УДК 342.4:327.7

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КРАЇНАХ ЦЕНТРАЛЬНОЇ ЄВРОПИ

INFORMATION SECURITY ENSURING IN THE COUNTRIES OF CENTRAL EUROPE

Ткачук Т.Ю.,
к.ю.н, доцент,
заступник завідувача кафедри організації захисту інформації
з обмеженим доступом
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

Стаття присвячена дослідженню політики й системи забезпечення інформаційної безпеки в країнах Центральної Європи. У ході дослідження визначаються пріоритети та проблеми забезпечення інформаційної безпеки у вказаних країнах. Також оцінюється значущість досвіду країн Центральної Європи у сфері забезпечення інформаційної безпеки для України.
Ключові слова: інформаційна політика, інформаційна безпека, безпека інформації, кібербезпека, Центральна Європа.

Статья посвящена исследованию политики и системы обеспечения информационной безопасности в странах Центральной Европы. В ходе исследования определяются приоритеты и проблемы обеспечения информационной безопасности в указанных странах. Также оценивается значимость опыта стран Центральной Европы в сфере обеспечения информационной безопасности для Украины.
Ключевые слова: информационная политика, информационная безопасность, безопасность информации, кибербезопасность, Центральная Европа.

The problems of ensuring the information security of a person, society, the state, protecting them from various types of threats, both external and internal, now occupy one of the prominent places in the priorities of state policy and national security strategies of the countries of Central Europe, which are primarily oriented in this issue on the EU and NATO standards. The corresponding this standards should become a guide for Ukraine on the way to the realization of its European integration directions.

For Ukraine, as a state that faced the problem of hybrid war and temporarily occupied territories, the experience of Central European countries in providing information security is useful. In particular, the experience of Croatia, which successfully defeated sepratism and reintegrated the self-proclaimed "republic" - Ukraine also needs to use advanced methods to counteract Russian information aggression. It would be right to use Germany's principle of "active defense" in ensuring information security, because the information security of the state is a constant process of activity of the competent authorities aimed at preventing, countering threats in the information sphere, as well as applying active measures of information influence and the set of conditions for such activities that are implemented and are able to be controlled for a long time.

Ukraine should join Central European countries in the development of the international information security system in order to counter the threats to strategic stability, such as cyberterrorism and cybercrime, and to promote equitable strategic partnership in the global information space.
Key words: information policy, information security, information security, cybersecurity, Central Europe.

Аналізуючи підходи до забезпечення інформаційної безпеки, прийняті в країнах Європи, слід дійти висновку, що на сьогодні не існує уніфікованої моделі побудови національної системи безпеки в цій сфері. Втім, потреба реалізації ефективних заходів із протидії сучасним загрозам інформаційній безпеці, передусім – кіберзагрозам, зумовлює потребу у вдосконаленні форм і методів захисту інформації, критичної інформаційної інфраструктури та інформаційно-психологічної безпеки громадян всіма без винятку європейськими країнами.

Обравши євроінтеграційний курс, Україна має орієнтуватися на стратегію розвитку країн-учасниць Європейського Союзу в інформаційній сфері [1, с. 18]. При цьому, з урахуванням геополітичного положення України, її провідним орієнтиром мають стати передусім країни Східної та Центральної Європи, особливо останні, адже саме вони є успішним прикладом втілення в життя оптимальної моделі інформаційного суспільства шляхом створення розвиненої інфраструктури інформаційних технологій, які характеризуються унікально високим рівнем доступу насе лення до них, випереджаючи за цими показниками інші країни світу [2, с. 35].

Аналіз, оцінка та використання позитивних здобутків європейських країн мають важливе значення при розбудові системи забезпечення інформаційної безпеки в Україні, оскільки, як зазначають В. Шатун та О. Гладун [3, с.179], події останніх років у нашій державі показали, наскільки влада є неготовою протистояти інформаційним війнам, оскільки питання інформаційної політики досі не вирішені на достатньому рівні.

Дослідження з питань інформаційної безпеки в зарубіжних країнах, у тому числі у країнах Центральної Європи, здійснювали К. Андерсон, Г. Діллон, Р. Дорф, Т. Ламбо, М. Лібікі, Дж. Нарел, М. Прайс, П. Сігел та інші науковці. Проблематику забезпечення інформаційної безпеки в країнах Європи досліджували у своїх роботах О. Климчук, В. Ліпкан, В. Панченко, В. Петров, Н. Ткачук, М. Чеховська, О. Чернухін тощо. Дослідженням інформаційної безпеки України в контексті світового досвіду займалися І. Беззуб, В. Глуховеря, Л. Задорожня, В. Кирик, О. Костенко, В. Ліпкан, А. Марущак, Е. Макаренко, В. Політанський, В. Роговець та інші науковці, однак питання забезпечення інформаційної безпеки в країнах Центральної Європи, в тому числі з точки зору євроінтеграційних спрямувань України, поки що недостатньо висвітлені в науковій літературі.

Метою статті є дослідження специфіки політики та систем забезпечення безпеки інформації в країнах Центральної Європи, а також оцінка значущості досвіду країн Центральної Європи у сфері забезпечення інформаційної безпеки для України в контексті її євроінтеграційних спрямувань.

Питання щодо умовних кордонів Центральної Європи наразі лишається дискусійним. Традиційно до країн Центральної Європи відносять Німеччину, Ліхтенштейн, Австрію, Швейцарію тощо, втім де-факто країнами Центральної Європи вважаються й учасники Вишеградської групи – Угорщина, Польща, Чехія та Словаччина [4], а також частина країн Балканського півострову. Зважаючи на те, що питання інформаційної безпеки в країнах позаблокового статусу доцільно буде розглянути окремо, в рамках цієї статті зосередимось на забезпеченні інформаційної безпеки в Німеччині, Польщі, Угорщині та Хорватії [5], котрі є репрезентативними для відповідного регіону.

Передусім зауважимо, що Федеративна Республіка Німеччина, Угорська Республіка, Республіка Польща та Рес-

публіка Хорватія є членами Північноатлантичного Альянсу (НАТО) та Європейського Союзу (ЄС). Відповідно, на них поширюються стандарти цих міжнародних організацій щодо інформаційної політики та забезпечення інформаційної безпеки. Це, зокрема, стандарти НАТО щодо захисту інформації, викладені в Документі СМ (2002)49 «Безпека в організації Північноатлантичного договору (НАТО)» [6], офіційна політика НАТО у сфері кіберзахисту [7-8], стратегічна концепція кібербезпеки, сформульована за результатами Лісабонського саміту [9] й уточнена за результатами Варшавського саміту [10] тощо.

Активну політику у сфері забезпечення інформаційної безпеки проводить не лише НАТО, але й ЄС, який сьогодні об'єднує високо розвинуті країни, що справляють відчутний вплив на міжнародні відносини, встановлюючи норми і стандарти поведінки держав у політичній, економічній, соціальній, інформаційній та інших сферах.

Ще в 1991 році країни Європи було розроблено «Європейські критерії безпеки інформаційних технологій» [11], якими, зокрема, визначені завдання забезпечення інформаційної безпеки: захист інформаційних ресурсів від несанкціонованого доступу з метою забезпечення конфіденційності; забезпечення цілісності інформаційних ресурсів шляхом їх захисту від несанкціонованої модифікації або знищення; забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні. У 1996 стандарти європейської інформаційної безпеки було втілено в «Єдиних критеріях безпеки інформаційних технологій» [12], згідно з якими для характеристики основних критеріїв інформаційної безпеки застосовується модель тріади CIA (CIA Triad), яка передбачає три основні характеристики інформаційної безпеки: конфіденційність, цілісність та доступність [13].

У 2001 році Європейською Комісією було представлено документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід», в якому окреслено сучасний підхід ЄС до проблеми інформаційної безпеки. У документі використовується термін «мережева та інформаційна безпека», який трактується як здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, які становлять загрозу доступності, автентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через ці мережі і системи [14]. Документ визначає основні напрями європейської політики інформаційної безпеки: підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами; створення європейської системи попередження та інформування про нові загрози; забезпечення технологічної підтримки; підтримка ринково орієнтованої стандартизації та сертифікації; правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності; зміцнення інформаційної безпеки на державному рівні шляхом впровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання країнами-членами електронних підписів під час надання державних он-лайн послуг тощо; розвиток міжнародного співробітництва з питань інформаційної безпеки.

У країнах ЄС значна увага приділяється також проблемі кібербезпеки як складової частини інформаційної безпеки. З 1999 року ЄС реалізує програми «Безпечніший Інтернет» (Safer Internet), у рамках яких здійснюються заходи, спрямовані не лише на боротьбу зі шкідливим контентом, але й з небезпечною поведінкою в мережі [15]. У 2007 році Європейською Комісією представлено документ «На шляху до загальної політики в сфері боротьби з кіберзлочинністю», в якому кіберзлочинність визначається як кримінальні дії, вчинені з використанням електронних комунікаційних мереж та інформаційних систем або проти таких мереж та систем, і включає: традиційні форми злочину (шахрайство та підробки в електронних комунікаційних мережах та інформаційних системах); публікацію незаконного контенту в електронних медіа; специфічні злочини в електронних мережах (атаки на інформаційні системи, хакерство тощо) [16]. У 2009 році було опубліковано Повідомлення Європейської Комісії під назвою «Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості», в якому визначено основні виклики/проблеми, які потребують негайного реагування з боку країн ЄС, а також окреслено основні заходи, необхідні для посилення безпеки та здатності європейської критичної інформаційної інфраструктури протистояти зовнішнім впливам [17]. Згідно із цим документом основними викликами безпеці інформаційних інфраструктур країн ЄС є некоординовані національні підходи до безпеки інформаційних інфраструктур, що знижує ефективність національних заходів; відсутність на європейському рівні партнерства між державним та приватним секторами; обмежені можливості щодо раннього попередження та реагування на безпекові інциденти, зумовлені нерівномірністю розвитку систем моніторингу і сповіщення про інциденти у країнах-членах, нерозвиненістю міждержавного співробітництва та обміну інформацією щодо цих проблем; відсутність міжнародного консенсусу щодо пріоритетів у реалізації політики захисту критичної інформаційної інфраструктури.

Основоположною тезою для країн-членів ЄС у сфері інформаційної відкритості органів державної влади є така: «загальновизнано, що демократична система може функціонувати найбільш ефективно лише у випадку, коли громадськість повністю поінформована» [18, с. 110]. Водночас у рекомендації Ради Європи № R(81)19 «Про доступ до інформації, яка знаходиться в роз порядженні державних органів» зазначено, що для забезпечення адекватної участі всіх у суспільному житті необхідно забезпечити, з урахуванням неминучих винятків й обмежень, доступ громадськості до інформації, що знаходиться в розпорядженні державних органів усіх рівнів [19]. Таким чином, європейські стандарти інформаційної діяльності органів державної влади передбачають їх максимальну інформаційну відкритість за винятком обмежень, пов'язаних із дотриманням конфіденційності інформації з обмеженим доступом. Передусім це стосується забезпечення безпеки персональних даних.

Зокрема, в резолюції Генеральної Асамблеї ООН «Право на приватність у цифрову епоху» від 18 грудня 2013 року підкреслено глобальну і відкриту природу Інтернету і швидкий розвиток у сфері інформаційних та комунікаційних технологій як рушійної сили для прискорення прогресу на шляху до розвитку в різних формах. У документі підтверджено, що «ті ж права, що люди мають в оффлайн-режимі, також повинні бути захищені онлайн, у тому числі право на приватність» [20]. Засади захисту персональних даних у правовій практиці країн ЄС зводяться до наступного: пріоритетним є право особи розпоряджатися своїми персональними даними, а їх використання без дозволу володільця тягне відповідальність згідно із законодавством; для будь-кого, хто здійснює користування персональними даними фізичних осіб з їх дозволу, встановлено відповідальність у разі умисного розголошення цих даних третім особам (крім випадків, коли на це надано дозвіл) [21, с. 5–6; 22, с.46].

Основним документом, що регулює право громадян країн ЄС на захист персональних даних, є директива 95/46/ЄС « Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних» [23]. У цьому документі одночасно декларується прагнення до вільного переміщення інформації між країнами-членами ЄС та надаються гарантії захисту основних прав громадян, до яких входить право на недоторканність особистих

даних і їх захист від третіх осіб. Директива зобов'язує кожну державу, що входить до ЄС, прийняти свій власний закон про захист приватних відомостей, сумісний з рекомендаціями OECD 1980 року. Серед цих рекомендацій варто відзначити «Принцип гарантованої безпеки N11» [24], який вимагає, щоб «персональні дані були захищені розумними засобами безпеки від таких загроз, як втрата або неавторизований доступ, руйнування, використання, модифікація або розголошення».

Нові правила захисту персональних даних (GDPR), обов'язкові для країн-членів ЄС, які схвалено 14 квітня 2016 року, набудуть чинності у 2018 році. Ці правила буде поширено не тільки на європейські компанії, але й на компанії з інших країн, які пропонують товари й послуги в ЄС. У відповідному документі переглянуті цивільні права користувачів, відповідальність за схоронність даних, а також уведені деякі обмеження переміщення даних між різними країнами. Також важливим нововведенням є введення більш суворого покарання за несвоєчасне повідомлення інформації про виток даних. Компаніям, що порушили положення нової директиви та не доповіли про факт витоку або злому протягом 72 годин із моменту виявлення інциденту, загрожує штраф до 4% річного доходу або до 20 млн. євро [25]. Крім того, відповідна Директива передбачає необхідність отримання згоди користувачів на обробку їх персональних даних, причому на обробку даних з різними цілями потрібні будуть окремі згоди. Згода повинна бути вільною, свідомою і конкретною, а також може бути відкликана в будь-який момент. Згода не буде вважатися вільною, якщо користувач змушений дати таку згода, щоб одержати доступ до сайту, програми або додатка. Виключенням є випадки, коли персональні дані користувача потрібні для виконання угоди. У випадках, коли персональні дані збираються й обробляються для маркетингових цілей, користувач повинен мати можливість не погоджуватися зі збором і обробкою його даних. Компанії, що працюють із персональними даними, також повинні будуть вести облік операцій із персональними даними (тип даних і цілі, для яких вони обробляються), мінімізувати використання персональних даних відповідно до принципу data protection by design, а також проводити внутрішній аудит [26].

Отже, слід констатувати, що країни Центральної Європи як учасники ЄС мають «у певному сенсі злагоджену систему захисту інформації» [27, с.129], але в той же час кожна країна має свої закони, положення, інструкції щодо врегулювання питань інформаційної безпеки.

Зокрема, для законодавства Німеччини характерна детальна розробка системи різних видів інформації з обмеженим доступом, чіткі формулювання їх визначень у федеральному законодавстві. Так, відповідно до Закону «Про перевірку безпеки» [28] секретною інформацією є факти, вироби та відомості незалежно від форми їх представлення, які в державних інтересах повинні зберігатися в таємниці та яким наданий державним органом чи за його дорученням ступінь секретності, котрий відповідає необхідному рівню захисту: «цілком таємно», «таємно», «конфіденційно» чи «для службового користування». У систему секретної інформації входить державна таємниця (відомості з грифом «цілком таємно» і «таємно») та відомча таємниця (відомості з грифом «конфіденційно» і «для службового користування»), охорона яких, на відміну від інших видів таємниць, що стосуються конфіденційної сфери приватних осіб, зумовлена інтересами зовнішньої безпеки держави. Зокрема, особливо важливою та такою, що підлягає особливому захисту, вважається конфіденційна інформація про етнічне походження, політичні погляди, релігійні і філософські переконання, членстві в об'єднаннях, здоров'я й статевого життя фізичних осіб.

У жовтні 1997 року в Німеччині був прийнятий Акт захисту інформації в телекомунікаціях (TDPA) [29]. Відповідно до його загальних принципів збирання, обробка та використання інформації дозволяється лише у випадках, коли це дозволено законом або здійснюється за згодою користувача. Інформація може бути лише зібрана, оброблена або використана окремо для різних послуг, яких потребує один і той самий користувач, причому згода користувача не є умовою для надання послуг.

При цьому з 2005 року в Німеччині діє так званий «Акт про свободу інформації», який регламентує питання доступу до інформації [30]. Нагляд за виконанням положень цього нормативних акту покладений на комісара із захисту інформації та персональних даних. Починаючи з 1990 року в країні також діє закон про доступ приватних осіб і дослідників до архівів «Штазі» – колишньої Служби безпеки Східної Німеччини [31].

Провідну роль у забезпеченні інформаційної безпеки Німеччини відіграє Федеральна служба інформаційної безпеки (BSI), адже Законом ФРН «Про посилення безпеки інформаційних систем» завдання щодо попередження й реагування на інциденти, викликані кібернетичними загрозами, управління й координація сил та засобів із захисту критичної інформаційної інфраструктури, зокрема, у взаємодії із приватним сектором, покладається саме на це відомство. BSI входить до Федерального міністерства внутрішніх справ, яке, серед інших функцій, забезпечує внутрішню безпеку і захист конституційного ладу Німеччини, здійснює боротьбу з тероризмом, екстремізмом, шпигунством і саботажем. Відповідно до Закону «Про Федеральне відомство безпеки інформаційних систем» BSI збирає та оцінює інформацію стосовно загроз кібербезпеці держави, виявляє нові типи кібератак, аналізує відповідні контрзаходи [32]. Також на BSI у взаємодії з НАТО і ЄС покладається виконання наступних функцій: оцінка ризику впровадження інформаційних технологій; розробка критеріїв, методів і іспитових засобів для оцінки ступеня захищеності національних комунікаційних систем; перевірка ступеня захищеності інформаційних систем і видача відповідних сертифікатів; видача дозволів на впровадження інформаційних систем у важливі державні об'єкти; здійснення спеціальних заходів безпеки інформаційного обміну в державних органах, поліції тощо; консультування представників промисловості з питань інформаційної безпеки. Крім того, відомство займається пропагандою необхідності забезпечення інформаційної безпеки [33].

З метою оптимізації оперативного співробітництва між усіма державними установами та поліпшення координації заходів із протидії кібератакам у ФРН на базі Федерального відомства безпеки інформаційних систем створено національний центр кіберзахисту (NCAZ), який безпосередньо взаємодіє з іншими суб'єктами кібербезпеки країни, в тому числі з приватним сектором, країнами-партнерами з ЄС, НАТО, а також міжнародними організаціями [34, с. 78].

Питаннями забезпечення інформаційної безпеки Німеччини в межах своєї компетенції також опікуються Федеральне бюро захисту конституції (BFV) [35] та Управління інформаційних операцій, створене в 2009 року в структурі бундесверу через масовані атаки на обчислювальні мережі державних структур ФРН у лютому 2009 року. Також наприкінці 2010 року в рамках реалізації концепції кіберзахисту в структурі командування бундесверу остаточно завершене формування підрозділу інформаційних і комп'ютерних мережних операцій, який з 5 квітня 2017 року функціонує як «Сили кібернетичного та інформаційного простору Німеччини». До завдань відповідного підрозділу входить, зокрема: розробка нових методів кібератак; проникнення в комп'ютерні мережі іноземних держав і організацій з метою отримання розвідувальних даних; проведення операцій деструктивного впливу на мережі й автоматизовані системи або блокування їх роботи [36].

Нарощування потенціалу для ведення кібервійн свідчить про перехід Німеччини до принципу «активної оборони», адже раніше основна увага приділялася тільки питанням забезпечення безпеки інформації. Виділення наступальної складової частини інформаційного протиборства в окрему структуру, за оцінками німецьких експертів, є адекватною відповіддю на існуючі загрози інформаційній безпеки, а також підкреслює прагнення Німеччини забезпечити відповідність можливостей бундесверу сучасним реаліям.

Національна інформаційна політика Республіки Польщі зорієнтована на побудову вільного відкритого суспільства, забезпечення прав людини, впровадження концепції вільного транскордонного обігу інформації, створення незалежних і плюралістичних мас-медіа. Її правовим підґрунтям є прийняті 90-х роках минулого століття «Закон про пошту і телекомунікації», «Закон про телебачення і радіомовлення», «Закон про державні відносини з римською католицькою церквою в Республіці Польща», в яких визначаються напрями інформаційної політики, встановлюються технологічні стандарти інформаційного зв'язку, форми залучення іноземних інвестицій (від 33%-49% зарубіжного капіталу), ліцензування інформаційної діяльності. Окремо визначаються права церкви на інформаційну діяльність, з огляду значного впливу клерикальної інформації на політичні пріоритети та моральність польського суспільства [37, p.61-67; 38, с. 114].

Ключову роль у забезпеченні кібернетичної безпеки Польщі відіграє Агентство внутрішньої безпеки (ABW). У 2013 році ABW розробило Стратегію кібербезпеки Польщі та ініціювало створення Центру криптології при Міністерстві національної оборони, на який покладено завдання із захисту інформації, кібероборони та проведення наступальних кібероперацій [39]. ABW також створило урядову команду реагування на комп'ютерні інциденти (CERT) [40], головним завданням якої є забезпечення і розвиток можливостей органів державного управління щодо захисту від кіберзагроз, зокрема від атак на інфраструктуру, що складається з IT-систем та комп'ютерних мереж, порушення роботи або руйнація яких може значною мірою загрожувати життю і здоров'ю людей, національним багатствам та навколишньому середовищу або призвести до значних фінансових збитків і збоїв у функціонуванні органів державної влади [34, с. 79]. Під керівництвом ABW у 2015 році було розроблено й Доктрину кібербезпеки Польщі, яка оперує ключовими поняттями теорії безпеки на кшталт «загроз», «викликів», «ризиків» тощо [41].

У зв'язку з ескалацією гібридних загроз інформаційного характеру, як наприклад, пропаганда, дезінформація чи психологічне залякування з боку інших країн і недержавних виконавців (терористичних та інших організацій) Бюро національної безпеки Польщі (BBN) у 2015 році розпочало роботу над польською Доктриною інформаційної безпеки. Серед загроз інформаційній безпеці в Доктрині названі, зокрема, ескалація напруження в міжнародних стосунках, дискредитація польської міжнародної політики і формування негативного іміджу Польщі на міжнародній арені, в тому й серед союзників в рамках НАТО чи ЄС, формування образу Польщі як країни ксенофобів та антисемітів, провокування польсько-литовського конфлікту на тлі польської меншини у Литві, а також провокування польсько-українського конфлікту на історичному тлі при можливому застосуванні терористичних замахів, які буцімто могли б здійснити українці проти поляків чи навпаки. Для боротьби з негативними тенденціями пропонується «розпізнавати інформаційне середовище, в тому числі визначати дружні, нейтральні і ворожі суб'єкти». Доктрина інформаційної безпеки Польщі розглядається як виконавчий документ до Стратегії національної безпеки [42].

До участі в забезпеченні інформаційної безпеки Польщі активно залучається громадянське суспільство. Зокрема, в поточному році було створено неурядову організацію – Центр аналізу пропаганди і дезінформації, яка займатиметься виявленням і протидією російській пропаганді. Вказана фундація є першою такого роду інституцією в Польщі, діяльність якої спрямовуватиметься на аналіз і пошук системного підходу до ідентифікації і протидії російській дезінформації в польському інформаційному просторі. Окрім науково-дослідної і аналітичної роботи, фундація співпрацюватиме з іншими суб'єктами, аби творити фундамент розуміння в польському суспільстві загроз, оскільки інформаційна і психологічна війна проникає в різні сфери функціонування суспільства і держави [44].

Якщо вести мову про захист інформації з обмеженим доступом, слід зауважити, що при вступі до НАТО Польща, так само, як Чехія і Словаччина, розробила нове законодавство щодо захисту класифікованої інформації на підставі нових принципів. Так, у січні 1999 року набув чинності Закон «Про захист конфіденційної інформації», прийняття якого було умовою вступу Польщі в НАТО. Закон поширюється на засекречену інформацію й дані, зібрані державними структурами, «розголошення яких може завдати шкоди державним або суспільним інтересам, або захищеним за законом інтересам громадян або організації» [37, с. 53].

На відміну від Польщі, Угорщина адаптувала до вимог НАТО раніше існуюче законодавство про захист державних та офіційних секретів. Зокрема, в 1995 році Угорщина прийняла закон про державні та офіційні секрети, який у 2001 році був доповнений і виправлений виходячи з практики Альянсу [45, с. 155]. У цілому ж угорська політика у сфері забезпечення інформаційної безпеки налаштована переважно на впровадження обмежень. Так, закон про засоби масової інформації, прийнятий у 2010 році, викликав критику з боку світових ЗМІ та ЄС – Угорщину звинуватили в запровадженні тотального контролю за ЗМІ, включно з Інтернетом, у ліквідації свободи слова й навіть у прагненні встановити тоталітарний режим. Європейський парламент прийняв резолюцію [46] (вперше стосовно країни – члена ЄС) із засудженням того, як угорський уряд ставиться до демократії, свободи слова, прав людини. Згодом парламент Угорщини прийняв косметичні поправки до закону, які не торкнулися ключових питань (структури управління угорськими ЗМІ), але були сприйняті ЄС позитивно [47, с.11].

Угорщина стала першою з постсоціалістичних країн, де був прийнятий правовий акт про захист персональних даних – «Закон про захист інформації про особу та доступ до інформації, що становить суспільний інтерес» 1992 року, який впровадив інститут Парламентського комісара із захисту інформації та свободи інформації [48]. Відповідно до цього Закону будь-яка інформація, обробку якої здійснюють органи, що виконують суспільні обов'язки, становить суспільний інтерес, за винятком інформації про особу. Проте доступ і поширення інформації про діяльність політичних діячів і державних посадових осіб не можуть обмежуватися на підставі захисту інформації про особу. Закон також покладає на органи державної влади обов'язок надавати громадськості точну і своєчасну інформацію та надає право угорським громадянами звертатися із запитами про надання доступу до інформації, що становить суспільний інтерес. При цьому персональні дані можуть збиратися і оброблятися тільки з відома самої особи або відповідно до вимог закону. Особа, чиї персональні дані обробляються, повинна бути повністю поінформована про мету такої обробки. Можуть збиратися лише ті дані, які необхідні для досягнення цієї мети, і зберігатися вони можуть лише протягом терміну, поки мета не буде досягнута. Кожному надається право діставати

доступ до своєї персональної інформації і за необхідності вимагати її виправлення або знищення. Особливий захист передбачений для «чутливих» (sensitive) даних, які визначаються як дані, що відносяться до «расового походження, національності й етнічного статусу, політичних думок або партійної приналежності, релігійного або інших переконань» або «відомостям про хвороби, сексуальне життя або судимості». Крім того, до правового підґрунтя забезпечення інформаційної безпеки в частині захисту персональних даних в Угорщині належать Закон «Про право на інформаційне самовизначення та свободу інформації» 2011 року та Закон «Про обробку і захист медичної інформації та пов'язаних з нею персональних даних» 1997 року. З будь-яких питань, пов'язаних із захистом персональних даних, особа може звернутися до Національного бюро із захисту даних та свободи інформації [49].

Питанням забезпечення інформаційної безпеки Угорщини, в т.ч. кібербезпеки, присвячений також Закон «Про електронну інформаційну безпеку державних та муніципальних органів» 2013 року [50] та п. 31 Стратегії національної безпеки Угорщини, затвердженої у 2012 році [51]. Стратегія національної безпеки, зокрема, передбачає, що Угорщина повинна бути готова управляти ризиками й загрозами, пов'язаними з національною безпекою, обороною, боротьбою проти злочинності, а також запобігати нештатним ситуаціям у кіберпросторі, а також гарантувати адекватний рівень кібербезпеки й виконувати інші завдання, пов'язані із забезпеченням кібербезпеки. При цьому основним завданням визначається систематичне визначення пріоритетів у сфері потенційних загроз і ризиків у кіберпросторі, а також підвищення поінформованості суспільства щодо них. Відповідні положення дістали свого подальшого розвитку у Національній стратегії кібербезпеки Угорщини, затвердженій у 2013 році [52].

У Хорватії з 2007 року діє Акт про інформаційну безпеку [53], що визначає поняття інформаційної безпеки, заходи й стандарти інформаційної безпеки, а також сфери інформаційної безпеки та компетентні органи для прийняття й реалізації рішень у сфері забезпечення інформаційної безпеки, а також нагляду за дотриманням стандартів інформаційної безпеки. Зокрема, інформаційна безпека визначена як стан конфіденційності, цілісності й доступності інформації, що досягається шляхом реалізації політики заходів і стандартів і організаційної підтримки робочих місць, планування, реалізації, оцінки й відновлення заходів і стандартів. Сферами інформаційної безпеки, на які поширюються відповідні заходи і стандарти, вважаються: безпека персоналу; фізичний захист інформації та інфраструктури; безпека інформації; промислова безпека; INFOSEC (сфера інформаційної безпеки, в рамках якої заходи і стандарти інформаційної безпеки визначаються для класифікованих і несекретних даних, які обробляються, зберігаються або передаються в межах інформаційної системи, а також захист цілісності й доступності інформаційної системи в процесі планування, проектування, створення, використання й припинення її роботи) тощо. Реалізація державної політики у сфері забезпечення інформаційної безпеки відповідно до цього законодавчого акта покладається на Управління Ради національної безпеки (NSA), Бюро з безпеки інформаційних систем (NCSA), а також національний орган із питань профілактики й захисту від комп'ютерних загроз системам суспільної інформації Республіки Хорватія (CERT).

Крім того, в 2015 році в Хорватії було прийнято національну стратегію кібербезпеки [54]. Стратегія кібербезпеки Хорватії базується на наступних принципах: всебічність підходу до кібербезпеки, що охоплює кіберпростір, інфраструктуру й користувачів відповідно до хорватської юрисдикції (громадянство, реєстрація, домен, адреса); інтеграція заходів у різних сферах забезпечення кібербезпеки; проактивність внаслідок постійного коректування заходів та періодичне корегування їх стратегічних кордонів; зміцнення стійкості, надійності й керованості шляхом застосування універсальних критеріїв конфіденційності, цілісності й доступності певних груп інформації й соціальних цінностей; захист прав і свобод людини у кіберпросторі, передусім – конфіденційності та власності; постійне вдосконалення правової бази; субсидіарність при розподілі повноважень; пропорційність витрат на забезпечення кібербезпеки та ступеню ризику тощо. Стратегія кіберзахисту являє собою частину стратегії оборони, що підпадає під відповідальність Міністерства оборони Хорватії. Кібертероризм, кіберзлочинність та деякі інші кібер-аспекти національної безпеки розглядаються також компетентними органами в системі безпеки й розвідки як такі, що вимагають спеціального підходу.

Слід зазначити, що забезпечення інформаційної безпеки, в тому числі й шляхом активних інформаційних операцій, наприкінці минулого століття стало важливим компонентом боротьби Хорватії за свої тимчасово окуповані території, на яких понад чотири роки існувала сепаратистська «Республіка Сербська країна». При цьому, за оцінками експертів, якщо в мілітарному значенні боротьба за повернення вказаних територій закінчилася у серпні 1995 року під час операції «Буря», в дипломатичному – на початку 1998-го, водночас із мирною реінтеграцією хорватського Подунав'я, то в інформаційному сенсі війна закінчилася лише через 15 років з дня закінчення бойових дій [55], і запорукою перемоги в цій інформаційній війні була постійна боротьба за «вуха, очі та розум» населення окупованих територій, а також протидія інформаційній агресії супротивника.

Проблеми забезпечення інформаційної безпеки особи, суспільства, держави, їх захисту від різного виду загроз, як зовнішніх, так і внутрішніх, наразі посідають одне з чільних місць у пріоритетах державної політики та стратегіях забезпечення національної безпеки країн Центральної Європи, які в цьому питанні орієнтуються передусім на стандарти ЄС та НАТО. Відповідні стандарти мають становити орієнтир і для України на шляху нашої держави до реалізації своїх євроінтеграційних спрямувань.

Для України, як держави, що зіштовхнулося із проблемою втягнення в гібридну війну та тимчасово окупованих територій, не зайвим буде досвід країн Центральної Європи в забезпеченні інформаційної безпеки, зокрема, Хорватії, протидія сепаратизму в якій закінчилась успішною реінтеграцією самопроголошеної «республіки». Тож наразі нам слід брати на озброєння передові методи протидії російської інформаційної агресії, треба постійно представляти якісний інформаційний продукт на тимчасово окупованих територіях. Доцільним буде також наслідувати досвід Німеччини в переході до принципу «активної оборони» в забезпеченні інформаційної безпеки, адже інформаційна безпека держави становить постійний процес діяльності компетентних органів, направлений на попередження, протидію загрозам в інформаційній сфері, а також застосування активних заходів інформаційного впливу та сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час.

Крім того, Україна має приєднатися до інших європейських країн у розбудові системи міжнародної інформаційної безпеки з метою протидії загрозам стратегічній стабільності, таким як кібертероризм та кіберзлочинність. Співробітництво з країнами Центральної Європи у сфері формування системи міжнародної інформаційної безпеки відповідає національним інтересам України і сприяє зміцненню її національної безпеки.

ЛІТЕРАТУРА

1. Політанський В.С. Інформаційне суспільство в Україні: від зародження до сьогодення / В.С. Політанський // Науковий вісник Ужгородського національного університету: серія «Право». – Випуск 42. – 2017. – С. 16.

2. Політанський В.С. Світові моделі та фундаментальні принципи інформаційного суспільства / В.С. Політанський // Науковий вісник Ужгородського національного університету: серія «Право». – Випуск 43, том 1. – 2017. – С. 34.

3. Шатун В., Гладун О. Інформаційна безпека – невід'ємна складова національної безпеки України / В. Шатун, О. Гладун // Наукові праці. Державне управління. – Випуск 255, Том 267. – 2016. – С. 174 –180.

4. The World Factbook: Central Intelligence Agency: [Online tool]. – Available at : https://www.cia.gov/library/publications/the-world-factbook/fields/2144.html.

5. Республика Хорватия // Гуманитарные технологии: Аналитический портал [Електронний ресурс]. – Режим доступу : http://gtmarket.ru/ countries/croatia/ croatia-info.

6. Document C-V(2002)49: Security within tne North Atlantic Treaty Organization (NATO): [Online tool]. – Available at : www.statewatch.org/ news/2006/sep/nato-sec-classifications.pdf.

7. NATO Bucharest Summit Declaration, 3 April 2008: [Online tool]. – Available at : http://www.nato.int/docu/pr/2008/p08-049e.html.

8. North Atlantic Treaty Organization. Active Engagement/ Modern Defence Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation: [Online tool]. – Available at : http://www.nato.int/ lisbon2010/strategic–concept–2010–eng.pdf.

9. NATO Lisbon Summit Declaration, 20 Nowember 2010: [Online tool]. – Available at : http://www.nato.int/docu/pr/2010/p10-049e.html.

10. NATO Warsaw Summit Communiqué, 9 July 2016: [Online tool]. – Available at : http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

11. Information Tecnhology Security Evaluation Criteria: [Online tool]. – Available at : https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ Zertifizierung/ITS icherheitskriterien/itsec-en_pdf.pdf.

12. Common Criteria for Information Technology Security Evaluation: [Online tool]. – Available at : https://www.commoncriteriaportal.org/files/ccfiles/CCPART 2V3.1R4.pdf.

13. Нестеряк Ю.В. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз / Ю.В. Нестеряк [Електронний ресурс]. – Режим доступу : http://visnyk.academy.gov.ua/wp-content/uploads/2014/02/2013-3-8.pdf.

14. Communication from the European Commission: Network and Information Security: Proposal for a European Policy Approach. COM (2001) 298: [Online tool]. – Available at : http://ec.europa.eu/information_society/eeurope/2002/ news_library/pdf_files/netsec_en.pdf.

15. Safer Internet Programme: [Online tool]. – Available at: http : //ec.europa.eu/ information_society/activities/sip/policy/programme/current_prog/index_en.htm.

16. Communication from the Commission: Towards a general policy on the fight against cyber crime. COM (2007): [Online tool]. – Available at : http://eurlex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf.

17. Communication from the Commission on Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. COM (2009)149: [Online tool]. – Available at : http://ec.europa.eu/information_society/policy/nis/strategy/activities/ ciip/index_en.htm.

18. Костенко О.В. Європейські стандарти правового регулювання обігу інформації з обмеженим доступом у роботі органів прокуратури/ О.В. Костенко// Науковий вісник Ужгородського національного університету: серія «Право». – Випуск 34, том 3. – 2015. – С. 109.

19. Про доступ до інформації, яка знаходиться в розпорядженні державних органів : Рекомендації Ради Європи № R(81)19 [Електронний ресурс]. – Режим доступу : http://medialaw.org.ua/library/rekomendatsiya-r-81-19-pro-dostup-do-informatsiyi-shho-znahodytsya-u-rozporyadzhenni-derzhavnyh-organiv.

20. General Assembly Resolution «The right to privacy in the digital age», A/RES/68/167: [Online tool]. – Available at : мhttp://www.ohchr.org/EN/Issues/ DigitalAge/Pages/DigitalAgeIndex.aspx.

21. Гнатюк С.Л. Особливості захисту персональних даних в сучасному кіберпросторі: правові та техніко-технологічні аспекти: Аналітична доповідь / С.Л. Гнатюк. – К. : Нац. ін-т стратегічних досліджень, 2013. – 51 с.

22. Размєтаєва Ю.С. Приватність в інформаційному суспільстві: проблеми правового розуміння та регулювання / Ю.С. Размєтаєва // Науковий вісник Ужгородського національного університету : серія «Право». – Випуск 37, том 1. – 2016. – С. 43.

23. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_242.

24. Nigel Waters, Graham. Interpreting the Security Principle: [Online tool]. – Available at : http://www.cyberlawcentre.org/ipp/wp/WP1%20Security.pdf.

25. В Евросоюзе приняли новый закон о защите данных [Електронний ресурс]. – Режим доступу : https://threatpost.ru/v-evrosoyuze-prinyali-novyj-zakon-o-zashhite-dannyh/15749/.

26. Персональные данные: новые правила в Европейском Союзе [Електронний ресурс]. – Режим доступу : https://habrahabr.ru/post/300348/.

27. Василенко Д.П., Маслак В.І. Законодавство провідних країн світу в сфері захисту інформації / Д.П. Василенко // Вісник КДУ імені Михайла Остроградського. – Випуск № 61, частина 1. Частина 1. – С.128.

28. Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz - SÜG: [Online tool]. – Available at : http://www. gesetze -im-internet.de/s_g/BJNR086700994.html.

29. Teleservices Data Protection Act: [Online tool]. – Available at : http://ourworld.compuserve.com/homepages/ckuner/multimd.

30. Federal Act Governing Access to Information held by the Federal Government (Freedom of Information Act): [Online tool]. – Available at : http://www.gesetze-im-internet.de/ifg/BJNR272200005.html.

31. Stasi Files Act (Stasi-Unterlagengesetz, StUG): [Online tool]. – Available at : http://germanlawarchive.iuscomp.org/?p=714.

32. Act on the Federal Office for Information Security (BSI Act - BSIG): [Online tool]. – Available at : https://www.bsi.bund.de/DE/DasBSI/Gesetz/ gesetz.html (Accessed 18.09.2017).

33. Taking advantage of opportunities – avoiding risks: [Online tool]. – Available at : https://www.bsi/bund.de//EN/Home/home_node.html$ jsessionid= EA326461A185448F29C194C194C91BC85F23.2_cid286.

34. Климчук О.О., Ткачук Н.А. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки / О.О. Климчук // Інформаційна безпека людини, суспільства, держави. – 2015. – № 3(19). – С. 75.

35. Verfassungsschutz (Bfv): [Online tool]. – Available at : http://www. verfassungsschutz.de.

36. Cyber und Informationsraum: [Online tool]. – Available at http://cir. bundeswehr.de/portal/a/cir/start.

37. Laura Chappell, Palgrave Macmillan. Germany, Poland and the Common Security and Defence Policy: Converging Security and Defence Perspectives in an Enlarged EU. – 29 august 2012. – 232 p.

38. Тихомирова Є., Смик Р. Інформаційна політика Польщі / Є. Тихомирова, Р. Смик // Матеріали V Всеукраїнської науково-практичної конференції «Сучасні проблеми гуманітаристики: світоглядні пошуки, комунікативні та педагогічні стратегії». – Рівне, 2015. – С. 113.

39. Across Europe? Nations Mold Cyber Defenses: [Online tool]. – Available at : http:// archive.defensenews.com/article/20130709/DEFREG01/307090008/Across-Europr-Nations-Mold-Cyber-Defenses.

40. Countering cyberterrorism: [Online tool]. – Available at : http://msz.gov.pl/ en/foreign_policy/security_policy/international_terrorism/countering_cyber_terrorism/&printMode=true.

41. Доктрина кибезбезопасности Польщи [Електронний ресурс]. – Режим доступу : constitutions.ru/?p=11083.

42. Польща створює Доктрину інформаційної безпеки [Електронний ресурс]. – Режим доступу : http://www.eurointegration.com.ua/news/2015/07/ 26/7036321/.

43. Biuro Bezpieczeństwa Narodowego: [Online tool]. – Available at: en.bbn.gov.pl.

44. У Польщі створили центр боротьби з російською пропагандою [Електронний ресурс]. – Режим доступу : https://zaxid.net/u_polshhi stvorili_ tsentr_borotbi_z_rosiyskoyu_propagandoyu_n1424662.

45. Телеховський Ю. Досвід трансформації спецслужб Угорщини: висновки для України / Ю. Телеховський // Стратегічні пріоритети. – № 3(28). – 2013 р. – С. 151–155.

46. Европарламент принял резолюцию с осуждением Венгрии [Електронний ресурс]. – Режим доступу : http://www.novayagazeta.ru/news/ 54209.html.

47. Затинайко О., Павленко В., Бочарніков В., Свєшніков С. Політика безпеки і воєнно_політичні відносини Угорщини / О. Затинайко, В. Павленко, В. Бочарніков, С. Свєшніков // Наука і оборона. – № 1. – 2014. – С. 9.

48. Баранов А.А., Брижко В.М., Базанов Ю.К. Права людини і захист персональних даних / А.А. Баранов [Електронний ресурс]. – Режим доступу : library.khpg.org/files/docs/Kn_L_.pdf.

49. Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information): [Online tool]. – Available at : http://www.naih.hu/uegyfelszolgalat, kapcsolat.html.

50. Act on the Electronic Information Security of Central and Local Government Agencies): [Online tool]. – Available at : http://njt.hu/cgi_bin/njt_doc.cgi?docid= 160206.240508.

51. Hungary's National Security strategy (2012): [Online tool]. – Available at : http://2010-2014.kormany.hu/download/4/32/b0000/National%20Security% 20Strategy.pdf.

52. National Cyber Security Strategy of Hungary (2013): [Online tool]. – Available at: http://www.nbf.hu/anyagok/Government%20Decision%20No% 201139_2013%20on%20the%20National%20Cyber%20Security%20Strategy%20of%20Hungary.docx.

53. Information security act of the Republic of Croatia (2007): [Online tool]. – Available at: http://www.uvns.hr/UserDocsImages/en/dokumenti/info-security/ Information-Security-Act.pdf.

54. The national cyber security strategy of the republic: [Online tool]. – Available at: http://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20 National%20Cyber%20Security%20Strategy%20(2015).pdf.

55. Хорватія повернула свої території за три дні, а інформаційна війна тривала ще 15 років [Електронний ресурс]. – Режим доступу : http://milnavigator.com.ua/%D1%85%D0%BE%D1%80%D0%B2%D0%B0%D1%82%D1%96%D1%8F-%D0%BF%D0%BE%D0%B2%D0%B5%D1%80%D0% BD%D1%83%D0%BB%D0%B0-%D1%81%D0%B2%D0%BE%D1%97-%D1%82%D0%B5%D1%80%D0%B8%D1%82%D0%BE%D1%80%D1%96%D1%97-%D0%B7%D0%B0/.