Інформаційна і національна безпека

УДК 342.4:327.7

ТКАЧУК Т.Ю., *кандидат юридичних наук, доцент*, заступник завідувача кафедри організації захисту інформації з обмеженим доступом Навчально-наукового інституту інформаційної безпеки Національної академії СБ України

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ДОСВІД ОКРЕМИХ КРАЇН СХІДНОЇ ЄВРОПИ

Анотація. *Стаття присвячена дослідженню питань забезпечення інформаційної безпеки у країнах Східної Європи. В ході дослідження визначаються пріоритети та проблеми забезпечення інформаційної безпеки у вказаних країнах. Також оцінюється значущість досвіду країн Східної Європи у сфері забезпечення інформаційної безпеки для України.*

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

Summary. *The article is devoted to the research of the information security subject in the countries of Eastern Europe. The study identifies priorities and problems of ensuring information security in these countries. The importance of the experience of Eastern European countries in the field of information security for Ukraine is also assessed.*

Keywords: *information security, the defense of information, personal data, cybersecurity, Eastern Europe.*

Аннотация. *Статья посвящена исследованию вопросов обеспечения информационной безопасности в странах Восточной Европы. В ходе исследования определяются приоритеты и проблемы обеспечения информационной безопасности в указанных странах. Также оценивается значимость опыта стран Восточной Европы в сфере обеспечения информационной безопасности для Украины.*

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

Постановка проблеми. Підходи до забезпечення інформаційної безпеки, прийняті у країнах Східної Європи, наразі не є уніфікованими, що зумовлено геополітичною специфікою відповідних країн, одні з яких входять до Північноатлантичного Альянсу (НАТО) та Європейського Союзу (ЄС), інші – прямують до членства у вказаних організаціях, а деякі – входять до євразійських міждержавних утворень. Обравши євроінтеграційний курс та визначивши вступ до НАТО своїм стратегічним пріоритетом, Україна має орієнтуватися передусім на стратегію розвитку країн-учасниць ЄС та НАТО в інформаційній сфері [1, с. 18]. Втім, не менш важливим є і досвід інших країн Східної Європи, які проходять аналогічний шлях у процесі становлення та розвитку інформаційного суспільства. Тож дослідження, оцінка та імплементація позитивного досвіду східноєвропейських країн мають важливе значення при розбудові системи забезпечення інформаційної безпеки в Україні, оскільки події останніх років в нашій державі показали, що наша країна поки що не готова протистояти інформаційним війнам, а її політика у сфері забезпечення інформаційної безпеки та інформаційна політика в цілому потребує вдосконалення [2, с. 179].

Результати аналізу наукових публікацій. Проблематику інформаційної безпеки у країнах Європи, в тому числі – у східноєвропейських, досліджували у своїх роботах О. Запорожець, О. Климчук, С. Лазовський, Р. Лук’янчук, О. Павловська, В. Петров, А. Руснак. Дослідженням інформаційної безпеки України у контексті світового досвіду займалися І. Беззуб, О. Довгань, 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 Східної Європи та доцільності використання їх досвіду для України поки що недостатньо висвітлені у науковій літературі.

Метою статті є дослідження питань забезпечення інформаційної безпеки у країнах Східної Європи, а також оцінка значущості для України досвіду країн Східної Європи у цій сфері.

Виклад основного матеріалу. З точки зору забезпечення інформаційної безпеки у Східній Європі доцільно буде визначити репрезентативними країни різних геостратегічних спрямувань, тому в рамках цієї статті пропонуємо зосередитись на огляді питань забезпечення інформаційної безпеки у Румунії, Болгарії, Молдові та Білорусі.

Передусім зауважимо, що Румунія та Болгарія є членами Північноатлантичного Альянсу та Європейського Союзу. Відповідно, на них поширюються стандарти цих міжнародних організацій щодо інформаційної політики та забезпечення інформаційної безпеки. Це, зокрема, стандарти НАТО щодо захисту інформації, викладені у Документі СМ (2002)49 “Безпека в організації Північноатлантичного договору (НАТО)” [3], офіційна політика НАТО у сфері кіберзахисту [4 – 5], стратегічна концепція кібербезпеки, сформульована за результатами Лісабонського саміту [6] й уточнена за результатами Варшавського саміту [7] тощо. Також Румунія та Болгарія, як країни-члени ЄС, втілюють у національній політиці забезпечення інформаційної безпеки стандарти ЄС, в тому числі передбачені “Європейськими критеріями безпеки інформаційних технологій” (1991 р.) [8], “Єдиними критеріями безпеки інформаційних технологій” (1996 р.) [9], документом “Мережева та інформаційна безпека: європейський політичний підхід” (2001 р.) [10], документом “На шляху до загальної політики в сфері боротьби з кіберзлочинністю” (2007 р.) [11] тощо. Відповідно, основними напрямами забезпечення інформаційної безпеки у вказаних країнах є: 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. Основними викликами інформаційній безпеці Румунії та Болгарії, як 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 [12].

Одним з найбільш важливих питань політики інформаційної безпеки Румунії та Болгарії, як країн-членів ЄС, є захист персональних даних, в якому вони керуються положеннями Директиви 95/46/ЄС “Про захист фізичних осіб у зв’язку з обробкою персональних даних і вільного обігу таких даних”. 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 [13 – 14]. Крім того, з 2018 року для Румунії та Болгарії, як і інших країн-членів ЄС, набудуть чинності нові правила захисту персональних даних (GDPR), які схвалено 14 квітня 2016 року. 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 з моменту виявлення інциденту, загрожує штраф до 4 % річного доходу або до 20 млн. євро [15]. 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 згоду, 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 з 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 [16].

Не менш гостро, ніж проблема захисту персональних даних, у Румунії та Болгарії усвідомлюється небезпечність загроз, що виходять з кіберпростору.

Так, у Румунії на сьогоднішній день активно триває процес розбудови системи кібернетичної безпеки держави як на законодавчому, так і на організаційному рівнях. При цьому ключова роль у забезпеченні кібербезпеки Румунії відводиться її спеціальному контррозвідувальному органу – Румунській службі інформації, у структурі якої створено національний центр кібербезпеки [17, с. 79-80]. Головною функцією цього центру є поєднання систем технічного захисту із можливостями спецслужби з метою отримання інформації, необхідної для попередження, припинення та подолання наслідків кібератак на інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури держави [18]. Законопроект “Про кібербезпеку”, який у грудні 2014 року був схвалений сенатом Румунії, також передбачає створення Національної системи кібернетичної безпеки Румунії, технічну координацію якої покладено на Румунську службу інформації як головного суб’єкта кібербезпеки держави [19].

Національна стратегія забезпечення кібербезпеки Румунії (2013 р.) при цьому передбачає, що Румунія забезпечує функціонування динамічного інформаційного середовища на основі функціональної сумісності й послуг, характерних для інформаційного суспільства, а також забезпечення відповідності основних прав і свобод громадян та інтересів національної безпеки у відповідних правових рамках. Важливим

для цього є розвиток культури кібербезпеки користувачів комп’ютерів і телекомунікаційних систем, їх поінформованість щодо потенційних ризиків, а також про можливості їх мінімізації. Збільшення поінформованості щодо ризиків і загроз, пов’язаних з діяльністю, здійснюваною в кіберпросторі, а також способів запобігання та протидії їм вимагають ефективної комунікації й співробітництва між всіма учасниками діяльності у цій сфері, тож Румунська держава бере на себе роль координатора заходів, здійснюваних на національному рівні, забезпечуючи кібербезпеку відповідно до визначених під керівництвом ЄС і НАТО підходів.

З метою забезпечення кібербезпеки Румунії Стратегія визначає наступні цілі: адаптація нормативного й інституціонального підґрунтя до динаміки конкретних загроз у кіберпросторі; встановлення й застосування мінімальних профілів і вимог безпеки для національних кіберсистем, що забезпечують правильну роботу критичної інфраструктури; забезпечення стійкості кіберінфраструктури; забезпечення безпеки шляхом усвідомлення й запобігання уразливостям та ризикам, а також протидії загрозам кібербезпеці Румунії; використання можливостей кіберпростору для просування інтересів, цінностей та національних цілей в кіберпросторі; сприяння та розвиток співробітництва між державним і приватним секторами на національному рівні, а також міжнародне співробітництво у сфері кібербезпеки; розвиток культури безпеки населення шляхом усвідомлення уразливостей, ризиків і загроз з кіберпростору та необхідності захисту власних інформаційних систем; активна участь в ініціативах міжнародних організацій, учасницею яких є Румунія, в рамках реалізації комплексу заходів щодо зміцнення довіри до міжнародного використання кіберпростору. Особливу увагу Стратегія приділяє розвитку національних можливостей щодо управління ризиками у сфері кібернетичної безпеки [20].

На думку Консультативної ради з питань національної безпеки Болгарії, кібербезпека і стабільність мають стратегічне значення для розвитку електронного урядування в Болгарії й досягнення оперативної сумісності в роботі адміністрації в цифровому середовищі шляхом введення загальних стандартів. Відповідно, необхідно прискорене впровадження комплексу заходів щодо забезпечення безпеки електронної ідентичності громадян, а також щодо забезпечення захищеної й оптимізованої сумісності електронної ідентичності з такими компонентами, як електронний підпис. Тож у квітні 2016 року Консультативна рада представила Парламенту Болгарії проект Національної стратегії кібербезпеки під назвою “Стійка до кібератак Болгарія 2020”, яка передбачає реалізацію наступних заходів: ініціювання законодавчих змін з метою остаточного прийняття й транспонування Директиви ЄС і Європейського Парламенту про заходи щодо забезпечення високого загального рівня мережної й інформаційної безпеки в ЄС, а також для захисту політичних і виборчих прав громадян і в кіберпросторі; забезпечення цільових ресурсів, необхідних для створення належного потенціалу для кібербезпеки та удосконалення ІТ-інфраструктури, а також реалізації мережної моделі обміну інформацією й координації між організаціями, відповідальними за кібербезпеку у Болгарії; забезпечення Міністерства внутрішніх справ, Агентства національної безпеки, Міністерства оборони, Міністерства транспорту й Державного агентства розвідки необхідними фінансовими ресурсами з поступовим збільшенням числа експертів з питань кібербезпеки для запобігання й боротьби з кіберзагрозами; організація й проведення національних навчань з кіберстійкості з тестуванням ключових елементів Національної стратегії кібербезпеки й ефективності чинних контрзаходів; зміцнення співробітництва з ЄС і НАТО щодо забезпечення кібербезпеки; покладання на державні установи обов’язку щодо вчасного інформування компетентних служб

щодо фактів здійснених на них кібератак. Національна стратегія була прийнята Радою міністрів Республіки Болгарії 13 липня 2016 року.

Відповідно до п. 4.7.1 Національної стратегії, провідну роль у забезпеченні кіберзахисту країни відіграє Міністерство оборони Болгарії. Ефективне забезпечення кібербезпеки при цьому передбачає розбудову існуючих та створення нових розширених можливостей для кіберзахисту, сумісних з вимогами НАТО і ЄС, а також проведення адекватних структурних і організаційних реформ, зокрема: розробку політики у сфері забезпечення кібербезпеки, розробку відповідної концепції й методичних документів, що передбачають захист національної безпеки шляхом активної протидії кібер- і гібридним загрозам у кіберпросторі; реалізацію інвестиційних проектів для кіберзахисту у рамках спільних ініціатив, у тому числі ініціативи НАТО/ЄС “Smart Defense” та “об’єднання й спільного використання”, а також створення можливостей для кібероборони в рамках загального процесу планування у сфері оборони; створення Оперативного центру кіберзахисту відповідно до плану розвитку Збройних сил Болгарії до 2020 року за допомогою центру NCIRC НАТО із забезпеченням безперервного моніторингу і повної оперативної інтеграції в національну мережу NKOMKS, розвиток колективного потенціалу реагування на кібер- і гібридні загрози на національному й міжнародному рівні; погоджений обмін інформацією про кіберінциденти за допомогою державних установ, НАТО і ЄС, а також співробітництво з діловими й науковими колами; накопичення досвіду у сфері кіберзахисту й підвищення професійної підготовки персоналу шляхом періодичної підготовки й участі в навчаннях, розширення участі у роботі центру кіберзахисту НАТО та інших партнерських центрів; удосконалювання й розвиток взаємодії із промисловістю й науково-дослідними організаціями на основі “кластерної кібероборони”; активну участь у міжнародних програмах НАТО і ЄС у рамках науково-дослідних проектів; адаптація й впровадження моделі ES75 щодо спільного використання ресурсів на національному рівні для професіоналів, інші форми залучення експертів з кіберпромисловості та наукових кіл. Пункт 7.3 Стратегії передбачає створення механізмів і технічних ресурсів для постійного моніторингу можливих загроз кібербезпеці з точки зору масштабів, джерел і природи (кібер-, гібридні), тенденцій у геополітичному контексті й аналізу національної картини кібербезпеки, а також розвитку здатності застосовувати адекватні форми протидії, в т.ч. підтримувати створення джерел контр-інформаційних впливів [21].

Незважаючи на критику політики забезпечення інформаційної безпеки у наукових колах [22, с. 63], у Молдові діє відносно надійна система протидії кіберзлочинності. Так, ще у 2009 році Парламентом була ратифікована Конвенція Ради Європи про кіберзлочинність [23]. Крім того, влада Молдови підписала Другий додатковий Протокол до Європейської Конвенції про взаємну допомогу у кримінальних справах у березні 2012 року [24]. Парламентом також був прийнятий Закон “Про попередження та боротьбу зі злочинністю у сфері комп’ютерної інформації” у січні 2010 року [25]. Згідно із цим Законом генпрокуратура Молдови наділена повноваженнями координувати й здійснювати кримінальне переслідування осіб, що вчинили кіберзлочини. Метою Закону є вдосконалення регламентації правовідносин за такими напрямками: запобігання та боротьба з кіберзлочинністю, сприяння провайдерам і користувачам інформаційних систем, співробітництво державних служб із неурядовими організаціями та іншими представниками громадянського суспільства, а також міжнародне співробітництво з організаціями й країнами, що мають досвід у відповідних питаннях. Генеральною прокуратурою з метою сприяння розслідуванням був відкритий Центр розслідування

кіберзлочинів, один з відділів якого уповноважений реагувати на випадки загроз безпеці в урядових структурах, бізнесі й громадському секторі.

Також у Молдові здійснено низку інших заходів щодо зміцнення інформаційної безпеки. Так, у результаті ратифікації Факультативного протоколу до Конвенції ООН про права дитини, що стосується торгівлі дітьми, дитячої проституції й порнографії [26], Конвенції Ради Європи про кіберзлочинність [23] й Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства [27], Молдова стала активним учасником процесу застосування загальної кримінальної політики у сфері боротьби з інформаційною злочинністю, у тому числі злочинами, пов’язаними із онлайн-експлуатацією дітей.

Важливим кроком на національному рівні стало також затвердження Закону Молдови “Про електронний підпис та електронний документ” від 29 травня 2014 року, розробленого з метою підвищення рівня безпеки електронних підписів та приведення у відповідність із міжнародними стандартами й рекомендаціями щодо інфраструктури відкритих ключів [28]. В цілому слід зауважити, що у Молдові розпочато процес приведення чинного законодавства у відповідність до положень Директиви 2006/24/ЄС “Про зберігання інформації, створеної або обробленої при наданні послуг зв’язку загального користування або мереж зв’язку загального користування й внесення змін у Директиву ЄС 2002/58/ЄС” від 15 березня 2006 року щодо захисту персональних даних [29], Директиву 2008/114/ЄС “Про ідентифікацію й призначення європейських критичних інфраструктур і заходах з їх захисту” від 8 грудня 2008 року [30] тощо.

З метою забезпечення системного підходу й формування державної політики у сфері забезпечення інформаційної безпеки, яка об’єднала б правові, організаційні, технічні, технологічні й фізичні заходи щодо захисту кіберпростору Молдови, а також чіткої регламентації функцій і повноважень підвідомчих структур, Уряд Республіки Молдова Постановою від 31 жовтня 2013 року № 857 затвердив Національну стратегію розвитку інформаційного суспільства “Moldova digitală 2020” (Цифрова Молдова 2020) і План дій з її впровадження, розроблений Міністерством інформаційних технологій та зв’язку [31]. У Стратегії вперше розглядається проблема створення умов для підвищення ступеня безпеки й довіри до кіберпростору, а ключові дії щодо створення цих умов становлять окрему главу вищезгаданого Плану дій. Стратегія визначає, що використання нових технологій породжує численні можливості розвитку, але й численні ризики й уразливості, що вимагають підвищеної уваги держави й зацікавлених учасників. Ці ризики характеризуються асиметрією, вираженою динамікою й глобальним характером, що ускладнює їхнє виявлення й протидію за допомогою заходів, пропорційних до ефекту їхньої матеріалізації. То ж попередження і боротьба з кібератаками, у тому числі зі злочинністю в цій сфері є одним із пріоритетів міжнародних організацій, а їх бурхливий ріст на світовому рівні на 600 % з 2005 року вказує на нагальну необхідність вжиття заходів щодо страхування інформаційної інфраструктури Республіки Молдова від можливих ризиків, пов’язаних з незаконною діяльністю у цій сфері. Важливість цієї проблеми була відзначена у Концепції національної безпеки й Стратегії національної безпеки Республіки Молдова, у яких були встановлені цілі системи забезпечення національної безпеки та загрози у інформаційній сфері [32].

Проект Концепції інформаційної безпеки, схвалений Парламентом Молдови в першому читанні 23 червня 2017 року, викликав у суспільстві неоднозначну реакцію. На думку експертів, останні ініціативи щодо регламентації інформаційного простору містять цілу низку серйозних прогалин, які можуть призвести до зловживань. Зокрема, Концепцію інформаційної безпеки доцільно узгодити із новою Стратегією національної

безпеки, однак останній проект Стратегії національної безпеки в червні 2017 року був відкликаний з Парламенту Президентом, а новий проект досі не розроблений. Крім того, проект Концепції припускає занадто суворий контроль Інтернету з боку деяких держустанов, зокрема Служби інформації та безпеки Республіки Молдова, які зможуть втручатися в діяльність провайдерів, а також контролювати інформаційний простір, включаючи соціальні мережі. Однак, з урахуванням того, що населення дедалі активнвше користується Інтернетом, і на цьому тлі влада починає втрачати контроль над інформацією, це не єдина законодавча ініціатива у сфері інформаційної безпеки, захисту інформації, протистояння кіберзлочинності й боротьби зі зловживаннями в Інтернеті – серед таких ініціатив слід згадати, зокрема, законопроект № 161, більш відомий як “Великий брат”, і законопроект № 281, що одержав назву “Мандат безпеки”, який уточнює правила проведення спеціальних розшукових заходів в інформаційному просторі й припускає розширення повноважень спеціальних служб у цій сфері. За оцінками фахівців, спроби держави встановити контроль над інформаційними мережами у спосіб, який передбачається цими законопроектами, не стільки забезпечать ефект безпеки інформаційного простору, скільки вдарить по громадянському суспільству, політичних партіях, простих громадянах, яким обмежать можливості висловлювати свою думку й критичні зауваження на адресу влади [33].

У Білорусі нагляд за інформаційним простором та система обмежень наразі є ключовими елементами державної політики забезпечення інформаційної безпеки, зокрема, державні органи відстежують протестні настрої за допомогою складного російського устаткування для моніторингу, впровадженого телекомунікаційними компаніями. З 2010 до 2015 року у країні діяла Постанова Оперативно-аналітичного центру при Президентові Республіки Білорусь і 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” від 29.06.10 р. № 4/11, за змістом якої провайдери мали фільтрувати Інтернет-контент відповідно до двох чорних списків url-адрес, один з яких перебував у публічному доступі, а інший – був доступний тільки провайдерам (закритий список містив приблизно 80 url-адрес, доступ до яких було обмежено у державних, культурних і урядових закладах, і включав популярні опозиційні сайти на кшталт Charter97.org і Belaruspartisan.org) [34]. Наразі ж відповідні обмеження реалізуються відповідно до Указу Президента Республіки Білорусь “Про заходи щодо вдосконалення використання національного сегменту мережі Інтернет” від 01.02.10 р. № 60, Декрету Президента Республіки Білорусь “Про невідкладні заходи з протидії незаконному обігу наркотиків” від 28.12.14 р. та Закону Республіки Білорусь “Про засоби масової інформації” від 17.07.08 р. [35].

У березні 2010 року від білоруських провайдерів зажадали більш тісного співробітництва з державними системами спостереження (СОРМ), які здійснює повний он-лайн-нагляд у всій країні, що регламентується значною кількістю нормативно-правових актів. Як і в Росії та сусідніх країнах, СОРМ Білорусі дає виконавчим органам і органам національної безпеки можливість здійснювати перехоплення повідомлень з будь-яких комунікаційних каналів з метою боротьби зі злочинністю. Провайдери Інтернет-послуг і оператори зв’язку зобов’язані встановлювати відповідне устаткування й надавати державним органам цілодобовий доступ до нього. Відповідно до Указу Президента Республики Беларусь “Про заходи щодо вдосконалення використання національного сегменту мережі Інтернет” від 01.02.10 р. № 60 [36], провайдери повинні вести облік IP-адрес, а держава може витребувати інформацію щодо Інтернет-діяльності будь-якого громадянина. З 2007 року до Інтернет-кафе пред’являється вимога зберігати

історію Інтернет-активності користувачів протягом одного року й інформувати виконавчі органі про підозрілі дії [34]. СОРМ працює, головним чином, відповідно до Закону “Про оперативно-розшукову діяльність” [37], Закону “Про органи державної безпеки Республіки Білорусь” [38] та Указу “Про затвердження Положення про порядок взаємодії операторів електрозв’язку з органами, що здійснюють оперативно-розшукову діяльність” № 129 [39].

У Білорусі немає спеціальних законів, присвячених протидії кіберзлочинності, але деякі аспекти регулюються Кримінальним кодексом і законами, що стосуються регламентації діяльності глобальної інформаційної мережі Інтернет. Білорусь також подавала заявку на приєднання до Конвенції про кіберзлочинність, прийнятої в Будапешті в 2012 році [23], що й визначило необхідність дотримуватись відповідних міжнародних стандартів. Це був доволі неочікуваний для Білорусі крок, особливо у контексті тісних зв’язків з Росією, адже Китай і Росія виступили проти конвенції й висловилися на захист альтернативної концепції боротьби з кіберзлочинністю, у рамках якої держава одержувала значно більше повноважень, ніж це передбачалося Будапештською конвенцією.

За розслідування комп’ютерних злочинів у Білорусі відповідає спеціальне управління Міністерства внутрішніх справ, яке координує роботу з іншими виконавчими органами в Білорусі й аналогічними міжнародними організаціями в США, Євросоюзі, країнах СНД і в інших державах. У суспільстві висловлюються непоодинокі підозри, що це управління має справу здебільшого з переслідуванням порушників кримінального кодексу й не займається розробкою законодавства з питань кібербезпеки, а також бере участь у переслідуванні та он-лайн-відстеженні політичних активістів [34].

Що стосується участі Республіки Білорусь у забезпеченні кібербезпеки на регіональному рівні, слід зауважити, що Рада голів держав Співдружності Незалежних Держав (СНД) у 2013 році прийняла Концепцію співробітництва держав-членів СНД у боротьбі зі злочинами, що вчиняються з використанням інформаційних технологій [40]. Відповідно до цього документу країни-члени СНД обмінюються робочою, статистичною й методологічною інформацією та ведуть єдину базу даних щодо кіберзлочинців. На підставі цієї Концепції з 2015 року здійснюється розробка програми співробітництва між країнами СНД у боротьбі з кіберзлочинністю, яка підлягає затвердженню Радою Міністрів країн СНД. Також у 2017 році розпочато підписання нової Угоди про співробітництво держав-членів СНД у боротьбі зі злочинами у сфері інформаційних технологій [41].

Висновки.

Наразі країни Східної Європи вважають вирішення проблеми забезпечення інформаційної безпеки особи, суспільства, держави, їх захисту від внутрішніх та зовнішніх, у тому числі гібридних загроз, одним з найбільш важливих стратегічних пріоритетів забезпечення національної безпеки.

Україна має співпрацювати з іншими країнами Східної Європи у розбудові систем регіональної та міжнародної інформаційної безпеки з метою протидії загрозам стратегічній стабільності, таким, як кібертероризм та кіберзлочинність, орієнтуючись при цьому на стандарти ЄС та НАТО.

В цьому контексті для України є важливим досвід країн Східної Європи щодо приведення національного законодавства у відповідність до вимог вказаних міжнародних організацій, передусім – щодо забезпечення балансу між свободою й безпекою в інформаційній сфері на законодавчому рівні.

Використана література

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

2. Шатун В.Т., Гладун О.В. Інформаційна безпека – невід’ємна складова національної безпеки України // Наукові праці. Державне управління. – Вип. 255. – Т. 267. – 2016. – С. 174-180.

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

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

5. 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

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

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

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

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

10. 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

11. 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

12. 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

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

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

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

16. Персональные данные : новые правила в Европейском Союзе. – Режим доступу : https://habrahabr.ru/post/300348

17. 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.

18. Cyberintelligence : [Online tool]. – Available at : https://www.sri.ro/cyberintelligence-en.html

19. The Senate passed the draft low regarding the cyber security of Romania : [Online tool]. – Available at: http://actmedia.ua/daily/the-senate-passed-the -draft-law-regarding-the ceber-security-of-romania/55734

20. Romania’s Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber Security (2013) : [Online tool]. – Available at : https://www.cert.ro/vezi/document/ strategia-de-securitate-cibernetica

21. National Cyber Security Strategy : Cyber Resilient Bulgaria 2020 (2016) : [Online tool]. – Available at : https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/Cybersecurity%20Forum%20Bulgaria/Bulgaria_sharkov_todorov.pdf

22. Руснак А.К. Молдова и информационная безопасность // SECURITATEA INFORMATIONALĂ 2011 : Conferinţa Internaţională, ediţia a VIII-a, 4 mai 2011. – P. 62-63.

23. Конвенція про кіберзлочинність від 23 листопада 2001 року. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/994_575

24. Другий додатковий Протокол до Європейської Конвенції про взаємну допомогу у кримінальних справах від 08 листопада 2001 року. – Режим доступу : http://zakon.rada.gov.ua/laws/show/994_518

25. Lege Nr. 20 din 03.02.2009 Privind prevenirea şi combaterea criminalităţii informatice : [Online tool]. – Available at : http://lex.justice.md/viewdoc.php?action=view&view=doc&id=333508&lang=1

26. Про права дитини, що стосується торгівлі дітьми, дитячої проституції й порнографії : Факультативний протокол до Конвенції ООН від 01 січня 2000 року. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/995_b09

27. Про захист дітей від сексуальної експлуатації та сексуального насильства : Конвенція Ради Європи від 25 жовтня 2007 року. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/ 994_927

28. Lege Nr. 91 din 29.05.2014 Privind semnătura electronică şi documentul electronic : [Online tool]. – Available at : http://lex.justice.md/viewdoc.php?action=view&view=doc&id=353612 &lang=1

29. Про збереження даних, створених або оброблених при наданні загальнодоступних послуг електронних повідомлень або громадських мереж зв’язку, та внесення поправок в Директиву 2002/58/ЄС : Директива 2006/24/ЄС Європейського парламенту та Ради Європи від 15 березня 2006 року. – Режим доступу : https://ain.ua/2009/10/27//директива-ес-о-сохранении-данных-укр

30. О европейских критических инфраструктурах и мерах по их защите : Директива 2008/114/ЕС Европейского парламента и Совета Європы от 08 декабря 2008 года. – Режим доступу : http://docs.pravo.ru/document/view/32671965/

31. HOTĂRÎRE Nr. 811 din 29.10.2015 Cu privire la Programul national de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 : [Online tool]. – Available at: http://lex.justice.md/viewdoc.php?action=view&view=doc&id= 361818&lang=1

32. Молдова : Национальный ИКТ-профайл. – (Информационная безопасность и защита информации). – Режим доступу : https://digital.report/moldova-informatsionnaya-bezopasnost

33. Мнения экспертов Молдовы : Законопроекты в области информационной безопасности противоречат друг другу, то есть ведут к злоупотреблениям. – Режим доступу : http://www.allmoldova.com/ru/project/mnenie/mnieniia-ekspiertov-moldovy-zakonoproiekty-v-oblasti-informatsionnoi-biezopasnosti-protivoriechat-drugh-drughu-to-iest-viedut-k-zloupotrieblieniiam

34. Беларусь : Национальный ИКТ-профайл. – (Информационная безопасность и защита информации). – Режим доступу : https://digital.report/belarus-informatsionnaya-bezopasnost

35. О признании утратившим силу постановления Оперативно-аналитического центра при Президенте Республики Беларусь и Министерства связи и информатизации Республики Беларусь от 29 июня 2010 года № 4/11 : Постановление Оперативно-аналитического центра при Президенте Республики Беларусь и Министерства связи и информатизации Республики Беларусь от 19 февраля 2015 года № 7/7. – Режим доступу : http://www.pravo.by/upload/docs/op/T21503058_1424811600.pdf

36. О мерах по совершенствованию использования национального сегмента сети Интернет : Указ Президента Республики Беларусь от 01 февраля 2010 года № 60. – Режим доступу : http://pravo.by/ document/?guid=3871&p0=P31000060

37. Об оперативно-розыскной деятельности : Закон Республики Беларусь от 15 июля 2015 года № 307-З. – Режим доступу : http://kgb.by/ru/zakon289-3

38. Об органах государственной безопасности Республики Беларусь : Закон Республики Беларусь от 10 июля 2012 года № 390-З. – Режим доступу : http://kgb.by/ru/zakon390-3

39. Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность : Указ Президента Республики Беларусь от 03 марта 2010 года № 129. – Режим доступу : http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm

40. Концепция сотрудничества государств-участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий : утверждена Решением Совета глав государств СНГ от 25 октября 2013 года. – Режим доступу : http://www.e-cis.info/page.php?id=23808

41. Страны СНГ будут сотрудничать в борьбе с киберпреступностью. – Режим доступу : https://www.ritmeurasia.org/news--2017-08-28--strany-sng-budut-sotrudnichat-v-borbe-s-kiberprestupnostu-32043

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~