УДК 342.9

DOI: 10.26565/2075-1834-2020-30-13

ДОСВІД ДЕРЖАВНОГО РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗАРУБІЖНИХ ДЕРЖАВ (НА ПРИКЛАДІ СПОЛУЧЕНИХ ШТАТІВ АМЕРИКИ, КАНАДИ, НІМЕЧЧИНИ, ФРАНЦІЇ)

Яковлєв П. О.,
кандидат юридичних наук,
докторант Харківського національного
університету імені В. Н. Каразіна,
м. Харків, 61022, майдан Свободи 4,
e-mail: Yakovlevo@i.ua
orcid: https://orcid.org/0000-0003-0172-5946

АНОТАЦІЯ: *Вступ.* Статтю присвячено висвітленню досвіду державного регулювання забезпечення інформаційної безпеки у розвинених зарубіжних державах. На прикладі Сполучених Штатів Америки, Канади, Німеччини, Франції проаналізовано аспекти реформування законодавчого підґрунтя забезпечення інформаційної безпеки у сучасний період, визначено компетенцію основних суб'єктів державного управління, які забезпечують інформаційну безпеку, акцентовано увагу на дотримання інформаційних прав громадян у процесі адміністрування процесів забезпечення інформаційної безпеки.

Короткий зміст основних результатів дослідження. Виокремлено, що досвід державного регулювання у сфері забезпечення інформаційної безпеки Німеччини і Франції є показовим в аспектів доцільності впровадження положень Угоди про асоціацію між Україною і Європейським Союзом 2014 р. Так, документом визначено, що режим партнерства України і Європейського Союзу передбачає розвиток і трансформацію національної правової системи в амбітний і інноватівний спосіб на основі принципів верховенства права, доброго врядування, недискримінації осіб, які належать до меншин, поваги прав людини і основоположних свобод, прав національних меншин, різноманітності, цінування людської гідності, відданості принципам вільної ринкової економіки тощо. Відповідно, повноцінне дотримання зазначених засад передбачає проведення ґрунтовної роботи щодо адаптації національної системи адміністрування забезпечення інформаційної безпеки України у відповідності з кращими практиками США і держав Європейського Союзу.

Висновки. Зауважено, що виокремлення і характеристика найважливіших аспектів регулювання забезпечення інформаційної безпеки у зарубіжних державах дозволяє вирішити деякі важливі завдання науково-практичного характеру. Зокрема, перед вітчизняними фахівцями відкривається можливість створення і розширення практичних можливостей вирішення вітчизняними спеціалістами завдань щодо змістовного наповнення програмних документів з питань інформаційної безпеки, накопичення емпіричної бази, яку можна використовувати у процесі розробки і прийняття нових нормативних актів у сфері забезпечення інформаційної безпеки, запровадження нових для правової системи України інститутів забезпечення інформаційної безпеки; удосконалення існуючої законодавчої бази для функціонування елементів сектору безпеки і оборони у сфері забезпечення інформаційної безпеки. Успіх реалізації зазначених орієнтирів значною мірою залежить від рівня кваліфікації українських спеціалістів, а також від технічного, організаційного, управлінського забезпечення діяльності суб'єктів, які уповноважені забезпечувати інформаційну безпеку України.

КЛЮЧОВІ СЛОВА: Україна, державне регулювання, інформаційна безпека, інформаційний простір, Сполучені Штати Америки, Канада, Європейський Союз, Німеччина, Франція.

ОПЫТ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЗАРУБЕЖНЫХ ГОСУДАРСТВ (НА ПРИМЕРЕ СОЕДИНЕННЫХ ШТАТОВ АМЕРИКИ, КАНАДЫ, ГЕРМАНИИ, ФРАНЦИИ)

Яковлев П. А.,
кандидат юридических наук,
докторант Харьковского национального
университета имени В. Н. Каразина,
г. Харьков, 61022, площадь Свободы 4,
e-mail: Yakovlevo@i.ua
orcid: https://orcid.org/0000-0003-0172-5946

АННОТАЦИЯ: Статья посвящена освещению опыта государственного регулирования обеспечения информационной безопасности в развитых зарубежных государствах. На примере Соединенных Штатов Америки, Канады, Германии, Франции проанализированы аспекты реформирования законодательной почвы обеспечения информационной безопасности в современный период, определена компетенция основных субъектов

государственного управления, которые обеспечивают информационную безопасность, акцентировано внимание на соблюдение информационных прав граждан в процессе администрирования процессов обеспечения информационной безопасности.

Выделено, что опыт государственного регулирования в сфере обеспечения информационной безопасности Германии и Франции является показательным у аспектов целесообразности внедрения положений Соглашения об ассоциации между Украиной и Европейским Союзом в 2014 г. Так, документом определенно, что режим партнерства Украины и Европейского Союза предусматривает развитие и трансформацию национальной правовой системы в амбициозный и інноватівний способ на основе принципов верховенства права, эффективного управления, недискриминации лиц, которые принадлежат к меньшинствам, уважения прав человека и основополагающих свобод, прав национальных меньшинств, разнообразия, ценит человеческое достоинство, преданность принципам свободной рыночной экономики и тому подобное.

КЛЮЧЕВЫЕ СЛОВА: Украина, государственное регулирование, информационная безопасность, информационное пространство, Соединенные Штаты Америки, Канада, Європейський Союз, Германия, Франция.

EXPERIENCE OF GOVERNMENT CONTROL OF PROVIDING OF INFORMATIVE SAFETY OF THE FOREIGN STATES (ON EXAMPLE OF THE UNITED STATES OF AMERICA, CANADA, GERMANY, FRANCE)

Pavlo Yakovlev,
Candidate of legal sciences,
competitor of scientific degree
Kharkiv National University V. N. Karazin,
Kharkiv, 61022, Maidan Svobody 4,
e-mail: Yakovlevo@i.ua
orcid: https://orcid.org/0000-0003-0172-5946

ANNOTATION: *Introduction.* The Article is sanctified to illumination of experience of government control of providing of informative safety in the developed foreign states. On the example of the United States of America, Canada, Germany, France the aspects of reformation of legislative soil of providing of informative safety are analysed in a modern period, the competense of basic subjects of state administration, that provide informative safety, is certain, attention is accented on the observance of informative rights for citizens in the process of administration of processes of providing of informative safety.

Summary of the main research results. It is distinguished, that experience of government control in the field of providing of informative safety of Germany and France is model at the aspects of expediency of implementing provision of Agreement about an association between Ukraine and European Union in 2014 So, by a document certainly, that the mode of partnership of Ukraine and European Union envisages development and transformation of the national legal system in ambitious and innovative method on the basis of principles of supremacy of right, kind goverment, to undiscrimination of persons that belongs to minority, respect human rights and fundamental freedom, right for a national minority, variety, value human dignity, devotion principle free market economy and others like that. Accordingly, the valuable observance of the marked principles envisages realization of sound work in relation to adaptation of the national system of administration of providing of informative safety of Ukraine in accordance with the best practices of the USA and states of European Union.

Conclusions. It is marked that a selection and description of major aspects of adjusting of providing of informative safety in the foreign states allow to decide some important tasks of research and practice character. In particular, before home specialists possibility of creation and expansion of practical possibilities of decision of tasks home specialists is opened in relation to the rich in content filling of position papers on questions informative safety, accumulation of empiric base, that can be used in the process of development and acceptance of new normative acts in the field of providing of informative safety, input of new for the legal system of Ukraine institutes of providing of informative safety; improvement of existent legislative base for functioning of elements to the sector of safety and defensive in the field of providing of informative safety. Success of realization of the marked reference-points largely depends on the level of qualification of the Ukrainian specialists, and also from technical, organizational, administrative providing of activity of subjects, what authorized agents to provide informative safety of Ukraine.

KEY WORDS: Ukraine, government control, informative safety, informative space, United States of America, Canada, European Union, Germany, France.

Вступ. Для сучасної України питання забезпечення інформаційної безпеки набуло в останні роки особливо важливого значення. Це пов’язано як з багаточисельними посяганнями на національний інформаційний простір з боку інших держав і контрольованих ними суб’єктів, так і з активізацією євроінтеграційних процесів України і участю держави у міжнародних безпекових заходах і програмах за підтримки Сполучених Штатів Америки і інших держав.

Положення вступної частини Угоди про асоціацію між Україною і Європейським Союзом 2014 р. закріплює, що режим партнерства України і Європейського Союзу передбачає розвиток і трансформацію національної правової системи в амбітний і інноватівний спосіб на основі принципів верховенства права, доброго врядування, недискримінації осіб, які належать до меншин, поваги прав людини і основоположних свобод, прав національних меншин, різноманітності, цінування людської гідності, відданості принципам вільної ринкової економіки тощо [1]. Реформування сфери державного управління забезпечення інформаційної безпеки не є виключенням і передбачає проведення ґрунтовної роботи щодо

адаптації національної системи адміністрування забезпечення інформаційної безпеки у відповідності з кращими практиками США і держав Європейського Союзу. Відповідно, актуальним є науково-практичне завдання щодо узагальнення досвіду забезпечення інформаційної безпеки у розвинених державах світу і, зокрема, США, Канади, деяких країн, що входять до Європейського Союзу.

Теоретичною основою статті стали напрацювання таких науковців як Р. Асланов, О. Бусол, А. Гуніна, А. Гордієнко, Г. Пєвцов, А. Мануйлов, Я. Малик, О. Береза, В. Щенанківський, І. Чернухін та ін.

Основні результати дослідження. На сьогодні нормативні документи, які визначають концептуальні засади забезпечення національної безпеки й оборони і, зокрема, інформаційної безпеки (Доктрина інформаційної безпеки, Стратегічний оборонний бюлетень) передбачають, що налагодження співпраці із зарубіжними цивільними і мілітарними структурами, які підтримують обороноздатність і державну безпеку, є вагомими запоруками зміцнення основ національної безпеки, у тому числі і інформаційної [2-3]. Відповідно, вивчення зарубіжних моделей забезпечення інформаційної безпеки надасть вітчизняним спеціалістам додатковий імпульс у реформування і оптимізації національної моделі державного управління відповідною сферою.

Абсолютно логічним є наведення у першу чергу досвіду забезпечення інформаційної безпеки, який накопичено найбільш впливовою в політико-економічному і військовому відношенні державі – Сполучених Штатах Америки (США). В аспекті забезпечення інформаційної безпеки США можна вважати піонерами, адже це не лише держава, яка уперше у світі запровадила електронне урядування з використанням новітніх інформаційних технологій, а й створила особливу систему захисту національного інформаційного суверенітету і безпеки інформаційних ресурсів.

Переходячи безпосередньо до характеристики системи американської моделі адміністрування інформаційної безпеки, слід зауважити, що у США функціонує кілька інституцій забезпечення інформаційної безпеки: Агентство національної безпеки (АНБ), Національне управління кібербезпеки міністерства внутрішньої безпеки США, Федеральне бюро розслідувань (ФБР), Центральне розвідувальне управління (ЦРУ). Слід зазначити, що серед державних інституцій забезпечення інформаційної безпеки АНБ розвиває також партнерство з приватним сектором і науковими установами у вигляді планування заходів протидії загрозам у неурядових комп'ютерних мережах (таким чином держава бере участь у захисті найважливіших приватних телекомунікаційних, електричних, банківських мереж (телекомунікації, електромережі, мережі банківських розрахунків, інтернет-провайдери). АНБ залучає до проведення заходів з протидії тероризму приватні установи і громадські організації (CERT, ISACA, CSX, CCSIS). Експерти зауважують, що на сьогодні в США у забезпеченні інформаційної безпеки задіяно більш ніж 150 державних організацій і ще більша кількість приватних, які координуються АНБ [4, с. 105]. Разом із тим, найважливішою інституцією, яка здійснює державне регулювання інформаційною безпекою є Президент США.

Чинні сьогодні організаційно-правові засади захисту національного інформаційного простору беруть початок з інформаційного забезпечення політики безпеки та експлуатації оборонних систем та систем управління в інтересах вищих органів державної влади [5]. Основні законодавчі засади забезпечення інформаційної безпеки США було сформовано після другої світової війни, коли американська інформаційна система зіштовхнулася з деструктивним впливом радянської пропаганди. Структурно законодавство США у сфері забезпечення інформаційної безпеки складається як з федеральних законів, так і законів штатів. Незважаючи на існуючи істотні відмінності законів штатів, акти інформаційного законодавства є одними із найбільш уніфікованих, адже в американському суспільстві існує розуміння того, що інформаційна безпека держави є запорукою безпеки кожного громадянина. Правову основу адміністрування інформаційної безпеки США становлять закони «Про охорону особистих таємниць» (1974 р.), «Про таємницю» (1974 р.), «Про висвітлення діяльності уряду», «Про право на фінансову таємницю» (1978 р.), «Про доступ до інформації про діяльність ЦРУ» (1984 р.), «Про безпеку комп'ютерних систем» (1987 р.), «Про комп'ютерне шахрайство та зловживання» (1986 р.). За ініціативи Президента США Р. Рейгана було розроблено та ухвалено Закон «Про свободу інформації», а забезпечення інформаційної безпеки стало пріоритетним завданням політики Державного департаменту. Пізніше, у 1987 р. прийнято Закон Mb HR-145 «Про забезпечення безпеки ЕОМ», норми якого лягли в основу майбутнього законодавства про кібернетичну безпеку. Цим законом уперше у правовій системі США регламентовано статус нового інституту – «інформації обмеженого доступу», під якою американські спеціалісти розуміють несекретну, але важливу з точки зору національної безпеки несекретну інформацію урядових відомств, а також інформаційні дані, що формуються і циркулюють або обробляються в інформаційно-телекомунікаційних системах корпорацій і приватних фірм, що працюють на замовлення уряду США. Окрім законів важливе значення для інформаційної безпеки США мають Директиви Президента США, який очолює Раду національної безпеки. Найважливішими серед них є: Директива PD/NSC-24 1977 р. «Політика в галузі захисту систем зв'язку» (у документі уперше зазначено про необхідність захисту важливої несекретної інформації для забезпечення національної безпеки), Директива SDD – 145 1984 р. «Національна політика США в галузі безпеки систем зв'язку в

автоматизованих інформаційних системах» (у документів на Агентство національної безпеки покладено функції щодо забезпечення захисту інформаційних ресурсів, здійснення контролю за безпекою циклів передання інформації каналами зв'язку, обчислювальних та інформаційно-телекомунікаційних систем, здійснення сертифікації технологій, систем і устаткування із захисту інформації в інформаційно-телекомунікаційних мережах, ліцензування діяльності в галузі захисту інформації.

У 1990-х роках на хвилі активізації і глобалізації інформаційних відносин було введено у дію федеральні закони «Про інформаційну безпеку», «Про удосконалення інформаційної безпеки» (1997 р.) [6]. Більш того, в останнє десятиліття XX ст. у сфері розробки нормативних основ забезпечення інформаційної безпеки ве більшу роль починають відігравати військові, адже інформаційні технології стають повноцінною складовою військових потенціалів не лише США, а й Росії, Китаю, Німеччини, Ізраілю та інших держав. У 1992 р. було введено у дію Директиву Міністерства оборони США TS «Інформаційна війна». У Директиві зазначалося про обов'язковість обліку інформаційних ресурсів у процесі функціонування систем військового управління в інтересах підвищення ефективності дії військових з'єднань в умовах протидії супротивника. Було визначено складові такого явища як «інформаційна війна»: психологічний вплив на супротивника, оперативна безпека, введення супротивника в оману, електронне втручання, інформаційна розвідка, виведення з ладу системи управління вірогідного супротивника, інформаційний захист власної системи управління під час бойових зіткнень. Фактично, введення цієї Директиви на юридичному рівні інформаційну безпеку прирівняло до військової безпеки. Більш того, основним концептом державного регулювання інформаційної безпеки США стало управління інформаційними ресурсами таким чином, щоб одночасно убезпечити від посягань власну систему інформаційної безпеки і вивезти з ладу систему інформаційної безпеки ймовірного супротивника, взяти під контроль його стратегічні комунікації [7]. Слід артикулювати на тому, що американська модель забезпечення інформаційної безпеки цілком допускає ведення інформаційних війн, що включає у себе планування і проведення активних інформаційно-психологічних операцій як інструменту зовнішньої політики. При цьому, як зазначають експерти використання подібних методів е призводить до виникнення прямої воєнної конфронтації з державами і в цілому мирні відносини з ними зберігаються [8, с. 239; 9, с. 25].

Починаючи з 2001 р., коли тодішній президент США Д. Буш під час виступу з промовою перед особовим складом ЦРУ вказав, що забезпечення інформаційної безпеки є головним пріоритетом у забезпеченні національної безпеки США, у державі починають вводитися у дію загальнофедеральні урядові програми захисту національного інформаційного середовища у комп'ютерних мережах. Метою таких програм є створення всебічно сприятливих умов для розвідувальних органів з метою добування й обробки інформації щодо загроз інформаційному потенціалу інститутів публічного управління з боку інших держав та осіб. Значна увага при цьому приділяється, поряд з негласними інформаційними діями, системному аналізу відкритих джерел і добуванню інформації із конфіденційних баз даних з використанням комп'ютерного устаткування. Це дало старт формування нормативно-правової бази протидії кіберзлочинності. Так, у 2003 р. було введено у дію Національну стратегію безпечного кіберпростору. Пізніше – Огляд політики кібербезпеки (2009 р.), Міжнародну стратегія для кіберпростору (2011 р.), Директива Президента США «Щодо Проекту стратегії покращення кібербезпеки критично важливих об'єктів інфраструктури (2013 р.), Проект стратегії покращення кібербезпеки критично важливих об'єктів інфраструктури (2014 р.), Закон про кібербезпеку та обмін інформацією (2015 р.), Національна стратегія безпеки (2015 р.), Стратегія кібербезпеки Департаменту оборони (2015 р.). Положення вказаних документів регулюють значний масив аспектів забезпечення безпеки електронних інформаційних мереж і ресурсів. Також зазначені акти визначають адміністративні форми взаємодії державних інституцій з питань протидії загрозам кібербезпеці. Крім цього, у період з 1997 по 2001 р. у США велася активна робота по формуванню загальнофедеральної системи електронної аутентифікації. У відповідності до Директиви FIPS 186-2 (2000 р.) було запроваджено стандартизацію електронного підпису.

Привертає увагу те, що 2009 р. у Конгресі було представлено проект закону США «Акт про кібербезпеку» (The Cybersecurity Act of 2009) [10]. У документі було закріплено повноваження Президента США обмежувати доступ до Інтернет у будь-якій місцевості США у випадку існування загроз національній безпеці. Це стало початком нової ери в історії державного регулювання інформаційної безпеки США: було визначено ключову роль глави держави в управлінні системою кібербезпеки з метою демонстрування американським платникам податків значний управлінський потенціал президента, яки виступає гарантією успіху розвитку інформаційної сфери і захисту інформаційних проектів загальнофедерального, регіонального та місцевого значення у сфері кібербезпеки.

За часів президентства Барака Обами цифрова інфраструктура США була оголошена «стратегічною національною цінністю», а захист цієї інфраструктури – національним пріоритетом [11]. В основу цієї тези американський лідер поклав напрацювання наукової доктрини. Мова йде про відому думку

американського дослідника аспектів забезпечення інформаційної безпеки Маршалла Макклюєна про те, що в наш час економічні зв'язки і відносини усе більше набирають форму обміну знаннями, а не обміну товарами [12, с. 220]. Відповідно, боротьба за гуманітарні ресурси, капітал, ринки збуту стають дуругорядними, тоді як головним зараз стає доступ до інформаційних ресурсів, знань, що призводить до того, що війни ведуться вже більше в інформаційному просторі та за допомогою інформаційних видів озброєнь. Президентом США було сформульовано перелік першочергових безпекових проблем в інформаційній сфері держави: необхідність постійного удосконалення і доопрацювання стратегії забезпечення безпеки інформаційних і комунікаційних мереж, розробка систем попередження та реагування на кібератаки, посилення партнерства держави і приватного сектору у питаннях забезпечення інформаційної безпеки, залучення інвестицій в інноваційні технології, роз'яснення широким верствам населення переваг необхідності протидії кіберзагрозам.

У 2010 р. Президент США підписав «Ініціативу зі всеосяжної національної кібербезпеки», яка органічно доповнила Військову доктрини США. Було покладено початок заснуванню універсальної федеральної мережі захищених каналів зв'язку, яка б об'єднувала усі центри оперативного реагування на кіберзагрози і хакерські атаки. Було також засновано спеціальні підрозділи кіберконтррозвідки в центральних державних установах США з метою виявлення посягань на державні інформаційні мережі і попередження терористичних атак. Також було розроблено систему управління ризиками для прогнозування ймовірних наслідків несанкціонованого втручання в інформаційні мережі державних установ. Запроваджено роботу програми спеціальної програмної платформи «Ейнштейн», яка призначена для виявлення втручань у державні інформаційні мережі. З квітня 2012 р. хакерська атака у США кваліфікується як збройна агресія і передбачає весь арсенал заходів реагування. Вражає той факт, що на сьогодні у США 25% коштів, що надходять на науково-дослідні і дослідно-конструкторські роботи, використовуються на розробку систем захисту інформації. Це дуже значні кошти і не кожна держава сучасного світу може це собі дозволити.

Як і сусідні США, Канада сьогодні також приділяє значну увагу регулюванню забезпеченню інформаційної безпеки і проводить системну комплексну політику щодо її реалізації. У Канаді держава є головним суб'єктом управління всіма інформаційними потоками в суспільстві та забезпечення інформаційної безпеки. У порівнянні з низкою інших держав участь громадянського суспільства у відповідних процесах є мінімальною, що обумовлено високим ступенем довіри громадян до держави. Уряд сьогодні досяг значних успіхів в оптимальному правовому регулюванні всіх інформаційних відносин і процесів.

На сьогодні політика регулювання інформаційної безпеки Канади визнається показовою багатьма державами та міжнародними організаціями у світі. Слід зазначити, що інформаційна безпека Канади є невід'ємною частиною побудови інформаційного суспільства в державі. Питання про інформаційну безпеку актуалізувалося в Канаді на початку 1990-х років, коли спостерігалося стрімке зростання комп'ютеризації та інформатизації суспільних і управлінських процесів. У 1993 р. Центр безпеки національного відомства безпеки зв'язку Канади розробив «Канадські критерії безпеки комп'ютерних систем», які передбачали розробку єдиної шкали критеріїв для можливості порівняння різних систем обробки інформації за ступенем безпеки, створення основи для розробки специфікацій безпечних комп'ютерних систем, розробку уніфікованого підходу і стандартних засобів для опису характеристик безпечних комп'ютерних систем [13]. Основним досягненням Канади в адмініструванні інформаційної безпеки держави є створення «Інформаційної магістралі» - стратегічного документа, затвердженого урядом, який передбачає адміністративно-правові і технічні заходи, спрямовані на забезпечення автентичності інформації, що міститься в інформаційних мережах, виробничій сфері, надання публічних і приватних послуг та ін. у 1994 р було засновано Консультативна Рада з інформаційної магістралі, яка на постійній основі розробляє та вносить пропозиції щодо удосконалення нормативної основи забезпечення інформаційної безпеки в державі. Основним об'єктом охорони системи забезпечення інформаційної безпеки Канади є електронної уряд, який відкриває для громадян широкі можливості щодо взаємодії з державою за допомогою доступного і рівного доступу до публічних послуг.

У 1997 році Канада прийняла федеральні закони про позитивний доступі в Інтернет і про збереження конфіденційності в Інтернеті. Норми цих актів стали найважливішою правовою основою для захисту користувачів мережі Інтернет, в тому числі - забезпечення конфіденційності інформації про них самих [14, с. 48]. У 2001 р в Канаді, на тлі збільшення числа зазіхань на інформаційні комп'ютерні мережі, було створено спеціальний підрозділ Міністерства оборони - Група інформаційних операцій Канадських збройних сил. Завданням нового відомства стала розробка канадської моделі інформаційного протиборства в досягненні цілей інформаційної безпеки. в 2005 р при Уряді Канади створений Центр по кіберінцидентам, який виконує координаційні функції в частині протидії кіберзлочинів. Правовий статус зазначеної інституції передбачає боротьбу з погрозами і нападами на критичну інфраструктуру з використанням інформаційних технологій, моніторинг та аналіз кіберзагроз для державної системи

охорони навколишнього середовища, надання технічних консультацій по IT-безпеки, сприяння підвищенню інформаційної грамотності населення.

У 2010 році було введено у дію Канадську стратегію кібербезпеки, яка регламентує захист урядових інформаційних систем, забезпечення безпеки канадських громадян як учасників онлайн-середовища, обмін інформацією між федеральними міністерствами і відомствами, угоди з міжнародними партнерами і захист приватного сектора інформації. На сьогодні Канада, як і інші сучасні держави, активно розвиває організаційно-правові і технічні складові забезпечення інформаційної безпеки.

Що стосується досвіду забезпечення інформаційної безпеки державами Європи то зауважимо, що перші нормативні акти, що мали на меті її забезпечення датуються ще XVIII сторіччям: 2 грудня 1766 року було видано Милостивий указ Його Величності, короля Швеції, про свободу письма й друку, яким визначено зокрема, що є відкритою інформацією, а що – таємною (в інтересах держави) [15]. Першою державою, досвід регулювання забезпечення інформаційної безпеки якої ми розкриємо є Федеративна Республіка Німеччина. Адміністративно-правовий порядок забезпечення інформаційної безпеки ФРН здійснюється за умов суворого дотримання інформаційної повноправності особи. З 1977 р. діє Закон ФРН «Про захист персональних даних», який визначає порядок використання персональних даних у федеральних органах влади, органах влади земель, ЗМІ, у приватному секторі, а також регламентує автоматизований порядок персональної інформації [16]. Цим законом визначено основи захисту персональних даних. У 1997 році у ФРН прийнято Закон «Про основи надання інформаційних та комунікаційних послуг», який встановлює адміністративно-правові засади захисту інформації у інформаційно-телекомунікаційних мережах загального користування. Згідно із Законом Німеччини «Про мультизасоби інформації», збирання, обробка та використання інформації дозволяється лише у випадках, коли воно дозволене законом або здійснюється за наявності згоди користувача обслуговування. Інформація може бути зібрана, оброблена або використана окремо для різних послуг, яких потребує один і той же користувач. Згода користувача не може бути умовою для надання послуг. Інформація за договором може бути зібрана, дороблена та використана у тому обсязі, який є необхідним для виконання договору.

Національним органом Німеччини, що організаційно забезпечує інформаційну безпеку на федеральному рівні є Федеральне управління з інформаційної безпеки зі штаб-квартирою у Бонні. Ця структура працює в тісній взаємодії з Федеральною розвідувальною службою. Її було створено у 2009 р. згідно із Законом ФРН «Про посилення безпеки інформаційних систем» (Bundesamt für Sicherheit in der Informationstechnik, BSI). Пізніше, у 2011 р. затверджено федеральну Стратегію забезпечення кібернетичної безпеки Німеччини. Стратегія є головним актом ФРН із адміністрування захисту від кібернетичних атак. У документі зазначено, що кібернетичний простір являє собою віртуальний простір інформаційних мереж, які з'єднані між собою єдиними глобальними мережами (передусім інтер-нет). Кіберпростір Німеччини є відкритим для приєднання інших мереж передачі даних [17, с. 29]. Згідно концепції задля налагодження оперативного співробітництва між усіма державними установами й поліпшення координації заходів із захисту інформації, було засновано Національний центр кіберзахисту (Nationales Cyber-Abwehrzentrum – NCAZ), який підпорядковується федеральному МВС. Також у відповідності до стратегії у ФРН має бути засноване ще одне відомство - Національна рада кібербезпеки. Його завдання полягає у розробленні пропозицій із вироблення стратегічних основ державної політики інформаційної безпеки і протидії кіберзагрозам.

Серед інших органів, які безпосередньо забезпечують інформаційну безпеку слід виокремити Федеральну розвідувальну службу. Зазначена інституція виконує завдання з попередження, припинення, ліквідації наслідків кібернетичних загроз. Також федеральне управління відповідає за безпеку комп'ютерних додатків, захист державної інформаційної критичної інфраструктури, безпеку Інтернету, криптографію, контрспостереження, сертифікацію продуктів для забезпечення безпеки і акредитацію випробувальних лабораторій безпеки [18]. Розвідувальна служба займається забезпеченням кібербезпеки державних інформаційних ресурсів. У структурі управління функціонує структура «BSI», яка спеціалізовано від імені держави пропонує свої послуги для приватних IT-виробників, а також комерційних користувачів з метою спільної координації зусиль з інформаційної безпеки. Згадана структура також консультує виробників, дистриб'юторів та користувачів інформаційних технологій, аналізує розвиток і тенденції в області інформаційних технологій.

У сусідній Німеччині Франції система державного регулювання забезпечення інформаційної безпеки є дещо схожою на німецьку. Фактично, захист інформаційної безпеки у Франції, здебільшого, звівся до забезпечення кібернетичної безпеки і безпеки даних Інтернет. В цілому, у правовій системі Франції сьогодні немає спеціальних правових актів, що регулюють роботу спеціалістів з різними видами інформації. Безпека державної таємниці гарантується кримінальним, а персональної інформації та комерційних таємниць - кримінальним, трудовим і цивільними кодексами.

В основі управлінської французької національної моделі інформаційної безпеки – готовність до ведення інформаційної війни як у цивільній площині, так і по лінії військового відомства. Військова

складова передбачає обмежену роль інформаційних операцій, оскільки інформаційна війна розглядається, головним чином, у контексті конфліктів малої інтенсивності або у миротворчих операціях [19, с. 15]. В свою чергу, цивільний компонент передбачає більш широкий діапазон застосування спеціальних адміністративних інформаційних заходів, спрямованих на недопущення втручання у бази даних державних установ, підприємств, організацій, недопущення розголошення персональних даних та ін. Особливе місце у політиці інформаційної безпеки Франції посідає протидія інформаційним загрозам у сфері економіки. Точка зору французьких експертів відрізняється більш широким і більш глибоким вивченням конфліктів в економічній сфері. Їх підхід допускає, що союзник може одночасно бути об'єктом інформаційної війни.

З інституційної точки зору, протидія загрозам інформаційному середовищу у Франції традиційно здійснюється на місцях поліцейськими управліннями. При кожному регіональному французькому поліцейському управлінні існує спеціальний відділ по боротьбі зі злочинами у сфері інформаційних технологій [20]. «Яскравою» особливістю такого підходу є те, що інформаційною безпекою займаються не лише вузькопідготовлені спеціалісти, а й фінансисти, юристи, аудитори та ін. Причиною цього є розвиток електронної комерції у Республіці. Незважаючи на значні фінансові витрати на це, такий підхід дає позитивні результати: на сьогодні у Франції практично не вчиняються шахрайські дії з банківськими картками. Окрім цього, нещодавно у Франції було створено Центр електроніки і озброєнь (CELAR). Це орган, який займається широким спектром питань, в тому числі: проблемами електронної війни, інформаційних систем, телекомунікацій, інформаційної безпеки та електронних компонентів.

Висновки. В цілому, виокремлення і характеристика найважливіших аспектів регулювання забезпечення інформаційної безпеки у зарубіжних державах дозволяє вирішити деякі важливі завдання науково-практичного характеру. Зокрема, перед вітчизняними фахівцями відкривається можливість створення і розширення практичних можливостей вирішення вітчизняними спеціалістами завдань щодо змістовного наповнення програмних документів з питань інформаційної безпеки, накопичення емпіричної бази, яку можна використовувати у процесі розробки і прийняття нових нормативних актів у сфері забезпечення інформаційної безпеки, запровадження нових для правової системи України інститутів забезпечення інформаційної безпеки; удосконалення існуючої законодавчої бази для функціонування елементів сектору безпеки і оборони у сфері забезпечення інформаційної безпеки.

ЛІТЕРАТУРА

1. Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Закон України від 16.09. 2014 р. № 1678-VII. *Відомості Верховної Ради України*. 2014 р. № 40, Ст. 2021
2. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лютого 2017 року № 47/217. *Офіційний вісник Президента України*. 2017. № 5. стор. 15
3. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року «Про Стратегічний оборонний бюлетень України»: Указ Президента України від 06.06.2016 р. № 240/216. URL: https://www.president.gov.ua/documents/2402016-20137/ (дата звернення: 18.07.2018)
4. Бухарин В. В. Сравнительный анализ нормативной базы по обеспечению информационной безопасности в США и Российской Федерации (конец XX – начало XXI В.). *Вестник ИрГТУ*. 2016. № 12. С. 101 – 108
5. Політика гарантування інформаційної безпеки в Україні. Інтернет-сайт *«Проблеми інформаціної безпеки України».* URL: https://sites.google.com/site/bezpekiukraien223/politika-garantuvanna-informacijnoie-bezpeki-v-ukraieni (дата звернення: 11.05.2020)
6. Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України. *Інтернет-сайт Центру досліджень соціальних комунікацій НБУВ* URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350 (дата звернення: 27.05.2020)
7. The Administration's Priorities on Cybersecurity. White House. URL: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity#section-protect-critical-infrastructure (дата звернення: 04.03.2019)
8. Мануйло А. В. Государственная ифнормационная политика в особенных условиях : *монография*. Москва. ФИФИ. 2003. С. 293
9. Малик Я., Береза О. Забезпечення інформаційної безпеки України у контексті світового досвіду. Ефективність державного управління. 2012. № 32. С. 20 – 27
10. Cyber Security Strategy Documents. URL: https://ccdcoe.org/strategies-policies.html (дата звернення: 04.03.2019)
11. International Strategy for Cyberspace. *White House.* URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (дата звернення: 06.03.2019)
12. Щепанківський В. Г. Інформаційна безпека як складова образу країни. *Актуальні проблеми міжнародних відносин*. 2011. Вип. 102. Ч. 1. С. 219 – 228
13. Гунина А. А. Политика Канады в сфере обеспечения информационной безопасности. Интернет-сайт VI Международной студенческой научной конференции «Студенческий научный форум – 2014». URL: https://scienceforum.ru/2014/article/2014005707 (дата звернення: 05.03.2019)

14. Асланов Р. М. Зарубежный опыт правового регулирования обеспечения информационной безопасности. *Политика и общество*. 2012. №2 (86). С. 45 – 48

15. Історія доступу по-шведськи: королівський указ про свободу друку 1766 року. URL: https://dostup.pravda.com.ua/stories/publications/istoriia-dostupupo- shvedsky-korolivskyi-ukaz-pro-svobodu-druku-1766-roku (дата звернення: 04.11.2017)

16. Bundesdatenschutzgesetz (BDSG) vom 20.12.1990. *Офіційний сайт законодавства ФРН.* URL: http://www.gesetze-im-internet.de. (дата звернення: 04.11.2017)

17. Чернухін І. О. Досвід Федеративної Республіки Німеччини в побудові системи захисту інфраструктури від кібернетичних загроз. Інформаційна безпека людини, суспільства, держави. 2014. № 1. С. 28 – 43

18. Шохрух Рахмат. Органы обеспечения информационной безопасности: зарубежный опыт. Интернет-сайт «ictnews». URL: https://ictnews.uz/27/02/2018/infosec-agencies/ (дата звернення: 14.08.2019)

19. Пєвцов Г. В., Гордієнко А. М., Залкін С. В., Сідченко С. О., Хударковський К. І. Досвід і концепції веденян інформаційної боротьби у провідних країнах світу. *Наука і техніка Повітряних Сил Збройних Сил України*, 2015. № 1(18). С. 12 – 16

20. Национальная программа информационной безопасности Великобритании. *Інтернет-платформа «Tadviser».* URL: https://www.tadviser.ru/index.php/Статья:Национальная_программа_информационной_безопасности_Великобритании (дата звернення: 14.05.2020)

REFERENCES

1. Pro ratifIkatsIyu Ugodi pro asotsIatsIyu mIzh UkraYinoyu, z odnIEYi storoni, ta Evropeyskim Soyuzom, Evropeyskim spIvtovaristvom z atomnoYi energIYi I YihnImi derzhavami-chlenami, z InshoYi storoni: Zakon UkraYini vId 16.09. 2014 r. # 1678-VII. VIdomostI VerhovnoYi Radi UkraYini. 2014 r. # 40, St. 2021

2. Pro rIshennya Radi natsIonalnoYi bezpeki I oboroni UkraYini vId 29 grudnya 2016 roku «Pro Doktrinu InformatsIynoYi bezpeki UkraYini» : Ukaz Prezidenta UkraYini vId 25 lyutogo 2017 roku # 47/217. OfItsIyniy vIsnik Prezidenta UkraYini. 2017. # 5. stor. 15

3. Pro rIshennya Radi natsIonalnoYi bezpeki I oboroni UkraYini vId 20 travnya 2016 roku «Pro StrategIchniy oboronniy byuleten UkraYini»: Ukaz Prezidenta UkraYini vId 06.06.2016 r. # 240/216. URL: https://www.president.gov.ua/documents/2402016-20137/ (data zvernennya: 18.07.2018)

4. Buharin V. V. Sravnitelnyiy analiz normativnoy bazyi po obespecheniyu informatsionnoy bezopasnosti v SShA i Rossiyskoy Federatsii (konets HH – nachalo HHI V.). Vestnik IrGTU. 2016. # 12. S. 101 – 108.

5. PolItika garantuvannya InformatsIynoYi bezpeki v UkraYinI. Internet-sayt «Problemi InformatsInoYi bezpeki UkraYini». URL: https://sites.google.com/site/bezpekiukraien223/politika-garantuvanna-informacijnoie-bezpeki-v-ukraieni (data zvernennya: 11.05.2020).

6. Busol O. InformatsIyna bezpeka SShA: zakonodavche regulyuvannya ta perspektivi spIvpratsI dlya UkraYini. Internet-sayt Tsentru doslIdzhen sotsIalnih komunIkatsIy NBUV URL: . http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350 (data zvernennya: 27.05.2020).

7. The Administration's Priorities on Cybersecurity. White House. URL: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity#section-protect-critical-infrastructure (data zvernennya: 04.03.2019)

8. Manuylo A. V. Gosudarstvennaya ifnormatsionnaya politika v osobennyih usloviyah : monografiya. Moskva. FIFI. 2003. S. 293.

9. Malik Ya., Bereza O. Zabezpechennya InformatsIynoYi bezpeki UkraYini u kontekstI svItovogo dosvIdu. EfektivnIst derzhavnogo upravlInnya. 2012. # 32. S. 20 – 27.

10. Cyber Security Strategy Documents. URL: https://ccdcoe.org/strategies-policies.html (data zvernennya: 04.03.2019)

11. International Strategy for Cyberspace. White House. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (data zvernennya: 06.03.2019).

12. SchepankIvskiy V. G. InformatsIyna bezpeka yak skladova obrazu kraYini. AktualnI problemi mIzhnarodnih vIdnosin. 2011. Vip. 102. Ch. 1. S. 219 – 228.

13. Gunina A. A. Politika Kanadyi v sfere obespecheniya informatsionnoy bezopasnosti. Internet-sayt VI Mezhdunarodnoy studencheskoy nauchnoy konferentsii «Studencheskiy nauchnyiy forum – 2014». URL: https://scienceforum.ru/2014/article/2014005707 (data zvernennya: 05.03.2019).

14. Aslanov R. M. Zarubezhnyiy opyit pravovogo regulirovaniya obespecheniya informatsionnoy bezopasnosti. Politika i obschestvo. 2012. #2 (86). S. 45 – 48.

15. IstorIya dostupu po-shvedski: korolIvskiy ukaz pro svobodu druku 1766 roku. URL: https://dostup.pravda.com.ua/stories/publications/istoriia-dostupupo- shvedsky-korolivskyi-ukaz-pro-svobodu-druku-1766-roku (data zvernennya: 04.11.2017).

16. Bundesdatenschutzgesetz (BDSG) vom 20.12.1990. OfItsIyniy sayt zakonodavstva FRN. URL: http://www.gesetze-im-internet.de. (data zvernennya: 04.11.2017).

17. ChernuhIn I. O. DosvId FederativnoYi RespublIki NImechchini v pobudovI sistemi zahistu Infrastrukturi vId kIbernetichnih zagroz. InformatsIyna bezpeka lyudini, suspIlstva, derzhavi. 2014. # 1. S. 28 – 43

18. Shohruh Rahmat. Organyi obespecheniya informatsionnoy bezopasnosti: zarubezhnyiy opyit. Internet-sayt «ictnews». URL: https://ictnews.uz/27/02/2018/infosec-agencies/ (data zvernennya: 14.08.2019).

19. PEvtsov G. V., GordIEnko A. M., ZalkIn S. V., SIdchenko S. O., Hudarkovskiy K. I. DosvId I kontseptsIYi vedenyan InformatsIynoYi borotbi u provIdnih kraYinah svItu. Nauka I tehnIka PovItryanih Sil Zbroynih Sil UkraYini, 2015. # 1(18). S. 12 – 16.

20. Natsionalnaya programma informatsionnoy bezopasnosti Velikobritanii. Internet-platforma «Tadviser». URL: https://www.tadviser.ru/index.php/Statya:Natsionalnaya_programma_informatsionnoy_bezopasnosti_Velikobritanii (data zvernennya: 14.05.2020).