Адміністративне право і процес; фінансове право; інформаційне право
УДК 34.096+321.01

Малашко Олександр Євгенійович
викладач кафедри адміністративного права та процесу,
фінансового і інформаційного права
Львівський університет бізнесу та права
Малашко Александр Евгеньевич
преподаватель кафедры административного права и процесса,
финансового и информационного права
Львовский университет бизнеса и права
Malashko Oleksandr
Lecturer of the Department of Administrative Law and Process,
Financial and Information Law
Lviv University of Business and Law
ORCID: 0000-0001-8676-5837

ПОЛІТИКА ТА СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КРАЇНАХ ЦЕНТРАЛЬНОЇ ЄВРОПИ
ПОЛИТИКА И СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СТРАНАХ ЦЕНТРАЛЬНОЙ ЕВРОПЫ
POLICY AND SYSTEM FOR ENSURING INFORMATION SECURITY IN THE COUNTRIES OF CENTRAL EUROPE

Анотація. *У статті розкрито концептуальні основи політики та системи забезпечення інформаційної безпеки в країнах Центральної Європи, зокрема у Німеччині, Польщі, Угорщині і Хорватії. З'ясовано, що Німеччина, Польща, Угорщина і Хорватії виступають країнами-членами Європейського Союзу та НАТО, тому на них поширюються правила та стандарти цих міжнародних організацій. Встановлено, що основними*

документами та програмами забезпечення інформаційної безпеки та кібербезпеки у країнах-членах ЄС та НАТО є: Документ С-М (2002)49 "Безпека в організації Північноатлантичного договору (НАТО)", Концепція кібербезпеки, сформульована за результатами Лісабонського саміту, Концепція кібербезпеки, сформульована за результатами Варшавського саміту, "Європейські критерії безпеки інформаційних технологій", "Єдині критерії безпеки інформаційних технологій", "Мережева та інформаційна безпека: європейський політичний підхід", "Безпечний інтернет", "На шляху до загальної політики в сфері боротьби з кіберзлочинністю", "Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості", Директива 95/46/ЄС "Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних". Визначено, що у Німеччині політика та система забезпечення інформаційної безпеки та кібербезпеки базується на Законі "Про перевірку безпеки", "Акті захисту інформації в телекомунікаціях", "Акті про свободу інформації", Законі "Про посилення безпеки інформаційних систем". Встановлено, що у Польщі політика та система забезпечення інформаційної безпеки та кібербезпеки базується на Законі "Про пошту", Законі "Про телебачення і радіомовлення", Законі "Про державні відносини з Римсько-Католицькою церквою в Республіці Польща", Стратегії кібербезпеки Польщі, Доктрині кібербезпеки Польщі, Доктрині інформаційної безпеки Польщі. З'ясовано, що в Угорщині політика та система забезпечення інформаційної безпеки та кібербезпеки базується на Законі "Про захист інформації про особу та доступ до інформації, що становить суспільний інтерес", Законі "Про право на інформаційне самовизначення та свободу інформації", Законі "Про обробку і захист медичної інформації та пов'язаних з нею персональних даних", "Акті з питань електронної інформаційної безпеки державних та муніципальних органів", Стратегії національної безпеки Угорщини,

Національній стратегії кібербезпеки Угорщини. Визначено, що в Хорватії політика та система забезпечення інформаційної безпеки та кібербезпеки базується на "Акті про інформаційну безпеку" та Національній стратегії кібербезпеки. Доведено, що Україна, яка обрала курс євроінтеграції, повинна орієнтуватися на ряд стратегій забезпечення інформаційної безпеки, визначених у країнах-членах Європейського Союзу, зокрема у Німеччині, Польщі, Угорщині та Хорватії.

Ключові слова: *інформаційна безпека, кібербезпека, забезпечення, інформаційна сфера, загроза.*

Аннотация. *В статье раскрыто концептуальные основы политики и системы обеспечения информационной безопасности в странах Центральной Европы, в частности в Германии, Польше, Венгрии и Хорватии. Выяснено, что Германия, Польша, Венгрия и Хорватия выступают странами-членами Европейского Союза и НАТО, поэтому на них распространяются правила и стандарты этих международных организаций. Установлено, что основными документами и программами обеспечения информационной безопасности и кибербезопасности в странах-членах ЕС и НАТО являются: Документ С-М (2002)49 "Безопасность в организации Североатлантического договора (НАТО)", Концепция кибербезопасности, сформулирована по результатам Лиссабонского саммита, Концепция кибербезопасности, сформулирована по результатам Варшавского саммита, "Европейские критерии безопасности информационных технологий", "Единые критерии безопасности информационных технологий", "Сетевая и информационная безопасность: европейский политический подход", "Безопасный интернет", "На пути к общей политики в сфере борьбы с киберпреступностью", "Защита Европы от широкомасштабных кибератак и разрушений: усиление уровня подготовленности, безопасности*

и устойчивости", Директива 95/46/ЕС "О защите физических лиц в контексте обработки персональных данных и свободного обращения таких данных". Определено, что в Германии политика и система обеспечения информационной безопасности и кибербезопасности базируется на Законе "О проверке безопасности", "Акте защиты информации в телекоммуникациях", "Акте о свободе информации", Законе "Об усилении безопасности информационных систем". Установлено, что в Польше политика и система обеспечения информационной безопасности и кибербезопасности базируется на Законе "О почте", Законе "О телевидении и радиовещании", Законе "О государственных отношения с Римско-Католической церковью в Республике Польша", Стратегии кибербезопасности Польши, Доктрине кибербезопасности Польши, Доктрине информационной безопасности Польши. Установлено, что в Венгрии политика и система обеспечения информационной безопасности и кибербезопасности базируется на Законе "О защите информации о лице и доступ к информации, представляющей общественный интерес", Законе "О праве на информационное самоопределение и свободу информации", Законе "О обработку и защиту медицинской информации и связанных с ней персональных данных", "Акте по вопросам электронной информационной безопасности государственных и муниципальных органов", Стратегии национальной безопасности Венгрии, Национальной стратегии кибербезопасности Венгрии. Определено, что в Хорватии политика и система обеспечения информационной безопасности и кибербезопасности базируется на "Акте об информационной безопасности" и Национальной стратегии кибербезопасности. Доказано, что Украина, которая выбрала курс евроинтеграции, должна ориентироваться на ряд стратегий обеспечения информационной безопасности, определенных в странах-членах Европейского Союза, в частности в Германии, Польше, Венгрии и Хорватии.

Ключевые слова: *информационная безопасность, кибербезопасность, обеспечение, информационная сфера, угроза.*

Summary. *The article reveals the conceptual foundations of the policy and system for ensuring information security in the countries of Central Europe, in particular in Germany, Poland, Hungary and Croatia. It was found that Germany, Poland, Hungary and Croatia are member countries of the European Union and NATO, therefore they are subject to the rules and standards of these international organizations. It was established that the main documents and programs for ensuring information security and cybersecurity in the EU and NATO member states are: Document C-M (2002) 49 "Security in the North Atlantic Treaty Organization (NATO)", the Cybersecurity Concept, formulated based on the results of the Lisbon Summit, the Concept cybersecurity, formulated as a result of the Warsaw Summit, "European Criteria for Information Technology Security", "Common Criteria for Information Technology Security", "Network and Information Security: a European Political Approach", "Safe Internet", "Towards a Common Policy in the Field of Combating cybercrime","Protecting Europe from large-scale cyber attacks and disruption: strengthening preparedness, security and resilience", Directive 95/46 / EU "On the protection of individuals in the context of the processing of personal data and the free circulation of such data ". It was determined that in Germany the policy and system for ensuring information security and cybersecurity is based on the Law "On Security Inspection", the "Act for the Protection of Information in Telecommunications", the "Act on Freedom of Information", and the Law "On Strengthening the Security of Information Systems". It was established that in Poland the policy and system for ensuring information security and cybersecurity is based on the Law "On Mail", the Law "On Television and Radio Broadcasting", the Law "On State Relations with the Roman Catholic Church in the Republic of Poland", the Cybersecurity Strategy of Poland, the Doctrine of*

Cybersecurity Poland, Poland's Information Security Doctrine. It has been established that in Hungary the policy and system for ensuring information security and cybersecurity is based on the Law "On the Protection of Information about a Person and Access to Information of Public Interest", the Law "On the Right to Information Self-Determination and Freedom of Information", the Law "On Processing and Protection medical information and related personal data", "Act on Electronic Information Security of State and Municipal Bodies", Hungarian National Security Strategy, Hungarian National Cybersecurity Strategy. It was determined that in Croatia the policy and system for ensuring information security and cyber security is based on the "Information Security Act" and the National Cyber Security Strategy. It has been proved that Ukraine, which has chosen the course of European integration, should be guided by a number of information security strategies identified in the member states of the European Union, in particular in Germany, Poland, Hungary and Croatia.

Key words: *information security, cyber security, providing, information sphere, threat.*

Постановка проблеми. Практика забезпечення інформаційної безпеки в країнах Центральної Європи показує, що на даний час немає чіткої та водночас комплексної моделі формування національної системи безпеки у інформаційній сфері. При цьому, нагальною виступає проблематика впровадження заходів протидії загрозам у інформаційній сфері (у більшості випадків – кіберзагрозам). Окрім цього, удосконалення потребують також методи і форми захисту інформації та інформаційної інфраструктури у кожній із країн світу, зокрема і країн Центральної Європи.

Водночас Україна, яка обрала курс євроінтеграції, повинна орієнтуватися на ряд стратегій забезпечення інформаційної безпеки, визначених у країнах-членах Європейського Союзу [1, с. 18]. Окрім цього, Україна, в контексті забезпечення інформаційної безпеки, має враховувати і

особливості свого геополітичного розташування, при цьому базуватись на досвіді країн Центральної і Східної Європи.

Сучасна практика доводить, що саме країни Центральної і Східної Європи на сьогодні успішно впровадили оптимальну модель інформаційного суспільства, у якій присутні розвинена інформаційна інфраструктура та інноваційні інформаційні технології. Саме ці компоненти інформаційної безпеки країн Центральної та Східної Європи визначаються високим рівнем доступності та мають випереджаючі показники, на відміну від інших світових країн [2, с. 35].

В рамках формування політики та побудови системи забезпечення інформаційної безпеки Україні першочергово потрібно вивчати, аналізувати та використовувати досвід країн Центральної Європи. При цьому, одним із важливих аспектів таких дій є саме нинішня ситуація, у якій перебуває Україна, яка свідчить про неготовність державної влади протистояти інформаційним загрозам [3, с. 179].

Аналіз останніх досліджень і публікацій. Дослідження проблематики забезпечення інформаційної безпеки на сьогодні проводяться багатьма науковцями та вченими, зокрема значний внесок у цьому напрямку здійснили Д. П. Василенко [4], О. Гладун [3], О. О. Климчук [5], О. В. Костенко [6], В. І. Маслак [4], Ю. В. Нестеряк [7], В. С. Політанський [1–2], Н. А. Ткачук [5], В. Шатун [3], Р. М. Скриньковський та інші.

Проте, опираючись на дослідженнях, представлених вищезазначеними науковцями, варто відмітити, що ця проблематика є ще не до кінця вивченою та вимагає проведення більш комплексного дослідження, зокрема у сфері формування політики та побудови системи забезпечення інформаційної безпеки, базуючись при цьому на досвіді провідних європейських країн.

Мета статті. Метою статті є дослідження концептуальних основ політики та системи забезпечення інформаційної безпеки в країнах

Центральної Європи.

Виклад основного матеріалу дослідження. Офіційного підтвердження приналежності європейських країн до блоку країн Центральної Європи на сьогодні немає. Практика показує, що у більшості випадків до країн Центральної Європи відносять такі країни як Австрію, Ліхтенштейн, Німеччину та Швейцарію. За даними джерела [8] у цю категорію країн також слід віднести як країни Вишеградської групи, зокрема Польщу, Словаччину, Угорщину та Чехію, так і частину країн Балканського півострова.

Враховуючи вищезазначене, для розкриття концептуальних основ політики та системи забезпечення інформаційної безпеки в країнах Центральної Європи, як приклад, слід зосередити увагу на досвіді Німеччини, Польщі Угорщини і Хорватії.

Тут слід відмітити, що вищеперелічені чотири країни, а саме Німеччина, Польща, Угорщина і Хорватії виступають країнами-членами Європейського Союзу та НАТО. З огляду на те, на них поширюються правила та стандарти міжнародних організацій, учасниками яких вони є, стосовно політики та системи забезпечення інформаційної безпеки.

До прикладу, це:

1) Документ С-М (2002)49 “Безпека в організації Північноатлантичного договору (НАТО)” (Document C-M (2002)49 “Security within the North Atlantic Treaty Organisation (NATO)”) [9];

2) концепція кібербезпеки, сформульована за результатами Лісабонського саміту (Lisbon Summit Declaration) [10];

3) концепція кібербезпеки, сформульована за результатами Варшавського саміту (Warsaw Summit Communique) [11].

На відміну від НАТО, Європейський Союз також проводить подібну політику щодо забезпечення інформаційної безпеки. Як приклад, то ще у 1991 році країнами-членами Європейського Союзу розроблено та введено в

дію спеціальний документ під назвою “Європейські критерії безпеки інформаційних технологій” (“Information Technology Security Evaluation Criteria (ITSEC)”) [12]. Положеннями цього документу визначені ключові завдання забезпечення інформаційної безпеки, які полягають у:

1) захисті інформаційних ресурсів від впливу загроз, що виникають внаслідок несанкціонованого (незаконного) доступу та спричиняють порушення конфіденційності інформації;

2) забезпеченні цілісності інформаційних ресурсів внаслідок досягнення захисту інформаційних ресурсів від впливу несанкціонованої модифікації чи знищення;

3) досягненні безперебійної роботи систем інформаційної сфери внаслідок протидії та усунення загроз, які перешкоджають та сповільнюють процес обслуговування інформаційних систем.

Разом з тим, у 1996 році країнами-членами Європейського Союзу розроблено та введено в дію спеціальний стандарт європейської інформаційної безпеки під назвою “Єдині критерії безпеки інформаційних технологій” (“Common Criteria for Information Technology Security Evaluation”), які, до того, були дещо удосконалені у 2017 році [13].

Згідно із документом “Єдині критерії безпеки інформаційних технологій” (“Common Criteria for Information Technology Security Evaluation”), інформаційна безпека характеризується трьома ключовими ознаками, які формують модель тріади CIA [7]. Так, це такі ознаки як доступність, конфіденційність та цілісність.

Окрім зазначених вище документів, Європейською Комісією у 2001 році розроблено та введено в дію документ “Мережева та інформаційна безпека: європейський політичний підхід” (Document COM(2001)298 “Communication Network and Information Security: Proposal for A European Policy Approach”) [14]. Відповідно до положень цього документу Європейським Союзом розроблено спеціальний підхід до забезпечення

безпеки у інформаційній сфері внаслідок використання мережевої і інформаційної безпеки. Суть мережевої і інформаційної безпеки полягає у здатності мережі чи інформаційної системи протистояти загрозам автентичності, доступності, цілісності та конфіденційності інформації, які передаються чи зберігаються через відповідні мережі та системи.

Також документом “Мережева та інформаційна безпека: європейський політичний підхід” (Document COM(2001)298 “Communication Network and Information Security: Proposal for A European Policy Approach”) [14] у сфері забезпечення інформаційної безпеки визначено такі ключові напрямки:

1) підвищити обізнаність користувачів про можливі загрози, які виникають внаслідок користування комунікаційними мережами;

2) створити спеціальну систему попередження і інформування користувачів комунікаційних мереж про нові види інформаційних загроз та кіберзагроз;

3) забезпечити технологічну підтримку користувачів комунікаційних мереж;

4) у ході забезпечення інформаційної безпеки орієнтуватись на особливості ринкової стандартизації і сертифікації;

5) забезпечити правовий захист персональних даних та регламентацію телекомунікаційних послуг, що у перспективі сприятиме протидії кіберзлочинності;

6) посилити інформаційну безпеку на рівні країни внаслідок впровадження більш ефективних та сумісних засобів і використання більш результативних методів забезпечення інформаційної безпеки;

7) заохочувати країни-члени Європейського Союзу до використання електронних підписів внаслідок надання офіційних он-лайн послуг;

8) сприяти розвитку міжнародного співробітництва у сфері забезпечення інформаційної безпеки.

Дослідження доводять також, що у країнах-членах Європейського

Союзу в контексті забезпечення інформаційної безпеки особлива увага зосереджується саме на проблематиці кібербезпеки, адже кібербезпека виступає важливою складовою інформаційної безпеки.

Так, із 1999 року Європейським Союзом розроблено та введено в дію програму "Безпечний інтернет" ("Safer Internet Programme") [15]. Відповідно до положень цієї програми передбачається боротьба із шкідливим контентом та небезпечною поведінкою у мережі.

Водночас у 2007 році Європейською Комісією розроблено та введено в дію документ під назвою "На шляху до загальної політики в сфері боротьби з кіберзлочинністю" (Document COM (2007)267 "Communication from the Commission: Towards a general policy on the fight against cyber crime") [16]. У цьому документі кіберзлочинність трактується як особливі кримінальні дії, які вчинені, вчиняються та/чи будуть вчинені через використання електронних комунікативних мереж і інформаційних систем чи є проти цих мереж і систем та проявляються через такі форми злочину, як шахрайство, підробка у електронних комунікаційних мережах і інформаційних системах, публікація незаконного контенту у електронних медіа, хакерство, атаки у інформаційній сфері.

Крім того, у 2009 році Європейською Комісією опубліковано документ під назвою "Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості" (Document COM(2009)149 "Communication Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience") [17]. Так, цим Повідомленням визначаються ключові проблеми у сфері безпеки інформаційної сфері, які вимагають негайного реагування на їх вирішення зі сторони країн-членів Європейського Союзу. З огляду на те, це такі проблеми як:

а) некоординовані підходи до забезпечення безпеки інформаційної

інфраструктури, які пропонуються країнами-членами Європейського Союзу;

б) низький рівень партнерства між державою та приватним сектором;

в) недостатні можливості виявляти на ранньому етапі інформаційні загрози;

г) низький рівень міжнародного консенсусу у напрямку реалізації політики захисту інформаційної інфраструктури.

Також документом під назвою "Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості" (Document COM(2009)149 "Communication Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience") [17] окреслено низку заходів, які є необхідними для посилення інформаційної безпеки.

Дослідження доводять, що у європейських країнах інформаційна відкритість органів державної влади проявляється у тому випадку, коли громадськість є у повному обсязі поінформована, оскільки саме на таких умовах може будуватися сильна демократична система [6, с. 110].

Вищезазначене твердження також має місце і у рекомендаціях Ради Європи № R(81)19 "Про доступ до інформації, яка знаходиться в розпорядженні державних органів" [18]. Відтак, цими рекомендаціями передбачається забезпечення адекватної участі усіх в суспільному житті, зокрема відкритий доступ громадськості до різної інформації, якою володіють органи державної влади.

Варто також звернути увагу і на аспекти, визначені Генеральною Асамблеєю ООН стосовно особливостей приватності. Так, резолюцією "Право на приватність у цифрову епоху" ("General Assembly Resolution "The Right to Privacy in the Digital Age", A/RES/68/167") [19], яку прийнято 18 грудня 2013 року, визначається, що Інтернет має відкриту та глобальну

природу, а розвиток інформаційних і комунікативних технологій сьогодні проводиться швидкими темпами, що у перспективі виступає важливою рушійною силою інформаційного прогресу.

Що стосується особливостей захисту персональних даних, то тут слід зазначити, що у країнах-членах Європейського Союзу, зокрема і в країнах Центральної Європи, право громадськості на захист персональних даних забезпечується та регулюється Директивою 95/46/ЄС "Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних" [20]. Відповідно до положень цього документу передбачається вільне переміщення інформації між країнами-членами Європейського Союзу, а також захист основних прав громадськості, зокрема права на недоторканність особистих даних та забезпечення їх захисту від третіх осіб.

Директива 95/46/ЄС "Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних" [20] також зобов'язує кожну країну-учасника Європейського Союзу прийняти спеціальний закон про захист персональних (приватних) даних, який базуватиметься на положеннях рекомендацій Організації економічного співробітництва та розвитку (OECD), зокрема на положеннях рекомендації "Принцип гарантованої безпеки N11" ("Paragraph 11: Security Safeguards Principle") [21].

У 2016 році також ухвалено нові правила захисту персональних даних для країн-членів Європейського Союзу. Однак набуття чинності цих прав відбулося тільки у 2018 році.

Дослідження доводять, що у країнах Центральної Європи, які до того є країнами-членами Європейського Союзу, існує певна злагоджена система захисту інформації, однак у кожній із країн Центральної Європи вона має свої особливості [4, с. 129].

До прикладу у законодавстві Німеччини, зокрема відповідно до Закону "Про перевірку безпеки" ("Gesetz über die Voraussetzungen und das

Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitüberprüfungsgesetz – SÜG)") [22], секретною інформацією вважаються факти, вироби і відомості будь-якої форми пред'явлення, які, перебуваючи у державних інтересах, повинні зберігатися у таємниці та мати відповідний ступінь секретності, наданий спеціальним державним органом.

У Німеччині також прийнятий "Акт захисту інформації в телекомунікаціях" ("Teleservices Data Protection Act (Teledienstedatenschutzgesetz, TDDSG)") [23] (жовтень 1997 рік). Згідно положень цього документу передбачається, що збирання, обробка і використання інформації здійснюються за згодою користувача чи дозволяються у випадках, передбачених законодавством.

У 2005 році у Німеччині прийнято та введено в дію "Акт про свободу інформації" ("Federal Act Governing Access to Information held by the Federal Government") [24]. Цей документ регулює питання доступу до інформації, а нагляд за дотриманням положень цього документу покладений на комісара із захисту інформації та персональних даних.

Вивчаючи законодавство Німеччини стосовно забезпечення інформаційної безпеки, то тут варто також відмітити та водночас віднести до списку важливих документів і такий документ як Закон "Про посилення безпеки інформаційних систем" ("Act on the Federal Office for Information Security (BSI Act – BSIG)") [25].

Для сприяння оптимізації оперативної співпраці між органами державної влади і державними установами у Німеччині створено спеціальне Федеративне відомство безпеки інформаційних систем (Das Bundesamt für Sicherheit in der Informationstechnik (BSI)), одним із важливих секторів якого є національний центр кіберзахисту (NCAZ) [5, с. 78].

Що стосується особливостей політики та системи забезпечення інформаційної безпеки в Польщі, то варто зазначити, що ця країна

орієнтується на побудову відкритого вільного суспільства із особливим нахилом на забезпечення прав громадянина. Правова база Польщі стосовно захисту інформаційної сфери базується на законодавстві, прийнятому ще у 90-х роках XX-го століття. Так, основними законами цієї правової бази виступають:

– Закон "Про пошту" ("Prawo pocztowe") [26];

– Закон "Про телебачення і радіомовлення" ("Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji") [27];

– Закон "Про державні відносини з римською католицькою церквою в Республіці Польща" ("Ustawa z dnia 17 maja 1989 r. o stosunku Państwa do Kościoła Katolickiego w Rzeczypospolitej Polskiej") [28] тощо.

Стосовно основних суб'єктів забезпечення інформаційної безпеки у Польщі, то провідну роль у цьому процесі виконує Агентство внутрішньої безпеки (Agencja Bezpieczeństwa Wewnętrznego). Так, у 2013 році Агентством внутрішньої безпеки розроблено та введено в дію Стратегію кібербезпеки Польщі (Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej). Також за ініціацією Агентства внутрішньої безпеки створено Центр криптології при Міністерстві національної оборони (Narodowe Centrum Kryptologii), до основних компетенцій якого належить забезпечення захисту інформації, гарантування кібероборони і проведення різних кібероперацій по усуненні та нейтралізації кіберзагроз [29].

Варто зазначити і те, що окрім Агентства внутрішньої безпеки, питаннями забезпечення інформаційної безпеки та кібербезпеки у Польщі займається також Бюро національної безпеки Польщі (Biuro Bezpieczeństwa Narodowego). Так, під керівництвом Бюро національної безпеки Польщі розроблено та введено в дію Доктрину кібербезпеки Польщі (Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej) [30], згідно якої передбачається ряд заходів по забезпеченню інформаційної безпеки та кібербезпеки.

Також у 2015 році Бюро національної безпеки Польщі почало активно працювати над створенням Доктрини інформаційної безпеки Польщі (Doktryna bezpieczeństwa informacyjnego RP) [31], у якій повинні бути відображені основні засади досягнення положень Стратегії національної безпеки Польщі (Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej).

Досліджуючи особливості забезпечення інформаційної безпеки в Угорщині, то тут слід відмітити, що ця країна також активно здійснює політику захисту інформаційної безпеки. Так, в Угорщині у 1992 році прийнято Закон "Про захист інформації про особу та доступ до інформації, що становить суспільний інтерес" ("1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról") [32]. Згідно положень цього закону зазначається, що інформація будь-якої форми, обробка якої здійснюється органами в рамках виконання суспільних обов'язків, являє собою суспільний інтерес. До такої інформації не належить інформація про особу.

Окрім вищезазначеного закону, в Угорщині правове регулювання захисту інформаційної безпеки та кібербезпеки регулюється такими документами, як:

– Закон "Про право на інформаційне самовизначення та свободу інформації" ("2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról") [33];

– Закон "Про обробку і захист медичної інформації та пов'язаних з нею персональних даних" ("1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről") [34];

– "Акт з питань електронної інформаційної безпеки державних та муніципальних органів" ("2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról") [35];

– Стратегія національної безпеки Угорщини (Magyarország Nemzeti

Biztonsági Stratégiája) [36];

– Національна стратегія кібербезпеки Угорщини (Magyarország Nemzeti Kiberbiztonsági Stratégiájáról) [37].

Своєю чергою, у Хорватії також посиленими темпами проводиться політика забезпечення інформаційної безпеки та кібербезпеки. Так, із 2007 року у цій країні прийнято та введено в дію "Акт про інформаційну безпеку" ("Zakon o informacijskoj sigurnosti") [38]. Цим документом визначаються основні особливості та засади інформаційної безпеки, а також наведені ряд заходів і стандартів по забезпеченню інформаційної безпеки.

У 2015 році в Хорватії прийнято Національну стратегію кібербезпеки (Nacionalna strategija kibernetičke sigurnosti) [39]. Так положеннями цієї стратегії зазначається, що кібербезпека охоплює такі об'єкти як кіберпростір, користувачів та інфраструктуру.

Висновки і перспективи подальших розвідок. Результати опрацювання джерел [1–39] дали можливість розкрити концептуальні основи політики та системи забезпечення інформаційної безпеки в країнах Центральної Європи, зокрема в Німеччині, Польщі, Угорщині і Хорватії. У ході дослідження з'ясовано, що Німеччина, Польща, Угорщина і Хорватії виступають країнами-членами Європейського Союзу та НАТО, тому на них поширюються правила та стандарти цих міжнародних організацій. Встановлено, що основними документами та програмами забезпечення інформаційної безпеки та кібербезпеки у країнах-членах ЄС та НАТО є: Документ СМ (2002)49 "Безпека в організації Північноатлантичного договору (НАТО)", концепція кібербезпеки, сформульована за результатами Лісабонського саміту, концепція кібербезпеки, сформульована за результатами Варшавського саміту, "Європейські критерії безпеки інформаційних технологій", "Єдині критерії безпеки інформаційних технологій", "Мережева та інформаційна безпека: європейський політичний підхід", "Безпечний інтернет", "На шляху до загальної політики в сфері

боротьби з кіберзлочинністю", "Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості", Директива 95/46/ЄС "Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних". Визначено, що у Німеччині політика та система забезпечення інформаційної безпеки та кібербезпеки базується на Законі "Про перевірку безпеки", "Акті захисту інформації в телекомунікаціях", "Акті про свободу інформації", Законі "Про посилення безпеки інформаційних систем". Встановлено, що у Польщі політика та система забезпечення інформаційної безпеки та кібербезпеки базується на Законі "Про пошту", Законі "Про телебачення і радіомовлення", Законі "Про державні відносини з римською католицькою церквою в Республіці Польща", Стратегії кібербезпеки Польщі, Доктрині кібербезпеки Польщі, Доктрині інформаційної безпеки Польщі. З'ясовано, що в Угорщині політика та система забезпечення інформаційної безпеки та кібербезпеки базується на Законі "Про захист інформації про особу та доступ до інформації, що становить суспільний інтерес", Законі "Про право на інформаційне самовизначення та свободу інформації", Законі "Про обробку і захист медичної інформації та пов'язаних з нею персональних даних", "Акті з питань електронної інформаційної безпеки державних та муніципальних органів", Стратегії національної безпеки Угорщини, Національній стратегії кібербезпеки Угорщини. Визначено, що в Хорватії політика та система забезпечення інформаційної безпеки та кібербезпеки базується на "Акті про інформаційну безпеку" та Національній стратегії кібербезпеки. Доведено, що Україна, яка обрала курс євроінтеграції, повинна орієнтуватися на ряд стратегій забезпечення інформаційної безпеки, визначених у країнах-членах Європейського Союзу, зокрема у Німеччині, Польщі, Угорщині та Хорватії.

Література

1. Політанський В. С. Інформаційне суспільство в Україні: від зародження до сьогодення // Науковий вісник Ужгородського національного університету. Серія: Право. 2017. Випуск 42. С. 16–22.
2. Політанський В. С. Світові моделі та фундаментальні принципи інформаційного суспільства // Науковий вісник Ужгородського національного університету. Серія: Право. 2017. Випуск 43, Том 1. С. 34–39.
3. Шатун В., Гладун О. Інформаційна безпека – невід'ємна складова національної безпеки України // Наукові праці. Державне управління. 2016. Випуск 255, Том 267. С. 174–180.
4. Василенко Д. П., Маслак В. І. Законодавство провідних країн світу в сфері захисту інформації // Вісник КДУ імені Михайла Остроградського. 2010. Випуск 2 (61). С. 128–132.
5. Климчук О. О., Ткачук Н. А. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки // Інформаційна безпека людини, суспільства, держави. 2015. № 3 (19). С. 75.
6. Костенко О. В. Європейські стандарти правового регулювання обігу інформації з обмеженим доступом у роботі органів прокуратури // Науковий вісник Ужгородського національного університету. Серія "Право". 2015. Випуск 34. Том 3. С. 109–114.
7. Нестеряк Ю. В. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз // Публічне управління: теорія та практика. 2014. Випуск 1. С. 62–67.
8. The World Factbook: Central Intelligence Agency. URL: https://www.cia.gov/library/publications/the-world-factbook/
9. Security within the North Atlantic Treaty Organisation (NATO): Document C-M(2002)49, 17 June 2002 // North Atlantic Council. 2002. URL:

https://cryptome.org/nato-cm2002-49.htm

10. Lisbon Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon // North Atlantic Treaty Organization, 20 Nov. 2010. URL: https://www.nato.int/cps/en/natolive/official_texts_68828.htm
11. Warsaw Summit Communiqué: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 // North Atlantic Treaty Organization, 09 Jul. 2016. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm
12. Information Technology Security Evaluation Criteria (ITSEC). Provisional evaluation criteria: Document COM(90)314. Luxembourg: Office for Official Publications Office of the EU, 1991. URL: https://www.ssi.gouv.fr/uploads/2015/01/ITSEC-uk.pdf
13. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. April 2017. Version 3.1. Revision 5. URL: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
14. Document COM(2001)298 – Communication Network and Information Security: Proposal for A European Policy Approach // EU Monitor. URL: https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vikqhjbr2gzy
15. Safer Internet Programme – Call for Proposals and Work Programme for 2013. URL: https://ec.europa.eu/digital-single-market/en/news/safer-internet-programme-call-proposals-and-work-programme-2013
16. Document COM (2007)267 – Communication from the Commission: Towards a general policy on the fight against cyber crime. Commission of the European Communities, Brussels, 22.05.2007 // EUR-Lex.europa.eu. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF
17. Document COM(2009)149 – Communication Critical Information

Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience // EU Monitor. URL: https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vikqhne787z0

18. Про доступ до інформації, яка знаходиться в розпорядженні державних органів: Рекомендації Ради Європи № R (81)19 // Центр демократії та верховенства права, 20.06.2005. URL: https://cedem.org.ua/library/rekomendatsiya-r-81-19-pro-dostup-do-informatsiyi-shho-znahodytsya-u-rozporyadzhenni-derzhavnyh-organiv/
19. General Assembly Resolution "The Right to Privacy in the Digital Age", A/RES/68/167. URL: https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx
20. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних: Директива 95/46/ЄС Європейського Парламенту і Ради від 24.10.1995. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text
21. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. URL: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
22. Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitüberprüfungsgesetz – SÜG). URL: https://www.gesetze-im-internet.de/s_g/S%C3%9CG.pdf
23. Teleservices Data Protection Act (Teledienstedatenschutzgesetz, TDDSG). URL: http://www.iuscomp.org/gla/statutes/TDDSG.htm
24. Federal Act Governing Access to Information held by the Federal Government (Freedom of Information Act). URL: http://www.gesetze-im-internet.de/englisch_ifg/

25. Act on the Federal Office for Information Security (BSI Act – BSIG). URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf
26. Prawo pocztowe. URL: https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/prawo-pocztowe-17938059
27. Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji. URL: http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19930070034
28. Ustawa z dnia 17 maja 1989 r. o stosunku Państwa do Kościoła Katolickiego w Rzeczypospolitej Polskiej. URL: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19890290154
29. Across Europe, Nations Mold Cyber Defenses. URL: http://rpdefense.over-blog.com/across-europe-nations-mold-cyber-defenses
30. Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej. URL: https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf
31. Doktryna bezpieczeństwa informacyjnego RP – analiza syntetyczna. URL: https://obserwatorpolityczny.pl/doktryna-bezpieczenstwa-informacyjnego-rp-analiza-syntetyczna/
32. 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról. URL: https://mkogy.jogtar.hu/jogszabaly?docid=99200063.TV
33. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról. URL: https://net.jogtar.hu/jogszabaly?docid=a1100112.tv
34. 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről. URL: https://net.jogtar.hu/jogszabaly?docid=99700047.tv
35. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. URL: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv

36. Magyarország Nemzeti Biztonsági Stratégiája. URL: http://www.nemzetesbiztonsag.hu/letoltes.php?letolt=576
37. Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. URL: http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845
38. Zakon o informacijskoj sigurnosti. URL: https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti
39. Nacionalna strategija kibernetičke sigurnosti. URL: https://www.uvns.hr/hr/aktualnosti-i-obavijesti/nacionalna-strategija-kiberneticke-sigurnosti

References

1. Politanskyi V. S. Informatsiine suspilstvo v Ukraini: vid zarodzhennia do sohodennia // Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo. 2017. Vypusk 42. S. 16–22.
2. Politanskyi V. S. Svitovi modeli ta fundamentalni pryntsypy informatsiinoho suspilstva // Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Ceriia: Pravo. 2017. Vypusk 43, Tom 1. S. 34–39.
3. Shatun V., Hladun O. Informatsiina bezpeka – nevidiemna skladova natsionalnoi bezpeky Ukrainy // Naukovi pratsi. Derzhavne upravlinnia. 2016. Vypusk 255, Tom 267. S. 174–180.
4. Vasylenko D. P., Maslak V. I. Zakonodavstvo providnykh krain svitu v sferi zakhystu informatsii // Visnyk KDU imeni Mykhaila Ostrohradskoho. 2010. Vypusk 2 (61). S. 128–132.
5. Klymchuk O. O., Tkachuk N. A. Rol i mistse spetssluzhb ta pravookhoronnykh orhaniv providnykh krain svitu v natsionalnykh systemakh kiberbezpeky // Informatsiina bezpeka liudyny, suspilstva, derzhavy. 2015. № 3 (19). S. 75.
6. Kostenko O. V. Yevropeiski standarty pravovoho rehuliuvannia obihu informatsii z obmezhenym dostupom u roboti orhaniv prokuratury //

Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Ceriia "Pravo". 2015. Vypusk 34. Tom 3. S. 109–114.

7. Nesteriak Yu. V. Mizhnarodni kryterii informatsiinoi bezpeky derzhavy: teoretyko-metodolohichnyi analiz // Publichne upravlinnia: teoriia ta praktyka. 2014. Vypusk 1. S. 62–67.
8. The World Factbook: Central Intelligence Agency. URL: https://www.cia.gov/library/publications/the-world-factbook/
9. Security within the North Atlantic Treaty Organisation (NATO): Document C-M(2002)49, 17 June 2002 // North Atlantic Council. 2002. URL: https://cryptome.org/nato-cm2002-49.htm
10. Lisbon Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon // North Atlantic Treaty Organization, 20 Nov. 2010. URL: https://www.nato.int/cps/en/natolive/official_texts_68828.htm
11. Warsaw Summit Communiqué: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 // North Atlantic Treaty Organization, 09 Jul. 2016. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm
12. Information Technology Security Evaluation Criteria (ITSEC). Provisional evaluation criteria: Document COM(90)314. Luxembourg: Office for Official Publications Office of the EU, 1991. URL: https://www.ssi.gouv.fr/uploads/2015/01/ITSEC-uk.pdf
13. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. April 2017. Version 3.1. Revision 5. URL: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
14. Document COM(2001)298 – Communication Network and Information Security: Proposal for A European Policy Approach // EU Monitor. URL: https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vikqhjbr2gzy
15. Safer Internet Programme – Call for Proposals and Work Programme for

2013. URL: https://ec.europa.eu/digital-single-market/en/news/safer-internet-programme-call-proposals-and-work-programme-2013

16. Document COM (2007)267 – Communication from the Commission: Towards a general policy on the fight against cyber crime. Commission of the European Communities, Brussels, 22.05.2007 // EUR-Lex.europa.eu. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF
17. Document COM(2009)149 – Communication Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience // EU Monitor. URL: https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vikqhne787z0
18. Pro dostup do informatsii, yaka znakhodytsia v rozporiadzhenni derzhavnykh orhaniv: Rekomendatsii Rady Yevropy № R (81)19 // Tsentr demokratii ta verkhovenstva prava, 20.06.2005. URL: https://cedem.org.ua/library/rekomendatsiya-r-81-19-pro-dostup-do-informatsiyi-shho-znahodytsya-u-rozporyadzhenni-derzhavnyh-organiv/
19. General Assembly Resolution "The Right to Privacy in the Digital Age", A/RES/68/167. URL: https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx
20. Pro zakhyst fizychnykh osib pry obrobtsi personalnykh danykh i pro vilne peremishchennia takykh danykh: Dyrektyva 95/46/IeS Yevropeiskoho Parlamentu i Rady vid 24.10.1995. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text
21. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. URL: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

22. Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitüberprüfungsgesetz – SÜG). URL: https://www.gesetze-im-internet.de/s_g/S%C3%9CG.pdf
23. Teleservices Data Protection Act (Teledienstedatenschutzgesetz, TDDSG). URL: http://www.iuscomp.org/gla/statutes/TDDSG.htm
24. Federal Act Governing Access to Information held by the Federal Government (Freedom of Information Act). URL: http://www.gesetze-im-internet.de/englisch_ifg/
25. Act on the Federal Office for Information Security (BSI Act – BSIG). URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf
26. Prawo pocztowe. URL: https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/prawo-pocztowe-17938059
27. Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji. URL: http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19930070034
28. Ustawa z dnia 17 maja 1989 r. o stosunku Państwa do Kościoła Katolickiego w Rzeczypospolitej Polskiej. URL: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19890290154
29. Across Europe, Nations Mold Cyber Defenses. URL: http://rpdefense.over-blog.com/across-europe-nations-mold-cyber-defenses
30. Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej. URL: https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf
31. Doktryna bezpieczeństwa informacyjnego RP – analiza syntetyczna. URL: https://obserwatorpolityczny.pl/doktryna-bezpieczenstwa-informacyjnego-rp-analiza-syntetyczna/
32. 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról. URL: https://mkogy.jogtar.hu/jogszabaly?docid=99200063.TV

33. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról. URL: https://net.jogtar.hu/jogszabaly?docid=a1100112.tv
34. 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről. URL: https://net.jogtar.hu/jogszabaly?docid=99700047.tv
35. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. URL: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv
36. Magyarország Nemzeti Biztonsági Stratégiája. URL: http://www.nemzetesbiztonsag.hu/letoltes.php?letolt=576
37. Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. URL: http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845
38. Zakon o informacijskoj sigurnosti. URL: https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti
39. Nacionalna strategija kibernetičke sigurnosti. URL: https://www.uvns.hr/hr/aktualnosti-i-obavijesti/nacionalna-strategija-kiberneticke-sigurnosti