Юридичні науки

УДК 34.096+321.01

Сопільник Любомир Іванович
доктор юридичних наук, доктор технічних наук, професор,
професор кафедри адміністративного права та процесу,
фінансового і інформаційного права
Львівський університет бізнесу та права
Сопильник Любомир Иванович
доктор юридических наук, доктор технических наук, профессор,
профессор кафедры административного права и процесса,
финансового и информационного права
Львовский университет бизнеса и права
Sopilnyk Lyubomyr
D. Sc. (Law), D. Sc. (Engineering), Professor,
Professor of the Department of Administrative Law and Process,
Financial and Information Law
Lviv University of Business and Law
ORCID: 0000-0001-6581-7255

Скриньковський Руслан Миколайович
кандидат економічних наук, доцент,
професор кафедри економіки підприємств та інформаційних технологій
Львівський університет бізнесу та права
Скрыньковский Руслан Николаевич
кандидат экономических наук, доцент,
профессор кафедры экономики предприятий и информационных технологий
Львовский университет бизнеса и права

Skrynkovskyy Ruslan
PhD in Economics, Associate Professor,
Professor of the Department of Business Economy and Information Technology
Lviv University of Business and Law
ORCID: 0000-0002-2180-8055

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

Сопільник Ростислав Любомирович
доктор юридичних наук, професор,
професор кафедри судоустрою, прокуратури та адвокатури
Львівський університет бізнесу та права
Сопильник Ростислав Любомирович
доктор юридических наук, профессор,
профессор кафедры судоустройства, прокуратуры и адвокатуры
Львовский университет бизнеса и права

Sopilnyk Rostyslav
D. Sc. (Law), Professor,
Professor of the Department of Judiciary, Prosecution and Advocacy
Lviv University of Business and Law
ORCID: 0000-0001-9942-6682

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ДОСВІД ОКРЕМИХ КРАЇН СХІДНОЇ ЄВРОПИ
ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ОПЫТ ОТДЕЛЬНЫХ СТРАН ВОСТОЧНОЙ ЕВРОПЫ
FEATURES OF PROVIDING INFORMATION SECURITY: THE EXPERIENCE OF INDIVIDUAL COUNTRIES OF EASTERN EUROPE

Анотація. *У статті розкрито особливості забезпечення інформаційної безпеки у Білорусі, Болгарії, Молдові та Румунії. З'ясовано, що з ціллю забезпечення інформаційної безпеки Україна повинна активно співпрацювати із країнами Східної Європи. Суть співпраці України із країнами Східної Європи повинна, насамперед, полягати у формуванні регіональної та міжнародної системи інформаційної безпеки, основна спрямованість функціонування якої має бути націлена на запобігання, протидію та усунення уже виниклих інформаційних загроз, зокрема таких як кіберзлочинність і кібертероризм. Визначено, що контекст співпраці має базуватися саме на стандартах Європейського Союзу та НАТО стосовно забезпечення інформаційної безпеки. Встановлено, що одним із важливих аспектів забезпечення інформаційної безпеки в Україні є врахування практичного досвіду країн Східної Європи та недопущення попередніх помилок у цьому напрямі. Це, насамперед, стосується законодавства України у сфері державної інформаційної політики та*

забезпечення інформаційної безпеки, яке потрібно удосконалювати відповідно до вимог та стандартів Європейського Союзу та НАТО, якими передбачено, що між свободою та безпекою у інформаційній сфері повинна бути рівновага.

Ключові слова: *інформаційна безпека, забезпечення інформаційної безпеки, безпека інформації, персональні дані, кібербезпека, Східна Європа.*

Аннотация. *В статье раскрыты особенности обеспечения информационной безопасности в Беларуси, Болгарии, Молдове и Румынии. Установлено, что с целью обеспечения информационной безопасности Украина должна активно сотрудничать со странами Восточной Европы. Суть сотрудничества Украины со странами Восточной Европы должна, прежде всего, заключаться в формировании региональной и международной системы информационной безопасности, основная направленность функционирования которой должна быть нацелена на предотвращение, противодействие и устранения уже возникших информационных угроз, в частности таких как киберпреступность и кибертерроризм. Определено, что контекст сотрудничества должен базироваться именно на стандартах Европейского Союза и НАТО по обеспечению информационной безопасности. Установлено, что одним из важных аспектов обеспечения информационной безопасности в Украине является учет практического опыта стран Восточной Европы и недопущения предыдущих ошибок в этом направлении. Это прежде всего касается законодательства Украины в сфере государственной информационной политики и обеспечения информационной безопасности, которое нужно совершенствовать в соответствии с требованиями и стандартами Европейского Союза и НАТО, которыми предусмотрено, что между свободой и безопасностью в информационной сфере должно*

быть равновесие.

Ключевые слова: *информационная безопасность, обеспечение информационной безопасности, безопасность информации, персональные данные, кибербезопасность, Восточная Европа.*

Summary. *The article reveals the features of providing information security in Belarus, Bulgaria, Moldova and Romania. It has been established that in order to providing information security, Ukraine should actively cooperate with the countries of Eastern Europe. The essence of Ukraine's cooperation with the countries of Eastern Europe should, first of all, be in the formation of a regional and international information security system, the main focus of the functioning of which should be aimed at preventing, countering and eliminating information threats that have already arisen, in particular, such as cybercrime and cyber terrorism. It was determined that the context of cooperation should be based precisely on the standards of the European Union and NATO for providing information security. It was found that one of the important aspects of providing information security in Ukraine is taking into account the practical experience of Eastern Europe and avoiding previous mistakes in this direction. This primarily concerns the legislation of Ukraine in the field of state information policy and information security, which needs to be improved in accordance with the requirements and standards of the European Union and NATO, which stipulate that there should be a balance between freedom and security in the information sphere.*

Key words: *information security, providing information security, the defense of information, personal data, cybersecurity, Eastern Europe.*

Постановка проблеми. Багато країн в світі, зокрема і країни Східної Європи, не мають окремих уніфікованих підходів до забезпечення інформаційної безпеки. Так, одні країни Східної Європи обирають підходи

до забезпечення безпеки інформаційної сфери, які є загальноприйнятими у країнах-членах Європейського Союзу (стосується здебільшого країн, які є членами Європейського Союзу або націлені у перспективі на членство у цьому об'єднанні), деякі з них – опираються також на специфіку і пріоритети політики та системи забезпечення інформаційної безпеки країн-членів Північноатлантичного Альянсу (НАТО), а інші – керуються загальними і/або спеціальними принципами забезпечення інформаційної безпеки у євразійських міждержавних об'єднаннях.

Що стосується України, то тут варто зазначити, що її курс спрямований на членство у Європейському Союзі та НАТО у перспективі, і сьогодні Україна є активним партнером Європейського Союзу та НАТО [1, с. 18]. Результати попередніх досліджень також доводять, що деякі країни Східної Європи мали подібну практику стосовно становлення і розвитку інформаційного суспільства.

Звідси очевидно, що для ефективного забезпечення інформаційної безпеки Україні обов'язково потрібно враховувати досвід країн Східної Європи та не допускати попередніх помилок у цьому напрямі. Це, своєю чергою, дозволить побудувати більш потужну систему захисту інформаційної сфери в Україні, оскільки останнім часом Україна все частіше стикається із інформаційними загрозами [2, с. 179] і сьогодні протистоїть інформаційній агресії з боку Російської Федерації.

Аналіз останніх досліджень і публікацій. Окремі теоретичні та практичні аспекти забезпечення інформаційної безпеки досліджувати такі науковці та практики, як О. В. Гладун [2], О. О. Климчук [3], В. С. Політанський [1], Н. А. Ткачук [3], В. Т. Шатун [2] та інші. Тут варто також відмітити, що важливі питання щодо забезпечення інформаційної безпеки країн Східної Європи розкриті у міжнародних документах [4–24]. Проте, виходячи з аналізу джерел і публікацій [1–32], сьогодні проблематика забезпечення інформаційної безпеки є недостатньо

вивченою і потребує проведення більш глибоких та конструктивних досліджень, особливо для визначення основних напрямів удосконалення інформаційної безпеки України, виходячи з реалій сьогодення.

Мета статті. Метою статті є виявлення і дослідження особливостей забезпечення інформаційної безпеки у Білорусі, Болгарії, Молдові та Румунії з метою врахування їх практичного досвіду у цьому напрямі для України.

Виклад основного матеріалу дослідження. В контексті розкриття поданої тематики першочергово слід відмітити, що такі країни, як Болгарія і Румунія – це повноправні члени Північноатлантичного Альянсу (НАТО) і Європейського Союзу. Тому у поданих країнах процес забезпечення інформаційної безпеки реалізується відповідно до стандартів НАТО та Європейського Союзу. Основні засади забезпечення інформаційної безпеки, визначених стандартами НАТО, представлені у документі С-М(2002)49 "Політика безпеки НАТО" [4].

Поряд з тим, тут доцільно зазначити, що сьогодні НАТО проводить цілеспрямовану офіційну політику стосовно усунення кіберзагроз та забезпечення кіберзахисту, основні положення якої представлені у Декларації Бухарестського саміту (Bucharest Summit Declaration) [5], яка прийнята главами держав і урядів за результатами участі у засіданні Північноатлантичної ради у м. Бухарест 3-го квітня 2008 р. В контексті цього з'ясовано, що подані положення були закладені в стратегічну концепцію оборони і безпеки учасників Організації Північноатлантичного договору (Active Engagement, Modern Defence) [6], яка прийнята головами країн і урядів у м. Лісабон 19–20-го квітня 2010 р.

Водночас варто також відмітити, що за результатами проведення Лісабонського саміту розроблено стратегічну концепцію кібербезпеки (Lisbon Summit Declaration) [7], а в контексті проведення Варшавського

саміту (Warsaw Summit Communique) [8] здійснено удосконалення стратегічної концепції кібербезпеки.

Болгарія та Румунія у національній політиці стосовно забезпечення інформаційної безпеки також керуються такими стандартами та документами Європейського Союзу, як:

– "Європейські критерії безпеки інформаційних технологій" ("Information Technology Security Evaluation Criteria") [9];

– "Єдині критерії безпеки інформаційних технологій" ("Common Criteria for Information Technology Security Evaluation") [10];

– "Мережева та інформаційна безпека: європейський політичний підхід" ("COM(2001)298 – Communication Network and Information Security: Proposal for A European Policy Approach") [11];

– "На шляху до загальної політики в сфері боротьби з кіберзлочинністю" ("Towards a general policy on the fight against cybercrime") [12].

З огляду на те (в контексті дотримання вимог стандартів та документів Європейського Союзу, представлених у джерелах [9–12]) з'ясовано, що Болгарія та Румунія у своїй політиці дотримуються таких пріоритетних напрямів забезпечення інформаційної безпеки, як:

1) підвищення рівня обізнаності користувачів стосовно виникнення можливих загроз внаслідок користування комунікативними мережами;

2) формування єдиної європейської системи щодо попередження і інформування суспільства про нові інформаційні загрози та їхній вплив;

3) досягнення технологічної підтримки;

4) забезпечення та розвиток ринково-орієнтованої сертифікації та стандартизації;

5) гарантування захисту персональних даних та протидія кіберзлочинності через удосконалення нормативно-правового забезпечення інформаційної сфери;

6) посилення інформаційної безпеки на національному рівні внаслідок впровадження на практиці сумісних та більш результативних засобів забезпечення інформаційної безпеки;

7) заохочення суспільства до використання електронних підписів внаслідок користування онлайн-послугами;

8) розвиток міжнародної співпраці у сфері забезпечення інформаційної безпеки.

Також варто зазначити, що Болгарія та Румунія на шляху забезпечення інформаційної безпеки повинні подолати низку існуючих проблем, а також [25]:

– удосконалити координовані національні підходи стосовно забезпечення безпеки інформаційних інфраструктур, це, своєю чергою, дозволить підвищити ефективність національних заходів по забезпеченню інформаційної безпеки;

– підвищити партнерство між країнами і приватним сектором відповідно до рівня провідних європейських країн;

– розширити можливості раннього реагування і попередження інформаційних та кіберзагроз;

– підвищити розвиток міждержавної співпраці і забезпечити обмін інформацією стосовно проблем, спричинених інформаційними та кіберзлочинами;

– удосконалити міжнародний консенсус стосовно пріоритетів реалізації політики забезпечення інформаційної безпеки. З'ясовано, що в цих напрямах ведеться інтенсивна робота і вже є позитивні результати.

Окрім зазначеного вище, Болгарія та Румунія, як країни-члени Європейського Союзу, значну увагу приділяють саме захисту персональних даних, при цьому, керуючись Директивою 95/46/ЄС Європейського Парламенту і Ради Європейського Союзу "Про захист фізичних осіб у зв'язку з обробкою персональних даних і вільного обігу

таких даних" [13]. Цим документом регулюються основні засади вільного переміщення інформації між країнами-членами Європейського Союзу, а також надаються гарантії стосовно захисту основних прав громадян країн-членів Європейського Союзу, які здебільшого полягають у захисті права на недоторканність особистих (персональних) даних.

В контексті розкриття поданої тематики також слід наголосити на тому, що, починаючи із 2018 р., як Болгарія, так і Румунія, а також інші країни-члени Європейського Союзу, користуються новими правилами захисту персональних даних (General Data Protection Regulation (GDPR)) [14], які було схвалено ще 14-го квітня 2016 р. Дія цих правил стосовно захисту персональних даних поширюється не тільки на компанії, які функціонують у країнах-членах Європейського Союзу, але і на інші закордонні компанії, які співпрацюють із європейськими компаніями. Так, на основі General Data Protection Regulation [14] удосконалено цивільні права користувачів, а також посилено відповідальність винних осіб за схоронність інформації. Також цим документом обмежується переміщення інформації між країнами та регламентується притягнення до суворої відповідальності за несвоєчасне повідомлення про відтік інформації (даних). На компанії, які порушили умови цього документу та протягом 72-х годин не доповіли про відтік інформації (даних) може бути накладений штраф у розмірі 4-х % річного доходу чи у сумі до 20-ти млн. євро.

Водночас варто відмітити, що за правилами GDPR [14], перш ніж здійснювати обробку персональних даних, потрібно отримати згоду користувачів (до прикладу, сьогодні є досить багато різноманітних цілей обробки персональних даних, то відповідно до них вимагається укладення різних угод про обробку персональних даних користувачів). Згода користувачів на обробку персональних даних має бути вільною, конкретною та свідомою. Однак, досить частими є випадки, коли,

наприклад, користувач повинен надати персональні дані з метою отримання доступу до сайту чи програми, то такі дії вже свідчать про те, що згода на обробку персональних даних користувача є не вільною. Як виняток, можуть бути випадки, коли вимагається від користувача подати персональні дані для того, щоб виконати певні угоди. У разі використання персональних даних для маркетингових цілей, то користувач має можливість не погоджуватися із збором та обробкою його персональних даних. На компанії, які працюють із персональними даними, накладається зобов'язання ведення обов'язкового обліку із персональними даними відповідно до принципу "data protection by desing" [15].

Поряд з проблематикою забезпечення захисту персональних даних вирішення проблем протидії кіберзагрозам у Болгарії та Румунії є також надзвичайно актуальною.

Так, у Румунії сьогодні активно проводиться процес формування та розвитку системи кібернетичної безпеки на різних рівнях. Основні функції у цьому напрямку здійснює Румунська служба інформації, у структурі якої діє спеціально створений національний центр кібербезпеки [3, с. 79–80]. Основна із функцій національного центру кібербезпеки полягає у поєднанні систем технічного захисту із наявними можливостями спецслужби з ціллю одержання інформації, необхідної для дій попередження, припинення і нейтралізації (подолання) наслідків кібератак на середовище інформаційно-комунікаційної системи [26].

Для вирішення окресленої вище проблематики у грудні 2014 р. в Румунії було розроблено Законопроект "Про кібербезпеку", який був схвалений Сенатом Румунії. Цим проектом закону передбачалося створення Національної системи кібернетичної безпеки Румунії. Обов'язок технічної координації процесу створення Національної системи кібернетичної безпеки Румунії був покладений на Румунську службу інформації, яка виступає головним суб'єктом кібербезпеки Румунії [16].

У Румунії Національною стратегією забезпечення кібербезпеки, затвердженої постановою урядом у 2013 р., передбачено, що динамічне інформаційне середовище має функціонувати на засадах функціональної сумісності та послуг, які є характерними для інформаційного суспільства. При цьому визначено, що забезпечення відповідності основних свобод та прав громадян, включаючи інтереси національної безпеки, здійснюється відповідно до спеціальних правових режимів. Також у стратегії приділена особлива увага питанню розвитку культури у напрямку забезпечення кібербезпеки користувачів комп'ютерів та телекомунікаційних систем, включаючи поінформованість користувачів про можливі ризики та загрози, які виникають у рамках їх діяльності у кіберпросторі. В контексті цього з'ясовано, що часте інформування користувачів про можливі ризики та загрози у кіберпросторі, включаючи проведення ефективних комунікацій та співпраці між усіма учасниками кіберпростору, сприятиме запобіганню та протидії кібератак та кіберзагроз. Тут доцільно також відмітити, що сьогодні Румунія виконує головну роль координатора заходів у сфері забезпечення кібербезпеки на національному рівні, дотримуючись підходів забезпечення кібербезпеки, визначених Європейським Союзом і НАТО.

З метою забезпечення кібербезпеки Румунії у Національній стратегії забезпечення кібербезпеки визначено досягнення таких цілей [17]:

1) пристосування інституціональної та нормативної основи до процесів перебігу окремих загроз у кіберпросторі;

2) формування та впровадження на практиці мінімальних вимог до забезпечення безпеки у національних кіберсистемах, якими забезпечується правильна діяльність критичної інфраструктури;

3) досягнення стійкості кіберінфраструктури;

4) досягнення кібербезпеки за рахунок усвідомлення впливу та запобігання ризикам та загрозам, зокрема загрозам у кібербезпеці;

5) формування безпеки у кіберпросторі з ціллю досягнення інтересів, цінностей і національних цілей у сфері кіберпростору;

6) формування та розвиток співпраці між державною та приватними сферами на вищому національному рівні;

7) міжнародна співпраця у сфері кібербезпеки;

8) формування культури безпеки громадян через усвідомлення впливу загроз та ризиків у сфері кіберпростору;

9) забезпечення захисту інформаційних систем;

10) активна участь у заходах посилення довіри до міжнародної сфери використання кіберпростору, які розробляються та впроваджують за ініціативи міжнародних організацій.

Своєю чергою з'ясовано, що у Болгарії функціонує Консультативна рада з питань національної безпеки. Одним із стратегічних завдань цього органу є забезпечення кібербезпеки та стабільності в контексті розвитку електронного урядування у Болгарії. Разом з тим, Консультативною радою з питань національної безпеки Болгарії передбачається також забезпечення безпеки електронної ідентичності громадян внаслідок впровадження на практиці електронного підпису. З огляду на те, у квітні 2016 р. Консультативною радою з питань національної безпеки представлено Парламенту Болгарії проект Національної стратегії кібербезпеки (до прикладу Національна стратегія кібербезпеки була прийнята у липні 2016 р. Радою міністрів Республіки Болгарії). Основними цілями цього проекту, який офіційно називається "Стійка до кібербезпек Болгарія 2020", визначено такі [18]:

1) удосконалення законодавства у сфері забезпечення інформаційної безпеки відповідно до положень Директиви Європейського Союзу та Європейського Парламенту;

2) накопичення цільових ресурсів, які є необхідними для забезпечення кібербезпеки та удосконалення стану наявної IT-інфраструктури;

3) забезпечення державних органів Болгарії, зокрема Міністерства внутрішніх справ, Міністерства оборони, Міністерства транспорту, Агентства національної безпеки та Державного агентства розвідки належними фінансовими ресурсами для поступового збільшення кількості фахівців (експертів), які забезпечуватимуть кібербезпеку та запобігатимуть кіберзагрозам;

4) організування та проведення навчання на національному рівні стосовно посилення кіберстійкості та покращення рівня ефективності наявних контрзаходів, визначених Національною стратегією кібербезпеки;

5) посилення і розширення співпраці із Європейським Союзом та НАТО у рамках забезпечення кібербезпеки;

6) покладення відповідальності на державні органи за своєчасне інформування компетентних служб про випадки виникнення кібератак.

Тут слід також відмітити, що п. 4.7.1 Національної стратегії кібербезпеки передбачено, що ключова роль у напрямку забезпечення кіберзахисту Болгарії покладається на Міністерство оборони Болгарії. Зокрема зазначається, що рівень ефективності забезпечення кібербезпеки у Болгарії залежить від існуючих і потенційних можливостей досягнення кіберзахисту, які до того, мають бути сумісними вимогам Європейського Союзу та НАТО. Так, у ході забезпечення кіберзахисту визначено такі заходи [18]:

1) розроблення та реалізація спеціальної політики у напрямку забезпечення кібербезпеки;

2) формування концепції та необхідних методичних документів стосовно захисту національної безпеки внаслідок протидії кіберзагрозам та гібридним загрозам у сфері кіберпростору;

3) впровадження на практиці ряду інвестиційних проектів, якими передбачено кіберзахист (до прикладу, опираючись на ініціативу НАТО/ЄС під назвою "Smart Defense");

4) формування належних умов для забезпечення кібероборони;

5) створення спеціального Оперативного центру кіберзахисту в рамках розвитку Збройних сил Болгарії терміном до 2020 р. із використанням на цій основі рекомендацій центру NCIRC НАТО;

6) обмін інформацією про наявні кіберзлочини через систему державних органів, інформаційні канали Європейського Союзу та НАТО тощо.

Водночас заслуговує на особливу увагу п. 7.3 Національної стратегії кібербезпеки, згідно якого у Болгарії передбачається формування і розвиток ефективних механізмів та технічних ресурсів для здійснення моніторингу потенційних загроз у кіберпросторі, їх масштабності, джерел та природи виникнення [18].

Поряд з тим, в контексті дослідження питань щодо забезпечення інформаційної безпеки країн Східної Європи, потрібно також зазначити, що у Молдові діє спеціальна система протидії кіберзагрозам. У 2009 р. Парламентом Молдови ратифіковано Конвенцію Ради Європи про кіберзлочинність (Convention on Cybercrime – Council of Europe) [19]. Окрім Конвенції Ради Європи про кіберзлочинність, у березні 2012 р. Молдовою також підписано Другий додатковий Протокол до Європейської Конвенції про взаємну допомогу у кримінальних справах (Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters) [20]. Також дещо раніше (у січні 2010 р.) Парламентом Молдови був прийнятий Закон "Про попередження та боротьбу із злочинністю у сфері комп'ютерної інформації" (LEGE privind prevenirea si combaterea criminalitatii informatice) [21]. Відповідно до положень цього закону Генеральна прокуратура Республіки Молдова наділяється

повноваженнями здійснювати та координувати кримінальне переслідування осіб, які вчиняли та вчиняють кіберзлочини. При цьому, основна мета цього закону полягає у:

1) запобіганні і боротьбі із кіберзлочинністю;

2) сприянні провайдерам та користувачам інформаційних систем;

3) співпраці державних служб з представниками громадянського суспільства та із неурядовими організаціями;

4) міжнародному співробітництві із організаціями та країнами, які мають позитивний досвід боротьби із кіберзлочинністю.

Молдова також активно впроваджує низку заходів стосовно посилення інформаційної безпеки. Так, наслідки ратифікації Конвенції Ради Європи про кіберзлочинність [19] засвідчують, що Молдова на сьогодні виступає активним учасником кримінальної політики по боротьбі із інформаційною злочинністю.

Одним із ключових кроків, який зробила Молдова у сфері забезпечення інформаційної безпеки виступає затвердження Закону Молдови "Про електронний підпис та електронний документ" [22]. Реалізуючи положення цього закону на практиці, Молдова намагається підвищити рівень безпеки електронних підписів та привести їх у відповідність до міжнародних стандартів та рекомендацій.

З ціллю забезпечення інформаційної безпеки та досягнення захисту кіберпростору у Молдові проводиться чітка регламентація функцій та повноважень міжвідомчих структур. Так, Урядом Республіки Молдова прийнято постанову, якою затверджується Національна стратегія розвитку інформаційного суспільства ("Moldova digitala 2020"), а також Міністерством інформаційних технологій розроблено План дій з впровадження Національної стратегії розвитку інформаційного суспільства [23].

Також варто наголосити, що основні засади вирішення проблеми забезпечення інформаційної безпеки у Молдові представлені у Стратегії національної безпеки Республіки Молдова та Концепції національної безпеки Республіки Молдова, у яких чітко визначені ключові цілі системи забезпечення інформаційної безпеки і заходи по усуненню загроз у інформаційній сфері [27].

Своєю чергою у Білорусі здійснення нагляду за інформаційною сферою і системою обмежень на сьогодні виступають одними із основних напрямків державної політики у системі забезпечення інформаційної безпеки. Так, спеціальними державними органами Білорусі проводиться вистежування протестних настроїв в контексті використання спеціального устаткування, яке призначене для проведення моніторингу ситуації у інформаційній сфері. До прикладу із 2010 по 2015 рр. у Білорусі діяла спеціальна Постанова Оперативно-аналітичного центру при Президентові Республіки Білорусь та Міністерства зв'язку та інформатизації Республіки Білорусь "Про затвердження Положення про порядок обмеження доступу користувачів Інтернет-послуг до інформації, забороненої до поширення відповідно законодавчих актів", згідно якої провайдери повинні фільтрувати Інтернет-контент за двома чорними списками – один із списків перебуває у відкритому доступі, а доступ до іншого мають тільки державні, культурні та урядові заклади [28].

Водночас варто відмітити, що у Білорусі ще не розроблено спеціальних законів по протидії кіберзлочинності. Однак, деякі елементи регулювання кібербезпеки представлені у Кримінальному кодексі. Слід наголосити і на тому, що Білорусь також приєдналася до Конвенції про кіберзлочинність [19] та дотримується на цій основі відповідних міжнародних стандартів, які визначені у ній. Однак, для Білорусі приєднання до Конвенції про кіберзлочинність було доволі неочікуваним, оскільки її основні зовнішні партнери-країни, такі як Росія та Китай є

головними противниками цієї конвенції, оскільки вважають, що саме держава повинна мати більше повноважень, аніж ті, які передбачаються Конвенцією про кіберзлочинність.

Контроль за розслідування кіберзлочинів (зокрема комп'ютерних злочинів) у Білорусі здійснює Міністерство внутрішніх справ. Цим Міністерством спільно із іншими виконавчими органами держави координується робота по забезпеченню інформаційної безпеки. Сучасна практика забезпечення безпеки інформаційної сфери у Білорусі засвідчує, що сьогодні у цій країні проводиться діяльність із переслідування порушників, які порушують кібербезпеку, а також активно відстежується онлайн-діяльність політичних активістів [28].

Тут варто також відмітити, що Білорусь є учасником Конвенції співробітництва держав-членів СНД у боротьбі зі злочинами, що вчиняються з використанням інформаційних технологій [29]. Ця конвенція була прийнята Радою голів держав Співдружності Незалежних Держав (СНД) ще у 2013 р.

Згідно Конвенції співробітництва держав-членів СНД у боротьбі зі злочинами, що вчиняються з використанням інформаційних технологій [29], кожна із країн-учасниць цієї конвенції обмінюється методологічною, статистичною та робочою інформацією і веде спільну базу даних стосовно кіберзлочинців. На основі цієї конвенції із 2015 р. було розроблено спеціальну програму співпраці між країнами-членами Співдружності Незалежних Держав стосовно боротьби із кіберзлочинністю. Разом з тим, у 2017 р. також розпочалося підписання нової Угоди між державами-членами Співдружності Незалежних Держав про боротьбу із злочинами, які виникають у інформаційній сфері [29], і сьогодні ведеться активна робота у цьому напрямі.

Висновки. За результатами аналізу джерел і публікацій [1–32] можна стверджувати, що сьогодні країни Східної Європи (Білорусь,

Болгарія, Молдова та Румунія) посилено працюють над вирішенням проблем забезпечення інформаційної безпеки як окремої особи, так і суспільства, у тому числі країни, загалом. Забезпечення інформаційної безпеки повинно виходити із захисту інформаційної сфери від впливу зовнішніх та внутрішніх загроз, а також має бути одним із стратегічних завдань забезпечення національної безпеки.

У ході дослідження з'ясовано, що з ціллю забезпечення інформаційної безпеки Україна повинна активно співпрацювати із країнами Східної Європи. Ця співпраця повинна насамперед полягати у формуванні регіональної та міжнародної системи інформаційної безпеки, основна спрямованість функціонування якої має бути націлена на запобігання, протидію та усунення уже виниклих інформаційних загроз, зокрема таких як кіберзлочинність і кібертероризм. При цьому, контекст співпраці має базуватися саме на стандартах Європейського Союзу та НАТО стосовно забезпечення інформаційної безпеки.

Встановлено, що одним із важливих аспектів забезпечення інформаційної безпеки в Україні є врахування практичного досвіду країн Східної Європи та недопущення попередніх помилок у цьому напрямі для України. Це, насамперед, стосується законодавства України у сфері державної інформаційної політики та забезпечення інформаційної безпеки, яке потрібно удосконалювати відповідно до вимог та стандартів Європейського Союзу та НАТО, якими передбачено, що між свободою та безпекою у інформаційній сфері повинна бути рівновага.

Література

1. Політанський В. С. Інформаційне суспільство в Україні: від зародження до сьогодення // Науковий вісник Ужгородського національного університету. Серія: Право. 2017. Вип. 42. С. 16–22.

2. Шатун В. Т., Гладун О. В. Інформаційна безпека – невід'ємна складова національної безпеки України // Наукові праці [Чорноморського державного університету імені Петра Могили комплексу "Києво-Могилянська академія"]. Серія: Державне управління. 2016. Т. 267, Вип. 255. С. 174–180.
3. 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. 75–83.
4. Security within the North Atlantic Treaty Organisation (NATO): Document C-M(2002)49, 17 June 2002 // North Atlantic Council. 2002. URL: http://www.freedominfo.org/documents/C-M(2002)49.pdf (дата звернення: 17.06.2020).
5. Bucharest Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008 // North Atlantic Treaty Organization, 03 Apr. 2008. URL: https://www.nato.int/cps/en/natohq/official_texts_8443.htm (дата звернення: 17.06.2020).
6. Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon // North Atlantic Treaty Organization, 19 Nov. 2010. URL: https://www.nato.int/cps/en/natohq/official_texts_68580.htm (дата звернення: 17.06.2020).
7. 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 (дата звернення: 17.06.2020).

8. 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 (дата звернення: 17.06.2020).
9. 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://op.europa.eu/s/obKZ (дата звернення: 17.06.2020).
10. Common Criteria for Information Technology Security Evaluation. URL: https://www.commoncriteriaportal.org/ (дата звернення: 17.06.2020).
11. 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 (дата звернення: 17.06.2020).
12. Towards a general policy on the fight against cybercrime // EUR-Lex, Publications Office of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14560 (дата звернення: 17.06.2020).
13. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних: Директива 95/46/ЄС Європейського Парламенту і Ради Європейського Союзу від 24.10.1995 р. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text (дата звернення: 17.06.2020).
14. General Data Protection Regulation (GDPR) // Inter Consulting. URL: https://gdpr-info.eu/ (дата звернення: 17.06.2020).
15. Data protection by design and default // Information Commissioner's Office. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-

gdpr/accountability-and-governance/data-protection-by-design-and-default/ (дата звернення: 17.06.2020).

16. The Senate passed the draft law regarding the cyber security of Romania // ACTMedia – Romanian Business News, December 22, 2014. URL: https://mail.actmedia.eu/daily/the-senate-passed-the-draft-law-regarding-the-cyber-security-of-romania/55734 (дата звернення: 17.06.2020).
17. Cyber security strategy of Romania // CERT-RO. URL: https://cert.ro/vezi/document/NCSS-Ro (дата звернення: 17.06.2020).
18. Simonski K., Sharkov G. National Cyber Security Strategy – Cyber Resilient Bulgaria 2020. Council of Ministers, 2016. URL: http://infosec-journal.com/article/national-cyber-security-strategy-cyber-resilient-bulgaria-2020 (дата звернення: 17.06.2020).
19. Convention on Cybercrime. Council of Europe, Budapest, 23.11.2001 // Council of Europe Portal. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (дата звернення: 17.06.2020).
20. Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters. Council of Europe, Strasbourg, 08.11.2001 // Council of Europe Portal. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/182 (дата звернення: 17.06.2020).
21. LEGE privind prevenirea si combaterea criminalitatii informatice Nr. 20-XVI din 03.02.2009. Parlamentului Republicii Moldova. URL: http://old.mtic.gov.md/sites/default/files/legi/20_03.02.2009_lege_privind_prevenirea_si_combaterea_criminalitatii_informatice.pdf (дата звернення: 17.06.2020).
22. LEGE privind semnatura electronica si documentul electronic Nr. 91 din 27.06.2014. Parlamentul Republica Moldova. URL:

https://www.legis.md/cautare/getResults?doc_id=112497&lang=ro (дата звернення: 17.06.2020).

23. HOTARIRE cu privire la Programul national de securitate cibernetica a Republicii Moldova pentru anii 2016–2020 Nr. 811 din 29.10.2015. Guvernul Republicii Moldova. URL: http://old.mtic.gov.md/sites/default/files/legi/_ro_hg-nr-811-din-29.10.2015.pdf (дата звернення: 17.06.2020).
24. Концепция сотрудничества государств – участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий: Одобрена Решением Совета глав государств Содружества Независимых Государств (СНГ) от 25 октября 2013 года, г. Минск. URL: http://cis.minsk.by/reestr/ru/index.html#reestr/view/text?doc=4008 (дата звернення: 17.06.2020).
25. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection. Commission the European Communities, Brussels, 30.03.2009 URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF (дата звернення: 17.06.2020).
26. Cyberintelligence // Serviciul Roman de Informatii. URL: https://www.sri.ro/cyberint (дата звернення: 17.06.2020).
27. Обзор: Информационная безопасность и защита информации в Молдове // Digital.Report, 03.06.2017. URL: https://digital.report/moldova-informatsionnaya-bezopasnost/ (дата звернення: 17.06.2020).

28. Обзор: Информационная безопасность и защита информации в Беларуси // Digital.Report, 01.06.2017. URL: https://digital.report/belarus-informatsionnaya-bezopasnost/ (дата звернення: 17.06.2020).
29. Страны СНГ будут сотрудничать в борьбе с киберпреступностью // Ритм Евразии, 28.08.2017. URL: https://www.ritmeurasia.org/news--2017-08-28--strany-sng-budut-sotrudnichat-v-borbe-s-kiberprestupnostu-32043 (дата звернення: 17.06.2020).
30. Ткачук Т. Ю. Забезпечення інформаційної безпеки: досвід окремих країн Східної Європи // Інформація і право. 2017. № 4. С. 62–72.
31. Солодка О. М. Пріоритети удосконалення інформаційної безпеки України // Інформація і право. 2015. № 3 (15). С. 36–42.
32. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави: монографія / заг. ред. Р. А. Калюжний. Центр навчально-наукових та науково-практичних видань Національної академії Служби безпеки України, 2014. 196 с.