або) заснованого ним російської юридичної особи без вказівки на те, що ці повідомлення й матеріали створені й (або) поширені такими особами. Форма, вимоги до розміщення і порядок розміщення такої вказівки встановлюються уповноваженим центральним органом виконавчої влади [9]. Зазначений закон здебільшого переслідував обмеження діяльності іноземного мовлення США, яке наразі має розгалужену систему по усьому світу з охопленням великої глядацької аудиторії та доволі часто надає відмінну від національних засобів масової інформації точку зору [10].

Для організаторів поширення інформації в мережі «Інтернет» встановлено додаткові обов'язки зі зберігання інформації на території РФ, за їх невиконання передбачена адміністративна відповідальність (штраф від 3 тис. до 5 тис. руб.;

для посадових осіб від 30 до 50 неоподатковуваних мінімумів доходів громадян; юридичних осіб – від 8 тис. до 1 млн. рублів).

Наприклад, конфлікт державних органів з великими ІТ-компаніями зумовив обов'язок організаторів поширення інформації в Інтернеті надавати Федеральній службі безпеки РФ інформацію, необхідну для декодування електронних повідомлень їх користувачів. Так 2018 р., після відмови соціальної мережі «Телеграм» надати ключі шифрування органам державної безпеки, Роскомнагляд вирішив заблокувати інтернет-адреси, через які обслуговувалася соціальна мережа. Виконати вимоги влади було технічно неможливо, а інтернет-адреси часто збігалися з тими, які обслуговували інші інтернет-сервіси. У результаті дій Роскомнагляду було заблоковано 20 млн. інтернет-адрес, включаючи ті, що обслуговували сервіси Amazon, Google та ін. [11, с. 81].

Внаслідок запиту польського користувача російської мережі «ВКонтакте» про власні персональні дані, на який соціальна мережа була змушена відповісти, враховуючи, що в іншому випадку була б піддана великому штрафу через прийнятий Регламент про захист даних, з'ясувалися колосальні обсяги інформації, якою вона володіє. Багато недавніх судових справ свідчить про те, що «ВКонтакте», а також ряд інших великих компаній передають інформацію в правоохоронні органи, нехтуючи судовою процедурою [12].

Закон про інформацію в частині регулювання використання інформаційних систем закріплює їх види (федеральна, регіональна, муніципальна тощо), встановлює порядок застосування інформаційних технологій з метою ідентифікації громадян РФ, запроваджує національну систему доменних імен та низку реєстрів інформації, регламентує обмеження доступу до різних видів інформації.

Щодо посилення державного контролю за використанням ІТ згадаємо новий Федеральний Закон «Про внесення змін до статті 4 Закону РФ № 425- ФЗ «Про захист прав споживачів» 2019 р. Згідно з ним, при продажі окремих видів технічно складних товарів з попередньо встановленими програмами для електронних обчислювальних машин (ЕОМ), споживачеві забезпечується можливість використовувати окремі види технічно складних товарів із попередньо встановленими російськими програмами для електронних обчислювальних машин. Перелік окремих видів зазначених технічно складних товарів, складання і перелік російських програм для ЕОМ, які повинні бути введені, і порядок їх попередньої установки визначаються Урядом РФ [13].

Недавно Асоціація торгових компаній і товаровиробників електропобутової та комп'ютерної техніки (РАТЕК), у яку входять, у т.ч. Apple, Dell, IBM, HP, Google, Samsung, Intel, «М-Відео», надіслала листа В. Путіну, щоб відхилити цей закон, бо вступ його в силу негативно відіб'ється на розвитку галузі, призведе до монополізації у сфері розробки російського програмного забезпечення [14].

Зазначений закон передбачає, що регулювання відносин у сфері захисту інформації здійснюється шляхом встановлення вимог про захист інформації, відповідальності за порушення законодавства РФ про інформацію, інформаційні технології і захист інформації. Володілець інформації, оператор

інформаційної системи у встановлених законодавством РФ випадках, зобов'язані забезпечити таке:

1) запобігання несанкціонованому доступу до інформації та (або) передачі її особам, які не мають права на доступ до інформації;

2) своєчасне виявлення фактів несанкціонованого доступу до інформації;

3) попередження можливості несприятливих наслідків порушення порядку доступу до інформації;

4) недопущення впливу на технічні засоби обробки інформації, у результаті якого порушується їх функціонування;

5) можливість негайного відновлення інформації, модифікованою чи знищеною через несанкціонований доступ до неї;

6) постійний контроль за забезпеченням рівня захищеності інформації;

7) знаходження на території РФ баз даних інформації, з використанням яких здійснюються збір, запис, систематизація, накопичення, зберігання, уточнення (оновлення, зміна), витяг персональних даних громадян РФ [15].

Крім розглянутих змін до Закону про інформацію, які були внесені «законом Ярової», він зазнав ще поправок: Федеральний закон №139-ФЗ від 2012 р. – доповнення «про захист дітей», яким запроваджено «Єдиний реєстр заборонених сайтів»; Федеральний закон №187-ФЗ від 2013 р. – передбачає можливість блокування сайтів, що містять неліцензійний контент (на вимогу правовласника); Федеральний закон №398-ФЗ від 2013 р. – положення, пов'язані з блокуванням екстремістських сайтів; Федеральний закон №97-ФЗ від 2014 р. – «закон про блогерів», який зобов'язує власників популярних сайтів і блогів реєструватися в Роскомнагляді. Федеральний закон № 90-ФЗ від 2019 р. – закон про «суверенний Інтернет», мета якого збільшення стійкості Рунета.

У законодавстві РФ та дослідженнях інформаційна безпека розглядається як складова національної безпеки держави. Зокрема, у Концепції національної безпеки РФ (втратив чинність), внаслідок посилення засобів інформаційного ураження, до сфер, де національні інтереси становлять предмет національної безпеки, належать такі: економічна, соціальна, внутрішньополітична, інформаційна, міжнародна, військова, оборонна та екологічна. Національні інтереси Росії в інформаційній сфері полягають у дотриманні конституційних прав і свобод громадян у сфері отримання інформації і користування нею, розвитку сучасних телекомунікаційних технологій, захисті державних інформаційних ресурсів від несанкціонованого доступу.

У Концепції національної безпеки РФ зазначалося про посилення загроз національній безпеці РФ в інформаційній сфері, зокрема, серйозну небезпеку становлять собою прагнення ряду країн до домінування у світовому інформаційному просторі, витіснення Росії із зовнішнього і внутрішнього інформаційного ринку; розробка низкою держав концепції інформаційних війн, що передбачає створення засобів небезпечного впливу на інформаційні сфери інших країн світу; порушення нормального функціонування інформаційних та телекомунікаційних систем, а також збереження інформаційних ресурсів, отримання несанкціонованого доступу до них [15]. З огляду на визначені інтереси й загрози в інформаційному просторі РФ, у

Концепції національної безпеки РФ сформульовані такі завдання у сфері забезпечення інформаційної безпеки: захист та удосконалення інформаційної інфраструктури держави; створення умов для реалізації конституційних прав і свобод громадян у сфері інформаційної діяльності; інтеграції російської держави у світовий інформаційний простір; та протидія розв'язуванню інформаційних війн. Зміцнення інформаційної безпеки є важливим довгостроковим завданням, а її роль у системі національної безпеки країни визначається тим, що при їх взаємодії система інформаційної безпеки важлива сполучна ланка всіх компонентів державної політики в єдине ціле [16].

Проаналізовану Концепцію національної безпеки РФ замінено Стратегією національної безпеки РФ 2009 р.; на сьогодні діє її редакція 2015 р. У цьому базовому документі стратегічного планування наголошено на вчиненні інформаційного тиску на РФ з боку США, їх союзників; з'явилися нові види протиправної діяльності, пов'язаної з використанням ІКТ. Тому зазначено необхідність удосконалення системи виявлення й аналізу загроз в інформаційній сфері, протидії їм; вжиття заходів підвищення захищеності громадян і суспільства від деструктивного інформаційного впливу з боку екстремістських і терористичних організацій, іноземних спеціальних служб і пропагандистських структур; забезпечення розвитку інформаційної інфраструктури, доступності інформації про соціально-політичне, економічне і духовне життя, рівний доступ до державних послуг на території держави, у т.ч. з використанням інформаційних і комунікаційних технологій; розвитку гуманітарного та інформаційно-телекомунікаційного середовища на територіях держав СНД і суміжних регіонах; сприяння формуванню системи міжнародної інформаційної безпеки [17].

Звернемо увагу, що ідеологічні та стратегічні аспекти, «дорожні карти» реалізації російської моделі інформаційної безпеки відбиті в Доктрині інформаційної безпеки РФ 2016 р. і державних програмах. Зокрема у Доктрині інформаційна безпека РФ розуміється як стан захищеності особистості, суспільства і держави від внутрішніх і зовнішніх інформаційних загроз, при якому забезпечуються реалізація конституційних прав і свобод людини і громадянина, гідні якість і рівень життя громадян, суверенітет, територіальна цілісність і стійке соціально-економічний розвиток РФ, оборона і безпека держави. Водночас забезпечення інформаційної безпеки визначено як здійснення взаємопов'язаних правових, організаційних, оперативно-розшукових, розвідувальних, контррозвідувальних, науково-технічних, інформаційно-аналітичних, кадрових, економічних та інших заходів з прогнозування, виявлення, стримування, запобігання, відбиття інформаційних загроз і ліквідації наслідків їх прояву [19].

У Доктрині наводиться широкий аналіз сучасного стану інформаційної безпеки РФ та основних загроз для неї. Їх можна поділити та такі види: загрози конституційним правам і свободам людини і громадянина у сфері інформаційної діяльності та культурного життя, загрози індивідуальній, колективній та громадській свідомості; загрози ІТ мережам та засобам; загрози інформаційному забезпеченню політики держави; кіберзлочинність та терористична діяльність; загрози розвитку вітчизняної індустрії інформації. Значна увага приділяється загрозам інформаційному простору в аспекті військово-політичних та дестабілізуючих цілей. РФ обрала стратегію протидії

такому інформаційно-психологічному впливу через посилення державного регулювання інформаційного простору, обмеження права на інформацію та права конфіденційності в Інтернеті. Такий підхід є протилежним тому, що застосовується ЄС для боротьби з недостовірними новинами («фейками»).

Так із метою протидії російським «фальшивим новинам» в ЄС створена спеціальна робоча група з протидії російській дезінформації (EU vs Disinformation campaign). Не обмежуючи доступ європейських користувачів до інформації з російських джерел, на спеціальному сайті публікуються спростування фактів, які розміщуються в російському інформаційному просторі, особливо на іноземних мовах. Даний підхід відповідає практиці «мережевого нейтралітету» [19].

Інформаційна безпека в аспекті обороноздатності РФ характеризується збільшенням кількості та масштабів воєнно-політичних акцій із боку іноземних держав та організацій, посиленням розвідувальної діяльності іноземних держав та посиленням загроз для критично важливої інфраструктури держави.

У Доктрині, на підставі викладеного аналізу стану інформаційної безпеки, сформульовані кроки для поліпшення її забезпечення у наведених сферах. Такі заходи зводяться до таких напрямів: *протидія та запобігання* (використання ІТ з протиправною метою в політичній, економічній, соціальній та інших сферах); *підвищення захисту і безпеки* (суверенітету, інформації, критично важливої інфраструктури, інформаційних об'єктів, громадян та територій, єдиної мережі електрозв'язку РФ, функціонування зразків військового озброєння); *розвиток* (інновацій, науки й освіти, вітчизняної конкурентоздатності, кадрового потенціалу, культури особистої інформаційної безпеки, національної системи управління російським сегментом Інтернету тощо).

В умовах збройної агресії РФ проти України, велике значення в якій має й інформаційна війна, практичний інтерес становить стратегічні цілі РФ у сфері забезпечення інформаційної безпеки держави. Так, згідно військової політики РФ, основними напрямами забезпечення інформаційної безпеки в сфері оборони країни є: а) стратегічне стримування і запобігання військовим конфліктам через застосування інформаційних технологій; б) удосконалення системи забезпечення інформаційної безпеки Збройних Сил РФ, інших військ, військових формувань; в) прогнозування, виявлення та оцінка інформаційних загроз; г) сприяння забезпеченню захисту інтересів союзників РФ в інформаційній сфері; д) нейтралізація інформаційно-психологічного впливу [19].

Реалізація політики РФ у сфері інформаційної безпеки здійснюється й через розробку і виконання державних програм. Так розділ Державної програми РФ «Інформаційне суспільство (2011-2020 роки)», затвердженої розпорядженням Уряду РФ, присвячено забезпеченню інформаційної безпеки. Основними завданнями підпрограми «Безпека в інформаційному суспільстві» є таке: забезпечення контролю і нагляду, дозвільної та реєстраційної діяльності у сфері зв'язку, інформаційних технологій і масових комунікацій; забезпечення безпеки функціонування інформаційних і телекомунікаційних систем; розвиток технологій захисту інформації, що забезпечують недоторканність приватного життя, особистої і сімейної таємниці, безпеку інформації

обмеженого доступу; протидія поширенню ідеології тероризму, екстремізму, пропаганди насильства [19].

Організаційна складова інформаційної безпеки РФ характеризується розмежуванням повноважень гілок влади і визначенням компетенції федеральних органів влади, органів державної влади суб'єктів федерації. Склад системи забезпечення інформаційної безпеки РФ визначається Президентом РФ. Ідеться про Раду Федерації та Державну Думу Федеральних Зборів РФ (зокрема, Комітет Державної думи з безпеки), Раду Безпеки РФ, Уряд РФ (Міністерство цифрового розвитку, зв'язку і масових комунікацій РФ, МВС), Центральний банк РФ, Військово-промислова комісія РФ, органи судової влади, федеральні органи виконавчої влади (Федеральна служба нагляду у сфері зв'язку, інформаційних технологій і масових комунікацій – Роскомнагляд, Федеральна служба безпеки, Служба зовнішньої розвідки), міжвідомчі виконавчі органи суб'єктів федерації, місцеве самоврядування, компетенція яких включає забезпечення інформаційної безпеки. У той же час учасниками системи забезпечення інформаційної безпеки РФ є власники об'єктів критичної інформаційної інфраструктури і організації, які експлуатують такі об'єкти; ЗМІ; організації грошово-кредитної, валютної, банківської сфер фінансового ринку; оператори зв'язку, оператори інформаційних систем; організації, що здійснюють діяльність зі створення й експлуатації інформаційних систем і мереж зв'язку; розробки, виробництва і експлуатації засобів забезпечення інформаційної безпеки, з надання послуг у сфері забезпечення інформаційної безпеки; організації, що здійснюють освітню діяльність у цій галузі; громадські об'єднання; інші організації та громадяни, які за законодавством беруть участь у забезпеченні інформаційної безпеки [18].

Роскомнагляд є федеральним органом виконавчої влади, що здійснює функції контролю і нагляду у сфері ЗМІ, у т.ч. електронних, інформаційних технологій і зв'язку, функції з контролю і нагляду за відповідністю обробки персональних даних вимогам законодавства РФ, організації діяльності радіочастотної служби. Він наділений широкими повноваженнями, створює, формує та веде єдину автоматизовану інформаційну систему «Єдиний реєстр доменних імен, покажчиків сторінок сайтів у мережі «Інтернет» і мережевих адрес, котрі дозволяють ідентифікувати сайти в мережі «Інтернет», що містять інформацію, поширення якої в РФ заборонено. Для вжиття заходів з обмеження доступу до інформаційних ресурсів в інформаційно-телекомунікаційних мережах, у т.ч. Інтернеті, Роскомнагляд визначає порядок взаємодії оператора єдиного реєстру з провайдером хостингу і порядок отримання доступу до інформації в єдиному реєстрі, оператором зв'язку, що надає послуги з надання доступу до Інтернету [18]. Крім того, Роскомнагляд забезпечує роботу Універсального сервісу перевірки обмеження доступу до сайтів і (або) сторінок сайтів в Інтернеті та веде такі Реєстри: забороненої інформації; порушників авторських прав; організаторів поширення інформації; агрегаторів новин; інформації, що містить заклики до масових безладів; здійснення екстремістської діяльності; участі в несанкціонованих масових (публічних) заходах; недостовірну суспільно значущу інформацію, поширювану під виглядом достовірних повідомлень.

Отже, розглянута модель інформаційної безпеки РФ засновується на жорсткому державному регулюванні інформаційного простору та обмеженні доступу та свободи в онлайн-середовищі; також наявна тенденція ізолювання національного сегмента Інтернету. У вказаних аспектах ця модель набуває спільних ознак з китайськими державними проектами інформаційної безпеки, протилежна моделям забезпечення інформаційної безпеки західних країн.

Висновки. На відміну від європейської моделі забезпечення інформаційної безпеки, азіатська модель відзначається національними специфічними особливостями. Якщо американська система захисту кіберпростору є багатосторонньою моделлю управління Інтернетом – відкритого, функціонального, безпечного, інвестування передових технологій, розвитку кадрового потенціалу й економічної обґрунтованості забезпечення інформаційної безпеки, кібербезпеки і безпеки інфраструктури, – то китайська система інформаційної безпеки є прикладом негативної державної політики у сфері інформації. Вона заснована на державному контролі та цензурі. Тут за допомогою програми «Золотий щит» здійснюється маніпулювання громадською думкою, інтернет-цензура, контроль за ІТ- компаніями і користувачами. Закон про кібербезпеку КНР несе ризики для компаній, які працюють у сфері ІКТ в аспекті комерційного шпіонажу, кіберзлочинності та залежності від китайських спецслужб.

Забезпечення інформаційної безпеки РФ засновано на державному патерналізмі й консерватизмі, що посилює державний контроль за виробниками ІКТ, інформаційним простором країни, попри декларацію тріади інтересів держави, суспільства й особи. Головними суб'єктами реалізації інформаційної політики є Мінкомзв'язку і Роскомнагляд. Останній має широкі повноваження з блокування сайтів і акаунтів, порушення адміністративних справ проти ІТ-компаній та організаторів поширення інформації, відкликання ліцензій у ЗМІ, теле- та радіокомпаній, ведення реєстрів інформації тощо.

Загалом віднесення російської системи забезпечення інформаційної безпеки до азіатської моделі зумовлено запозиченням китайського досвіду й може вважатися негативним прикладом інформаційної державної політики. Постає витання: чи вартий запозичення такий досвід? На нашу думку, будь-яка модель забезпечення інформаційної безпеки має як переваги, так і недоліки. Проте для законодавства України є корисним вивчення таких нормативних й інституційних механізмів, водночас європейські цінності та стратегічні пріоритети у даній сфері більш близькі, демократичні, орієнтовані на інтереси людини.

Використані джерела:

1. Шемчук В. В. *Зарубіжний досвід забезпечення інформаційної безпеки* держави *Порівняльно-аналітичне право*. 2019. № 2. С. 34-40.

2. Нестерович В. Ф. Громадські протести на окремих територіях Українського Донбасу протягом весни 2014 року: причини та наслідки. *Віче*. 2014. № 21. С. 14-17.

3. Конституция КНР 1982 г. (редакция 2018 г.). URL: https://chinalaw.center/constitutional_law/china_constitution_revised_2018_russian/.

4. Lulu, Xia, and Zhao Leo. China's Cybersecurity Law: An Introduction for Foreign Businesspeople. China Briefing. 2018. URL: https://www.china-briefing.com.

5. Understanding China's Cybersecurity Law information for New Zealand businesse. Sep 2017.URL: https://www.mfat.govt.nz.

6. Cybersecurity Law of the People's Republic of China Passed November 6, 2016. URL: https://www.newamerica.org/cybersecurity- initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

7. Кремль объединил усилия с китайскими властями, чтобы усилить государственный контроль Интернета и его пользователей.УНИАН. 2016. URL: https://www.unian.net/world/1650792- soglashenie- o- kiberbezopasnosti- putin- ispolzuet-zolotoy-schit-v-rossii-the-guardian.html.

8. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993). Собрание законодательства РФ. 2014. № 31. Ст. 4398.

9. Об информации, информационных технологиях и о защите информации: Федеральній закон от 27.07.2006 № 149-ФЗ. Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

10. Нестерович В. Ф. Іноземне мовлення США у системі американської публічної дипломатії. *Віче*. 2016. № 7-8. С. 32-36.

11. Шариков П., Степанова Н. Подходы США, ЕС и России к проблеме информационной политики. *Современная Европа*, 2019. №2. С. 73-83.

12. Is Russian social media giant VKontakte sidestepping the GDPR? One user is trying to find out. Advox, 30.08.2018. URL: https://advox.globalvoices.org/2018/08/30/is-russian-social-media-giantvkontakte-sidestepping-the-gdpr-one-user-is-trying-to-find-out.

13. О внесении изменения в статью 4 Закона Российской Федерации «О защите прав потребителей»: Федеральный Закон от 02.12.2019 № 425-ФЗ. Российская газета 2019. № 275 (8033).

14. Бизнес попросил Путина отклонить закон о предустановке российского софта на гаджеты. Ведомости. 2019 URL: https://www.vedomosti.ru/technology/articles/2019/11/29/817525-biznes.

15. Об утверждении Концепции национальной безопасности Российской Федерации: Указ Президента РФ от 17.12.1997 №1300. URL: http://www.consultant.ru/ document/cons_doc_LAW_17186/defb41ab8ba4fdacc0715ce94f552abb03f39aaf/

16. Манойло, А. В. Государственная информационная политика в особых условиях. М.: МИФИ, 2003.

17. О Стратегии национальной безопасности РФ: Указ Президента РФ от 31.12.2015 № 653. URL: https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html.

18. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646. *Собрание законодательства РФ*. 2016. № 50. Ст. 7074.

19. EU vs Disinformation campaign. URL: https://euvsdisinfo.eu/about.

20. О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций: Положение, утвержд. Постановлением Правительства РФ от 16.03.2009 р. № 228. URL: https://rkn.gov.ru/about/p179.

21. Камінська Н. В. Міжнародна інформаційна безпека в умовах глобалізації та інтеграції. Міжнародне право: виклики сьогодення: матер. міжнар. конфер. (Київ, 20 грудня 2016 р.) Київ: КНТЕУ, 2016. С. 22-27.

References:

1. Shemchuk, V. V. (2019). Zarubizhniy dosvid zabezpechennya informatsiynoї bezpeki derzhavi. *Porivnyalno-analitichne pravo – Comparative analytical law, 2, 34-40.* [in Ukrainian].

2. Nesterovych, V. F. (2014) Hromads' ki protesty na okremykh terytoriyakh Ukrayins' koho Donbasu protyahom vesny 2014 roku: prychyny ta naslidky. *Viche – Viche 21, 14-17.* [in Ukrainian].

3. Konstitutsiya KNR ot 0.12.1982 g. (v redaktsii 2018 g.). URL: https://chinalaw.center/constitutional_law/china_constitution_revised_2018_russian/ [in Russian].

4. Lulu, Xia, and Zhao Leo. (2018). China's Cybersecurity Law: An Introduction for Foreign Businesspeople. China Briefing. URL: https://www.china-briefing.com.

5. Understanding China's Cybersecurity Law (2017). INFORMATION FOR NEW ZEALAND BUSINESSE. Ministry of Foreign Affairs and Trade, and New Zealand Trade and Enterprise. Sep URL: https://www.mfat.govt.nz. [in English].

6. Cybersecurity Law of the People's Republic of China Passed November (2016). URL: https://www.newamerica.org/cybersecurity initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. [in English].

7. Kreml obedinil usiliya s kitayskimi vlastyami, chtoby usilit gosudarstvennyy kontrol Interneta i ego polzovateley. (2016). UNIAN. URL: https://www.unian.net/world/1650792-soglashenie-o-kiberbezopasnosti-putin-ispolzuet-zolotoy-schit-v-rossii-the-guardian.html [in Russian].

8. Konstitutsiya Rossiyskoy Federatsii (prinyata vsenarodnym golosovaniem 12.12.1993). Sobranie zakonodatelstva RF. (2014). No 31, art. 4398. [in Russian]

9. Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii: Federalniy zakon ot 27.07.2006 № 149-FZ. Sobranie zakonodatelstva RF. (2006) Part 1. (No 31), art. 3448. [in Russian].

10. Nesterovych, V. F. (2016) Inozemne movlennya SSHA u systemi amerykans' koyi publichnoyi dyplomatiyi. *Viche – Viche, 7-8, 32-36.* [in Ukrainian].

11. Sharikov, P., Stepanova, N. (2019). Podkhody SShA, YeS i Rossii k probleme informatsionnoy politiki. *Sovremennaya Yevropa-Modern Europe, 2, 73-83.* [in Russian].

12. «Is Russian social media giant VKontakte sidestepping the GDPR? (2018). One user is trying to find out. Advox URL: https://advox.globalvoices.org/2018/08/30/is-russian-social-media-giantvkontakte-sidestepping-the-gdpr-one-user-is-trying-to-find-out. [in English].

13. O vnesenii izmeneniya v statyu 4 Zakona Rossiyskoy Federatsii «O zashchite prav potrebiteley»: Federalnyy Zakon ot 02.12.2019 № 425-FZ. (2019). *Rossiyskaya gazeta –Russian newspaper, 275(8033).* [in Russian].

14. Biznes poprosil Putina otklonit zakon o predustanovke rossiyskogo softa na gadzhety. (2019) URL: https://www.vedomosti.ru/technology/articles/2019/11/29/817525-biznes. [in Russian].

15. Ob utverzhdenii Kontseptsii natsionalnoy bezopasnosti Rossiyskoy Federatsii: Ukaz Prezidenta RF ot 17.12.1997 № 1300 (red. ot 10.01.2000). URL: http://www.consultant.ru/document/cons_doc_LAW_17186/defb41ab8ba4fdacc0715ce94f552abb03f39aaf/.[in Russian].

16. Manoylo, A.V. (2003) Gosudarstvennaya informatsionnaya politika v osobykh usloviyakh. Moskva: MIFI. [in Russian].

16. O Strategii natsionalnoy bezopasnosti RF: Ukaz Prezidenta RF ot 31.12.2015 № 653. URL: https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html. [in Russian].

17. Ob utverzhdenii Doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii: Ukaz Prezidenta RF ot 05.12.2016 № 646. (2016). *Sobranie zakonodatelstva RF-Collection of legislation of the Russian Federation,* 50, art. 7074. [in Russian].

18. «EU vs Disinformation campaign». N. d. N. p.URL: https://euvsdisinfo.eu/about. [in English].

19. O Federalnoy sluzhbe po nadzoru v sfere svyazi, informatsionnykh tekhnologiy i massovykh kommunikatsiy: Polozhenie, utverzhdennoe Postanovleniem Pravitelstva RF ot 16.03.2009 r. (No 228). URL: https://rkn.gov.ru/about/p179. [in Russian].

20. Kaminska, N. V. (2016). Mizhnarodna informatsiyna bezpeka v umovakh globalizatsiï ta integratsiï. Mizhnarodne pravo: vikliki sogodennya. *Mater. mizhnar. konfer. (Kiïv, 20 grudnya 2016 r.) -Mater. international. conference. (Kyiv, December 20, 2016)* Kyiv: KNTYeU, *22-27.* [in Ukrainian].

Стаття надійшла до редколегії 15.11.2019

Шемчук В. В.,
кандидат юридических наук,
Заслуженный юрист Украины,
доцент кафедры конституционного и международного права
Таврического национального университета
имени В. И. Вернадского
(г. Киев, Украина)

АЗИАТСКАЯ МОДЕЛЬ ОБЕСПЕЧЕНИЯ ИФНОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ ГОСУДАРСТВ

В статье раскрыто опыт обеспечения информационной безопасности некоторых зарубежных государств. На примере изучения законодательства и практики его реализации охарактеризовано азиатскую модель обеспечения информационной безопасности. Анализ конституций и законов Китайской Народной Республики и Российской Федерации позволил выделить их особенности по сравнению с американской и европейской моделями обеспечения информационной безопасности. Сделаны выводы относительно целесообразности заимствования такого опыта для Украины.

Ключевые слова: информационная безопасность, законодательство, кибербезопасность, азиатская модель, киберпространство.

Shemchuk V.,
Doctor of Law,
Honored Lawyer of Ukraine,
Associate Professor, Department of Constitutional
and International Law
V. I. Vernadsky Tavrida National University
(Kyiv, Ukraine)

ASIAN MODEL OF ENSURING THE INFORMATION SECURITY OF MODERN STATES

Unlike the European model of information security, based on the relevant EU legislation and national acts of the Member States, the Asian model is marked by more national specific features. If the American system of protection of cyberspace is based on the principle of

multilateral Internet governance model, open, functional, reliable and secure Internet, the principle of investing advanced technologies, the development of personnel Potential and economic validity of providing information security, cybersecurity and infrastructure security,

The Chinese information security model is an example of negative State policy in the field of information. It is based on state control and censorship. Here, using the program "Golden Shield" is carried out manipulation of public opinion, Internet censorship, control over IT companies and users. The Golden Shield program manipulates public opinion, internet censorship, controls over IT companies and users. China's cybersecurity law carries risks for ICT companies in terms of commercial espionage, cybercrime and dependency on Chinese intelligence services.

Ensuring information security of the Russian Federation is based on state paternalism and conservatism, which constantly strengthens state control over ICT producers, the information space of the country, despite the declaration of a triad of interests of the state, society and the individual in the information environment. The main subjects of information policy implementation are the Ministry of Communications and Roskomnadzor. The latter has broad powers to block websites and accounts, initiate administrative cases against IT companies and information dissemination organizers, revoke licenses in the media, television and radio companies, maintain information registers, and more.

In our opinion, any model of information security has both advantages and disadvantages. However, it is useful for the Ukrainian legislation to study the institutional framework analyzed, while at the same time European values and strategic priorities in this area are closer and more democratic, oriented towards the interests of the individual and the communities.

Key words: information security legislation**,** cybersecurity, cyberarea, asian model.