УДК 343.543

ПОЛІТИКА ДЕРЖАВ СХІДНОГО ПАРТНЕРСТВА ЩОДО ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРЗАГРОЗ

Петров Валентин Володимирович,
кандидат політичних наук

Проаналізовано досвід країн Східного партнерства щодо організації на національному рівні захисту критичної інфраструктури від кіберзагроз. Запропоновані практичні рекомендації щодо можливого впровадження цього досвіду в Україні.

Ключові слова: **національна безпека, кібербезпека, кіберпростір, критична інфраструктура, мережа Інтернет, кіберінциденти.**

Східне партнерство (СП) охоплює регіон політичних, економічних, енергетичних, екологічних та безпекових впливів на східному напрямі Європейського Союзу (ЄС), що набув офіційного статусу у травні 2009 р. Політика СП має на меті зміцнення стосунків ЄС із 6 східними сусідами та є продовженням східного напрямку Європейської політики сусідства.

Одним із чільних напрямів СП є підписання угод про асоціацію, які включають домовленості про зону вільної торгівлі між ЄС і кожною із 6-ти країн-партнерів, зокрема і з Україною. Особливий наголос робиться на співпраці з метою посилення боротьби з корупцією, організованою злочинністю, нелегальною міграцією тощо. Разом з тим менш виразно заявлені напрями безпекової співпраці, що стосуються захисту критичної інфраструктури (КІ) з використанням накопиченого досвіду і ЄС загалом, і партнерських країн.

Тому **метою даної статті** є аналіз сучасного стану забезпечення такого важливого сегмента національної безпеки, як КІ, зокрема й кібернетичної та інформаційної безпеки. Про актуалізацію загроз у цій сфері свідчить передусім політична конфліктність як у самій Україні, так і довкола неї на тлі підписання Україною Угоди про асоціацію з ЄС. Саме це геоекономічне та геополітичне тло зумовлює необхідність аналізу досвіду в даній сфері держав СП, до яких належить і Україна, та опрацювання шляхів його застосування.

Про актуальність питань забезпечення кібернетичної безпеки свідчить, зокрема, Рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» [1]. У зазначеному рішенні привертається увага до питань забезпечення кібернетичної безпеки.

До завдань цієї статті належить передусім дослідження сучасного стану забезпечення національної безпеки в кібернетичній сфері у країнах СП на рівні нормативно-правової бази та відпрацювання конкретних пропозицій стосовно вдосконалення цієї бази в Україні.

Різні аспекти забезпечення кібернетичної безпеки розглядались у працях вітчизняних та іноземних науковців, зокрема В. Богдановича, Г. Броді, В. Бутузова, К. Гаджиєва, Д. Дубова, С. Гнатюка, Дж. Катца, У. Ліпмана, М. Ожевана, М. Присяжнюка, Д. Прудникова, Г. Семигіна, В. Телелима, В. Толубка, М. Хікса, В. Шеломенцева, Л. Шеллі. Проте у їхніх працях недостатня увага приділялася саме питанням організації захисту КІ країн СП від кіберзагроз, що є особливо актуальним для забезпечення національної безпеки України з урахуванням спільних процесів суспільно-політичних трансформацій, які у різні часи відбувалися в наших державах.

Нині кіберзлочинність набула в усьому світі масштабів епідемії: щодня системи інформаційної безпеки відбивають близько 247 тис. атак. У середньому кожне успішне

зламування дає хакерам доступ до особистих даних 604 інтернет-користувачів. У 2012 р. хакерські атаки здійснено у 27 країнах світу і щодо державних організацій, і окремих компаній [2].

Можливість виникнення кібертероризму як засобу здійснення атак на КІ держави спонукає їх розробляти нові положення, що регулюють дані питання, а також здійснювати заходи з метою захисту КІ. У сучасних умовах жодна країна не може виключати можливість того, що найважливіші об'єкти критичної інформаційної інфраструктури держави стануть прямими об'єктами кібератак.

Зазначимо, що до КІ держави відносять ті об'єкти економіки, державного управління та соціальної сфери, руйнування та/або виведення з ладу яких призводить до суспільно небезпечних наслідків для держави, суспільства та особи незалежно від засобу та способу негативного впливу (вибух, підпал, кібернетична атака тощо).

Всебічна інформатизація українського суспільства та інтеграція нашої держави у світовий інформаційний простір зумовлюють актуальність вирішення проблем із захисту КІ від кіберзагроз. Враховуючи недостатню розробленість досліджуваної проблеми в Україні, доцільним є вивчення досвіду країн СП, зокрема Республіки Білорусь, Республіки Молдова, Республіки Грузія та Вірменії у сфері захисту КІ від кіберзагроз.

Республіка Білорусь (РБ)

РБ протягом останніх років докладає значних зусиль задля вдосконалення нормативно-правової бази, визначення основних принципів та підходів у сфері забезпечення як національної безпеки загалом, так і пріоритетних напрямів та способів забезпечення інформаційної безпеки зокрема. Тут створюються нові та реорганізуються існуючі органи, що виконують відповідні завдання. Фундаментальними документами, що регулюють відносини у цій сфері, є такі.

Концепція національної безпеки РБ [3], затверджена указом президента РБ від 9 листопада 2010 р. № 575. У ній визначено пріоритетні напрями національної політики, зокрема «забезпечення надійності та стійкості функціонування критично важливих об'єктів інформатизації» (п 14.6 гл. II Національні інтереси), а також уведено термін «інформаційна безпека». Пріоритетним напрямом на шляху нейтралізації загроз інформаційній безпеці відповідно до Концепції є удосконалення нормативно-правових актів і завершення формування комплексної державної системи забезпечення інформаційної безпеки.

Указом президента РБ «Про деякі заходи із забезпечення безпеки критично важливих об'єктів інформатизації» від 25 жовтня 2011 р. № 486 [4] введено термін «критична інфраструктура». До такої віднесено життєво важливі для держави об'єкти, відмова або руйнування яких може призвести до істотного негативного впливу на національну безпеку. Цим указом до критично важливих об'єктів інформатизації (КВОІ) віднесені ті, які:

• забезпечують функціонування екологічно небезпечних і (або) соціально значимих виробництв і (або) технологічних процесів, порушення штатного режиму яких може призвести до надзвичайної ситуації техногенного характеру;

• здійснюють функції інформаційної системи, порушення (припинення) функціонування якої може призвести до значних негативних наслідків для національної безпеки в політичній, економічній, соціальній, інформаційній, екологічній, інших сферах;

• забезпечують надання значного обсягу інформаційних послуг, часткове або повне припинення надання яких може призвести до значних негативних наслідків для національної безпеки в політичній, економічній, соціальній, інформаційній, екологічній, інших сферах.

Відповідно до згаданого указу створено Державний реєстр КВОІ та встановлено порядок віднесення таких об'єктів до критично важливих і забезпечення безпеки цих об'єктів. Контроль за виконанням указу покладено на Оперативно-аналітичний центр (ОАЦ) при президентові РБ. Цей орган:

• координує діяльність державних органів та інших організацій з технічного і криптографічного захисту інформації, що обробляється КВОІ;

• здійснює формування та ведення Державного реєстру критично важливих об'єктів інформатизації, а також надання відомостей з нього;

• вносить приписи про усунення власниками об'єктів інформатизації та іншими організаціями порушень вимог глав 3–5 цього Положення, у т.ч. з безпеки КВОІ, і виносить подання про притягнення їх до відповідальності згідно із законодавчими актами;

• ухвалює нормативно-правові акти з питань віднесення об'єктів інформатизації до КВОІ та забезпечення безпеки КВОІ;

• здійснює зовнішній контроль за забезпеченням безпеки КВОІ в порядку, встановленому ОАЦ;

• здійснює інші повноваження у сфері функціонування та забезпечення безпеки КВОІ, передбачені цим Положенням та іншими законодавчими актами.

З метою реалізації зазначеного указу *Постановою Ради Міністрів РБ «Щодо деяких питань безпеки експлуатації та належного функціонування критично важливих об'єктів інформатизації» від 30 березня 2012 р. № 293*[1] затверджено: перелік галузевих критеріїв віднесення об'єктів інформатизації до КВОІ; методику визначення відповідності об'єкта інформатизації галузевим критеріям, порядок захисту КВОІ за галузевим принципом; орієнтовний перелік показників рівня шкоди національним інтересам РБ у політичній, економічній, соціальній, інформаційній, екологічній та інших сферах у разі виникнення загроз різного характеру відносно об'єкта інформатизації (чи його елементів); перелік республіканських органів державного управління, відповідальних за підготовку і затвердження переліку показників рівня шкоди національним інтересам РБ у зазначених сферах.

Указ президента РБ «Про деякі питання розвитку інформаційного суспільства в РБ» від 8 листопада 2011 р. № 515 [6] спрямований на підвищення ефективності діяльності державних органів та організацій при здійсненні державної інформаційної політики, якнайшвидше створення єдиної системи надання державних послуг в електронній формі, вдосконалення регулювання у сфері інформаційно-комунікаційних технологій (ІКТ). З урахуванням зростаючого впливу інформаційної сфери на всі сторони життєдіяльності суспільства та необхідності посилення взаємодії різних зацікавлених сторін при формуванні інформаційного суспільства згідно з указом сформовано:

• Раду з розвитку інформаційного суспільства при президентові РБ, головним завданням якої є формування державної інформаційної політики та вдосконалення механізмів її реалізації. До складу цієї ради входять голова Ради – президент РБ, його заступники та секретар. Слід зауважити, що подібні органи на чолі з вищими посадовими особами вже сформовані в багатьох країнах, у т.ч. в Російській Федерації, Німеччині, Франції, Республіці Корея та ін. Основними напрямами діяльності ради є: визначення мети та завдань державної інформаційної політики, методів і способів її реалізації; загальна координація діяльності державних органів та організацій з питань розвитку інформаційного суспільства в країні тощо;

• унітарне підприємство «Національний центр електронних послуг», що здійснює координацію діяльності із забезпечення безпеки інформаційних систем державних органів та надає послуги, перелік яких визначений постановою Ради Міністрів РБ від 31 травня 2012 № 509.

Водночас згідно з цим указом незалежним регулятором у сфері ІКТ у державі визначено уже згаданий Оперативно-аналітичний центр при президентові РБ, на який покладені завдання з визначення стратегії розвитку ІКТ; погодження в установленому порядку інвестиційних проектів, законодавчих актів у цій сфері; підготовка пропозицій щодо внесення змін до чинного законодавства тощо.

Також цим указом визначено перелік міжвідомчих інформаційних систем, затверджено Положення про Раду з розвитку інформаційного суспільства при президентові РБ, Положення про незалежного регулятора у сфері ІКТ, у якому уточнюються функції незалежного регулятора, передбачені Указом президента «Про деякі заходи з розвитку мережі передачі даних у РБ» від 30 вересня 2010 р. № 515.

Указом президента РБ «Про деякі заходи зі вдосконалення захисту інформації» від 16 квітня 2013 р. № 196 [7] (набув чинності з 19 жовтня 2013 р.) затверджено Положення про технічний та криптографічний захист інформації в державі. Цим Положенням визначено об'єкти, на яких здійснюється криптографічний захист інформації.

РБ працює над постійним удосконаленням нормативно-правових актів, про що також свідчить постійне удосконалення *Кодексу про адміністративні порушення* [8] та *Процесуально-виконавчого кодексу про адміністративні порушення РБ* [9].

Республіка Молдова (РМ)

РМ останніми роками докладає значних зусиль для забезпечення своєї інформаційної та кібернетичної безпеки з урахуванням досвіду США та країн-членів ЄС. Базовими документами, що регулюють відносини у цій сфері, є:

Концепція національної безпеки РМ [10] (затверджена законом РМ від 22 травня 2008 р. № 112). Серед головних загроз національній безпеці Концепцією визначено загрози у сфері інформаційних технологій. Так, нестабільність або порушення функціональності інформаційних систем можуть бути

[1] Зареєстровано у Національному реєстрі правових актів Республіки Білорусь від 3.04.12 р. № 5/35494.

суттєвою загрозою національній безпеці. У Концепції зазначається, що прогресивний розвиток електронних інформаційних систем у РМ і високий рівень їх взаємодії з міжнародними інформаційними системами полегшують дію криміногенного чинника в інформаційній сфері та посилюють уразливість цих систем, у тому числі в найважливіших для національної безпеки сферах.

Закон РМ «Про інформатизацію та державні інформаційні ресурси» від 21 листопада 2003 р. № 467 [11] встановлює основні правила та умови діяльності в галузі створення та розвитку національної інформаційної інфраструктури як середовища функціонування інформаційного суспільства РМ, яке регулює правові відносини, що виникають у процесі формування та використання державних автоматизованих інформаційних ресурсів, створення та використання інформаційних технологій, систем і мереж. При цьому «інформаційна інфраструктура» визначається як сукупність інформаційно-обчислювальних центрів, банків даних і знань інтегрованої автоматизованої системи зв'язку та організації, яка забезпечує користувачам загальні умови доступу до інформації, що зберігається.

Відповідно до ст. 23 цього закону центральним галузевим органом публічного управління, уповноваженим реалізовувати інформаційну політику уряду та розробляти стратегію розвитку в цій галузі, зокрема щодо формування і використання державних інформаційних ресурсів та інформатизації, є Міністерство інформаційного розвитку, яке представляє уряд у спеціалізованих міжнародних організаціях відповідно до наданих йому повноважень і координує міжнародну співпрацю у цій сфері.

Відповідно до ст. 4 *Закону РМ «Про запобігання та боротьбу із злочинністю в галузі комп'ютерної інформації» від 3 лютого 2009 р. № 20-XVI* [12] завдання щодо захисту національних інтересів РМ у кібернетичному просторі покладені на:

• *Міністерство внутрішніх справ*, яке проводить оперативно-розшукову діяльність, кримінальне переслідування, міжнародне співробітництво, ідентифікацію осіб, що скоїли кібернетичні правопорушення;

• *Службу інформації та безпеки* [13], яка здійснює заходи з попередження та боротьби зі злочинністю у сфері комп'ютерної інформації, що представляє загрозу національній безпеці, проводить оперативно-розшукові заходи, вживає заходів з виявлення зв'язків міжнародних злочинних організацій, здійснює інші заходи в межах своєї компетенції. Міністерство внутрішніх справ і Служба інформації та безпеки готують і постійно актуалізують бази даних про злочинність у сфері комп'ютерної інформації;

• *Генеральну прокуратуру*, яка координує, керує і здійснює кримінальне переслідування у встановленому порядку; розпоряджається, в рамках здійснення кримінального переслідування у зв'язку зі зверненням органу кримінального переслідування або з власної ініціативи, про негайне збереження комп'ютерних даних або даних про інформаційні потоки, щодо яких існує небезпека їх знищення або пошкодження, відповідно до кримінально-процесуального законодавства; пред'являє від імені держави обвинувачення в судових інстанціях у порядку, передбаченому законом;

• *Національний інститут юстиції,* який забезпечує професійне вдосконалення персоналу, задіяного у здійсненні правосуддя у сфері боротьби з комп'ютерною злочинністю;

• *Міністерство інформаційних технологій і зв'язку*, яке спільно зі Службою інформації та безпеки представляють пропозиції щодо забезпечення захисту та безпеки комп'ютерних даних.

Крім того, окремі завдання у сфері забезпечення кібернетичної безпеки РМ покладені на:

• *Міністерство інформаційних технологій та зв'язку* [14], яке відповідає за формування і реалізацію державної політики у сфері інформаційних і телекомунікаційних технологій; супроводження єдиної системи створення та використання державних інформаційних ресурсів; координацію діяльності органів державної влади з розробки, впровадження та розвитку проектів і програм, пов'язаних із застосуванням сучасних інформаційних і телекомунікаційних технологій та здійснення їх експертизи; контроль за дотриманням чинного законодавства в інформаційній сфері;

• *Службу інформації та безпеки* [15], яка виконує завдання з розробки пропозицій щодо забезпечення інформаційної безпеки, просування державної політики та здійснення контролю за забезпеченням захисту державної таємниці інформації в кіберпросторі, а також створення, забезпечення функціонування та безпеки урядової електронної системи зв'язку, щодо розробки стратегії та реалізації державної політики в галузі управління і забезпечення функціонування та безпеки спеціальних електронних систем зв'язку;

• *державне підприємство «Центр спеціальних телекомунікацій»* [16], що забезпечує безпечне функціонування та розвиток державних захищених інформаційних систем і телекомунікаційних мереж;

• *Центр із забезпечення кібернетичної безпеки* [17], який створений на базі Державного підприємства «Центр спеціальних телекомунікацій» та призначений для забезпечення кібернетичної безпеки державних органів.

Головними завданнями цього центру є: виявлення, аналіз та класифікація кібератак; захист інформаційних ресурсів, систем і мереж органів державної влади від кібернетичного впливу; оперативне реагування на кіберзагрози та надання консультативної й технічної підтримки користувачам щодо запобігання кіберзагрозам; створення та супроводження баз даних виявлених кіберінцидентів; організація обміну інформацією з міжнародними групами (центрами) *CERT* (*Computer Emergency Response Team* – Центр швидкого реагування на комп'ютерні інциденти) щодо загроз кібернетичного характеру; розробка відповідних процедур, механізмів, алгоритмів і рекомендацій щодо забезпечення кібернетичної безпеки держави; організація науково-дослідної діяльності в рамках визначених повноважень; забезпечення підготовки спеціалістів за напрямом забезпечення кібернетичної безпеки.

Відповідно до п. 1.5 (Боротьба з тероризмом та забезпечення кіберзахисту) *Постанови уряду РМ «Про затвердження актуалізованого Індивідуального плану дій щодо партнерства РМ – НАТО» від 18 серпня 2010 р. № 746* [18] РМ продовжуватиме докладати зусиль щодо зміцнення захищеності систем інформації та зв'язку від кібернетичних атак.

Урядом РМ також розроблено «Дорожню карту», яка є основою для стратегії або програми із забезпечення кібернетичної безпеки в державі. Її основна мета – забезпечення безпеки національного кіберпростору. Наразі робоча версія «Дорожньої карти» в галузі кібербезпеки РМ запропонована громадськості для консультацій.

Республіка Грузія (РГ)

РГ з огляду на зростання рівня небезпеки в кіберпросторі країни докладає значних зусиль у напрямі забезпечення інформаційної безпеки з урахуванням досвіду країн-членів НАТО. З цією метою здійснюється комплекс нормативно-правових, організаційних і технічних заходів.

Так, 23 грудня 2011 р. парламент РГ затвердив *Концепцію національної безпеки країни* [19], яка визначає пріоритетні напрями зовнішньої політики країни та шляхи забезпечення національної безпеки у сучасних умовах. У розділі *«Загрози, ризики та виклики національній безпеці Грузії»* визначено основні загрози інформаційній безпеці, які пов'язані із залежністю національної КІ від інформаційних технологій та збільшенням кількості проблемних питань щодо захисту кіберпростору держави.

У розділі *«Пріоритети національної політики безпеки»* зазначається, що РГ прагне створити систему кібербезпеки, яка сприятиме ефективному захисту інформаційної інфраструктури країни, мінімізації наслідків від кібератак і швидкому відновленню пошкоджених мереж у разі нападу. Водночас наголошується на необхідності створення відповідної правової бази та інфраструктури для поліпшення інформаційних технологій та захисту інформації, а також важливості врахування зарубіжного досвіду та поглиблення міжнародного співробітництва з державами-партнерами у цій сфері.

Основним документом з визначення державної політики у сфері кібербезпеки та заходів, необхідних для створення у країні кібербезпечного середовища, є *Стратегія кібернетичної безпеки* [20]. 24 травня 2013 р. президентом РГ затверджено план дій з виконання цієї стратегії на 2013–2015 рр., який має забезпечити захищене функціонування державних органів, приватного сектору та громадськості в кіберпросторі. Координацію відповідних заходів міністерств і відомств здійснює Агентство обміну даними Міністерства юстиції Грузії.

15 березня 2014 р. набули чинності зміни до ст.ст. 284–286 (гл. 35) *Кримінального кодексу Грузії* [21], якими передбачена відповідальність як фізичних, так і юридичних осіб за скоєння кіберзлочинів. Зокрема, йдеться про позбавлення права на здійснення певної діяльності, накладення штрафу або конфіскацію майна, а також позбавлення волі від 2 до 6 років.

Крім того, у 2013 р. парламентом РГ розглянуто Проект закону *«Про інформаційну безпеку»* [22], який передбачає впровадження стандартів та механізмів державного контролю за діяльністю приватного сектору, сайтів державних органів РГ, засобів масової інформації (інформаційні портали, які здійснюють мовлення російською мовою). Депутати парламенту РГ пояснюють увагу до російськомовних ЗМІ кібератаками на подібні сайти, які мали місце саме в серпні 2008 р. Законопроект передбачає, що посилений моніторинг і контроль за діяльністю «суб'єктів критичної інфраструктури» (конкретний список визначатиме президент РГ відповідним указом на основі рекомендацій Ради національної безпеки) здійснюватиме Агентство обміну даними Міністерства юс-

тиції Грузії. Очікується, що цей закон набуде чинності до кінця 2014 р.

Водночас 1 листопада 2013 р. урядом РГ внесено в парламент проект змін до *Закону РГ «Про державну таємницю»*. Відповідно до законопроекту у структурах виконавчої, законодавчої та судової влади може бути створена скоординована система захисту інформації, що сприятиме виконанню зобов'язань з боку РГ, в рамках щорічного національного плану НАТО і міжнародної угоди від 12 грудня 1994 р. і приведення у відповідність до вимог НАТО систем інформаційної безпеки РГ.

До системи державних органів, що забезпечують інформаційну безпеку РГ, належать:

• Служба *SMART LOGIC* [24] («розумна оптимізація»), яка створена у березні ц.р. у складі Міністерства юстиції РГ, відповідає за впровадження сучасних ІКТ у державній системі (*Cloud systems*) і здійснює контроль за її безпечним функціонуванням. Крім того, з метою оптимізації фінансових витрат на впровадження і розвиток сучасних інформаційно-телекомунікаційних технологій в органах державної влади служба надаватиме їм практичну допомогу при реалізації цих заходів;

• Центр швидкого реагування на комп'ютерні інциденти [24] (*CERT*) підпорядковується Агентству обміну даними Міністерства юстиції РГ і спеціалізується на виявленні, реєстрації й аналізі критичних інцидентів; надає рекомендації, а також здійснює оперативне реагування на вказані інциденти; відіграє значну роль у підвищенні поінформованості з питань інформаційної безпеки в державі. З метою підвищення ефективності захисту інформаційної інфраструктури РГ від кібератак найближчим часом для забезпечення діяльності *CERT* передбачається впровадження:

– системи виявлення вторгнень у телекомунікаційні мережі (*NIDS – Network Intrusion Detection System)* із застосуванням спеціалізованих апаратних і програмних засобів;

– автоматизованої системи *Honey Network* – для виявлення на ранніх стадіях і нейтралізації вірусного програмного забезпечення в інформаційних системах і телекомунікаційних мережах.

Республіка Вірменія (РВ)

Система інформаційної безпеки РВ перебуває на етапі формування. Нині основоположними документами державної політики у сфері інформаційної безпеки РВ є такі:

• *Закон РВ «Про масову інформацію» від 14 січня 2004 р. № ЗР-14* [25]. Він регулює відносини, що виникають у галузі ЗМІ, встановлює гарантії забезпечення права на свободу слова, акредитації журналіста, права на спростування поширюваної інформації, а також ті підстави, за наявності яких суб'єкти інформаційної діяльності не нестимуть відповідальності;

• *Закон РВ «Про оборону» від 29 травня 1997 р. № ЗР-120* [26], у якому термін «інформаційна безпека» визначено як захищеність інформаційного середовища, що забезпечує формування, використання і розвиток інформаційного середовища громадян і організацій в інтересах держави;

• *Закон РВ «Про електронний документ та електронний цифровий підпис» від 15 січня 2005 р. № ЗР-40* [27]. Метою закону є створення правового поля для формування та регулювання правових відносин, пов'язаних з електронним документообігом та електронним підписом, що виникають у системі державного управління, приватному секторі, а також в інших сферах економіки. Закон регулює правові відносини, що виникають при процедурах створення та сертифікації електронних підписів. Крім основних понять у сфері електронної документації та електронного цифрового підпису, у законі зафіксовано поняття «інформаційна система», зміст якого визначено як систему підготовки, доставки, отримання, зберігання або іншого типу апаратно-програмної розробки електронних документів;

• *Закон РВ «Про персональні дані» від 7 листопада 2002 р. № ЗР-422* [28], який регулює відносини, пов'язані з обробкою державними органами управління та органами місцевого самоврядування, державними або муніципальними відомствами, юридичними або фізичними особами персональних даних. Водночас цей закон не регулює відносини, пов'язані з обробкою персональних даних, які вважаються державною таємницею, персональних даних, опублікованих у загальнодоступних джерелах, а також персональних даних фізичних осіб, які використовуються в особистій та інших подібних цілях. Згідно із законом «персональні дані» – це будь-які дані про факти, події, обставини, які відносяться до фізичної особи, зафіксовані на матеріальному носії інформації письмово або іншим чином, у такому вигляді, який надає або може надати можливість ідентифікувати особистість індивідуума;

• *Закон РВ «Про свободу інформації» від 22 жовтня 2003 р. № ЗР-11* [29], який регулює відносини, пов'язані зі свободою інформації, визначає права розпорядників інформації у сфері надання інформації, а також порядок, вид та умови отримання інформації. Дія цього

закону поширюється на органи державної влади та місцевого самоврядування, державні установи, організації, що фінансуються з бюджету, а також на організації, що мають суспільне значення, та їх керівні особи;

• *Закон РВ «Про електронний зв'язок» від 13 серпня 2005 р. № ЗР-176* [30], у якому визначено права та обов'язки операторів, що надають послуги у сфері електрозв'язку;

• *Закон РВ «Про телекомунікації» від 20 лютого 1998 р. № ЗР-197* [31], який встановлює правові основи діяльності у сфері надання телекомунікаційних послуг, а також компетенцію та відповідальність її учасників і норми щодо захисту прав користувачів зазначених послуг. Регулює правові відносини в галузі телекомунікації, включаючи питання надання радіочастот, за винятком теле- і радіомовлення, які регулюються окремим законом;

• *Закон РВ «Про органи національної безпеки» від 24 січня 2002 р. № ЗР-294* [32], згідно з яким органи національної безпеки здійснюють державний контроль у сфері інформаційної безпеки, а також координують діяльність у сфері шифрованого й технічного захисту інформації, що охороняється законодавством РВ.

Органами, що регулюють відносини у сфері кібербезпеки, є Служба національної безпеки РВ і Головне управління боротьби з організованою злочинністю Поліції РВ, у структурі якого у 2009 р. сформовано відділ з боротьби із злочинами у сфері високих технологій.

Розділом 24 «Злочини проти безпеки комп'ютерної інформації» Кримінального кодексу [33] (прийнятий 29 квітня 2003 р.) передбачено кримінальну відповідальність за такі злочини, як:

• несанкціонований доступ (проникнення) до систем комп'ютерної інформації (ст. 251);

• зміни комп'ютерної інформації (ст. 252);

• комп'ютерна диверсія (ст. 253);

• неправомірне копіювання комп'ютерної інформації (ст. 254);

• виготовлення або збут спеціальних засобів неправомірного доступу (проникнення) до комп'ютерної інформації (ст. 255);

• розроблення, використання та розповсюдження шкідливих програм (ст. 256);

• порушення правил експлуатації комп'ютерної системи або мережі (ст. 257).

Україна

В Україні, на жаль, досі не вирішена проблема створення ефективної системи фізичного захисту об'єктів КІ. При цьому слід зазначити, що в нашій державі присутні всі її сектори та елементи. З-поміж них є такі складні масштабні промислові комплекси, як АЕС, об'єкти ядерної промисловості, підприємства хімічної промисловості, ГЕС, греблі/дамби, інформаційні та платіжні банківські системи, транспортні мережі, нафто- і газопроводи, мережі зв'язку й передачі інформації тощо.

Вперше в Україні термін «об'єкти критичної інфраструктури» на нормативному рівні згадується у 2012 р. у новій редакції Стратегії національної безпеки України «Україна у світі, що змінюється». У Стратегії зосереджено увагу на питаннях захисту КІ паливно-енергетичного комплексу від екологічно-техногенних впливів та навмисних дій.

Привертає увагу той факт, що Указом Президента України від 10 грудня 2010 р. № 1119 уведено в дію Рішення РНБОУ «Про виклики та загрози національній безпеці і обороні України у 2011 році» від 17 листопада 2010 р., яким КМ України доручено розробити та затвердити Перелік об'єктів, що мають важливе значення для забезпечення національної безпеки і оборони України та потребують першочергового захисту від кібератак. Однак дорученням КМУ від 30 травня 2013 р. № 7123/0/2–13 [34] було перенесено строк виконання завдання, передбаченого п. 4 рішення РНБОУ, у зв'язку з відсутністю в державі спільного підходу щодо віднесення об'єктів до такого Переліку.

З метою визначення критеріїв віднесення об'єктів до зазначеного Переліку Адміністрацією Держспецзв'язку України розроблено проект Постанови КМУ «Про визначення порядку віднесення об'єктів до таких, що мають важливе значення для забезпечення національної безпеки і оборони України та потребують першочергового захисту від кібернетичних атак». Проектом встановлено, що найбільш прийнятним підходом до визначення цих критеріїв вважається їх розподіл за галузевим принципом.

Слід також зазначити, що нині в Україні визначено низку категорій об'єктів, стосовно яких передбачено особливі умови забезпечення захисту, зокрема: заходи з удосконалення охорони об'єктів державної та іншої форм власності [35]; перелік особливо небезпечних підприємств [36]; Положення про Державний реєстр потенційно небезпечних об'єктів [37]; перелік підприємств, які мають стратегічне значення для економіки та безпеки держави [38] тощо.

Водночас у державі паралельно функціонують Єдина система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків, Єдина державна система запо-

бігання і реагування на надзвичайні ситуації техногенного та природного характеру, Єдина державна система цивільного захисту населення і територій. При цьому Постановою КМУ від 15 серпня 2007 р. № 1051 затверджено Положення про Єдину систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків; Постановою КМУ від 8 грудня 2006 р. № 1700 (зі змінами) затверджено Положення про Єдину державну систему запобігання і реагування на надзвичайні ситуації техногенного та природного характеру, а Законом України від 24 червня 2004 р. № 1859-IV «Про правові засади цивільного захисту» затверджено Положення про Єдину державну систему цивільного захисту населення і територій.

Однак ефективність цих систем є досить умовною, і тому для України важливого значення набуває створення єдиної загальнодержавної системи відповідних норм і правил реагування на кризові явища, управління ними та виходу з них.

Зважаючи на зазначене, слід констатувати, що в Україні існує низка проблемних питань, пов'язаних із захистом об'єктів КІ, що потребують вирішення, до яких слід передусім віднести:

• відсутність загального механізму управління захистом та безпекою об'єктів критичної інформаційної інфраструктури;

• дублювання функцій, відсутність спільних підходів та узгодженості дій контролюючих органів;

• невизначеність механізмів взаємодії з керівниками підприємств, у власності яких перебувають об'єкти життєзабезпечення та підвищеної небезпеки (на яких впроваджені інформаційні технології управління) та втручання в роботу яких може призвести до тяжких наслідків;

• невідповідність сучасним реаліям критеріїв якості підготовки спеціалістів різноманітних спеціальностей, пов'язаних зі сферою кібербезпеки;

• відсутність багатопрофільних науково-дослідних інститутів для здійснення комплексних досліджень з питань кібербезпеки;

• відсутність комплексних навчань із залученням усіх військових і правоохоронних структур, задіяних у системі забезпечення кібербезпеки держави.

Висновки та рекомендації

Вивчення досвіду держав Східного партнерства – *Білорусі, Молдови, Грузії та Вірменії* – у сфері захисту КІ дає змогу зробити такі висновки.

1. Підсистема захисту критичних інфраструктур розглядається республіками Білорусь, Молдова, Грузія та Вірменія як невід'ємний елемент системи захисту національної безпеки і здійснюється на основі виконання прийнятих державами стратегій та відповідних планів дій. Отже, захищеність об'єктів КІ нерозривно пов'язана з національними інтересами держави.

2. Державою з найбільш розробленим законодавством у сфері захисту КІ можна вважати Республіку Білорусь. Зокрема, в ньому визначено поняття «критичної інфраструктури», сформульовано критерії віднесення об'єктів до КІ, створено Державний реєстр критично важливих об'єктів інфраструктури, визначено координуючий орган у сфері діяльності державних органів та інших організацій з технічного і криптографічного захисту інформації, що обробляється на критично важливих об'єктах інфраструктури – Оперативно-аналітичний центр при президентові Республіки Білорусь.

3. Республікою Грузією здійснено комплекс нормативно-правових заходів, у результаті яких прийнято Стратегію кібербезпеки та внесено на розгляд парламенту законопроект «Про інформаційну безпеку», яким визначено координуючий орган – Агентство обміну даними Міністерства юстиції Грузії.

4. Республіка Молдова перебуває на початковій стадії формування системи кібербезпеки. Уряд РМ постійно організовує заходи для обговорення важливих проблем кібербезпеки, свідченням чого є проведення протягом 2013 р. низки конференцій та «круглих столів» з відповідної тематики.

5. Свідченням активізації зусиль українського, грузинського та молдовського державного керівництва в напрямі поглиблення міжнародного співробітництва з питань забезпечення кібербезпеки є проведення конференції з питань боротьби з кібернетичною злочинністю.

6. Для вирішення проблемних питань забезпечення національної безпеки досліджуваними країнами застосовуються поняття, що визначають особливий статус об'єктів і систем. Усі вони відповідно до світового досвіду можуть бути об'єднані єдиним терміном – «критична інфраструктура».

Отже, аналіз нормативно-правового поля країн – учасників програми Східного партнерства дає змогу виділити основні заходи, що можуть суттєво посилити захист національних об'єктів КІ від кібератак. Зокрема, вбачається доцільним розробити та здійснити такі заходи.

1. Кабінету Міністрів України за участю заінтересованих органів державної влади необхідно:

• здійснити підготовку базових нормативно-правових актів, які мають містити визначення основних понять кібербезпекової сфери, визначатимуть напрями державної політики і власне механізм організації та здійснення захисту об'єктів КІ, визначатимуть критерії віднесення об'єктів до критично важливих, чітко розмежовуватимуть повноваження суб'єктів забезпечення безпеки і стійкого функціонування інформаційних, інформаційно-телекомунікаційних та автоматизованих систем керування технологічними процесами зазначених об'єктів;

• розробити перелік об'єктів критичної інформаційної інфраструктури держави та встановити пріоритетність їх захисту;

• створити Державний реєстр критичних елементів інформаційної інфраструктури;

• розробити регламент функціонування єдиної державної системи виявлення та запобігання кібератакам на об'єкти критичної інформаційної інфраструктури держави;

• визначити орган, який забезпечуватиме реалізацію державної політики з питань кібербезпеки, координацію дій уповноважених органів (насамперед сектору безпеки і оборони, державних органів, що відповідають за галузь телекомунікацій та інформатизації тощо, власників та розпорядників об'єктів критичної інформаційної інфраструктури), а також впровадження заходів із захисту національної інформаційної інфраструктури.

2. Міністерству закордонних справ України та органам, причетним до захисту національної інфраструктури від кіберзагроз, необхідно:

• налагодити ефективне співробітництво з іноземними державами, їх правоохоронними органами і спецслужбами, а також з міжнародними організаціями у напрямку забезпечення захисту об'єктів КІ, участі представників України у міжнародних навчаннях з цієї проблематики на регулярній основі.

3. Адміністрації Держспецзв'язку України слід:

• дати оцінку загроз конкретним об'єктам КІ та спланувати заходи для їх захисту з урахуванням імовірних сценаріїв загроз, оцінювання вартості заходів захисту.

Список використаних джерел

1. *Про рішення* Ради національної безпеки і оборони України від 28 квітня 2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» : указ Президента України від 1.05.2014 р. № 449 [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/17588.html

2. *Forbes* Україна [Електронний ресурс]. – Режим доступу: http://forbes.ua/business/1358089-samye-gromkie-kiberataks/1358103#cut

3. *Офіційний* сайт Національного зібрання Республіки Білорусь [Електронний ресурс]. – Режим доступу: http://www.sovrep.gov.by/index.php/.1.7943...0.0.0.html

4. *Національний* правовий інтернет-портал Республіки Білорусь [Електронний ресурс]. – Режим доступу: http://pravo.by/main.aspx?guid=3871&p0=P31100486&p2= {NRPA}

5. *Законодавство* держав СНД [Електронний ресурс]. – Режим доступу: http://base.spinform.ru/show_doc.fwx?rgn=47739

6. *Національний* правовий Інтернет-портал Республіки Білорусь [Електронний ресурс]. – Режим доступу: http://pravo.by/main.aspx?guid=3871&p0=P31300196&p1=1

7. *Офіційний* сайт Міністерства внутрішніх справ Республіки Білорусь [Електронний ресурс]. – Режим доступу: http://mvd.gov.by/main.aspx?guid=25703

8. *Офіційний* сайт Міністерства внутрішніх справ Республіки Білорусь [Електронний ресурс]. – Режим доступу: http://mvd.gov.by/main.aspx?guid=25693

9. *Державний* реєстр правових актів Республіки Молдова [Електронний ресурс]. – Режим доступу: http://lex.justice.md/viewdoc.php?action=view&view=doc&id=328010&lang=2

10. *Офіційний* сайт Міністерства інформаційних технологій і зв'язку [Електронний ресурс]. – Режим доступу: http://www.mtic.gov.md/img/pdf/467_2003-11-21_ru.pdf

11. *Офіційний* сайт Національного агентства з регулювання в галузі електронних телекомунікацій і технологій [Електронний ресурс]. – Режим доступу: http://ru.anrceti.md/laws?page=1

12. *Офіційний* сайт Служби інформації та безпеки Республіки Молдова [Електронний ресурс]. – Режим доступу: http://www.sis.md/en/ensuring-informational-security

13. *Офіційний* сайт Міністерства інформації та зв'язку Республіки Молдова [Електронний ресурс]. – Режим доступу: http://www.mtic.gov.md/sarcini_rus/

14. *Офіційний* сайт Служби інформації та безпеки Республіки Молдова [Електронний ресурс]. – Режим доступу: http://www.sis.md/en/ensuring-informational-security

15. *Офіційний* сайт ДП «Центр спеціальних телекомунікацій» [Електронний ресурс]. – Режим доступу: http://cts.md/ru/content/napravleniya-deyatelnosti

16. *Офіційний* сайт Центру із забезпечення кібернетичної безпеки [Електронний ресурс]. – Режим доступу: http://cert.gov.md/

17. *Державний* реєстр правових актів [Електронний ресурс]. – Режим доступу: http://lex.justice.md/viewdoc.php?action=view&view=doc&id=335977&lang=2

18. *Офіційний* сайт Міністерства закордонних справ Республіки Грузія [Електронний ресурс]. – Режим доступу: http://www.mfa.gov.ge/index.php?lang_id=ENG&sec_id=12

19. *Інформаційне* агентство Грузії [Електронний ресурс]. – Режим доступу: http://www.pirweli.com.ge/rus/?menuid=8&id=6694

20. *Кримінальний* кодекс Республіки Грузія : (пер. з грузинської мови) [Електронний ресурс]. – Режим доступу: http://www.parliament.ge/_special/kan/files/673.pdf

21. *Новини-Грузія* [Електронний ресурс]. – Режим доступу: http://newsgeorgia.ru/politics/20120223/214750556.html

22. *Новини-Грузія* [Електронний ресурс]. – Режим доступу: http://www.newsgeorgia.ru/economy/20120302/214783693.html

23. *Офіційний* сайт Національного центру швидкого реагування на комп'ютерні інциденти [Електронний ресурс]. – Режим доступу: http://www.CERT.GOV.GE

24. *Офіційний* сайт Національного Зібрання Республіки Вірменія [Електронний ресурс]. – Режим доступу: http://www.parliament.am/legislation.php?sel=show&ID=1890&lang=rus

25. *Офіційний* сайт Національного Зібрання Республіки Вірменія [Електронний ресурс]. – Режим доступу: http://www.parliament.am/legislation.php?sel=show&ID=3420&lang=rus

26. *Офіційний* сайт Національного Зібрання Республіки Вірменія [Електронний ресурс]. – Режим доступу: http://www.parliament.am/legislation.php?sel=show&ID=2252&lang=rus

27. *Офіційний* сайт Національного Зібрання Республіки Вірменія [Електронний ресурс]. – Режим доступу: http://www.parliament.am/legislation.php?sel=show&ID=1331&lang=rus

28. *Офіційний* сайт Національного Зібрання Республіки Вірменія [Електронний ресурс]. – Режим доступу: http://www.parliament.am/legislation.php?sel=show&ID=1390&lang=rus

29. *Офіційний* сайт Національного Зібрання Республіки Вірменія [Електронний ресурс]. – Режим доступу: http://www.parliament.am/legislation.php?sel=show&ID=2385&lang=rus

30. *Офіційний* сайт Національного Зібрання Республіки Вірменія [Електронний ресурс]. – Режим доступу: http://www.parliament.am/legislation.php?sel=show&ID=1465&lang=rus

31. *Офіційний* сайт Національного Зібрання Республіки Вірменія [Електронний ресурс]. – Режим доступу: http://www.parliament.am/legislation.php?sel=show&ID=1278&lang=rus

32. *Офіційний* сайт Національного Зібрання Республіки Вірменія [Електронний ресурс]. – Режим доступу: http://www.parliament.am/legislation.php?sel=show&ID=1349&lang=rus

33. *Законодавство* України [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/n0008525–10

34. *Про заходи* щодо вдосконалення охорони об'єктів державної та інших форм власності : постанова КМУ від 10.08.1993 р. № 615 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=615–93-%EF

35. *Перелік* особливо небезпечних підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання заподіянню шкоди життю та здоров'ю громадян, майну, спорудам, навколишньому природному середовищу : постанова Кабінету Міністрів України від 6.05.2000 р. № 765 [Електронний ресурс]. – Режим доступу: http://zakon.nau.ua/doc/?code=765–2000-%EF

36. *Про затвердження* Положення про Державний реєстр потенційно небезпечних об'єктів : постанова КМУ від 29.08.2002 р. № 1288 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/1288–2002-%D0 %BF

37. *Про затвердження* переліку підприємств, які мають стратегічне значення для економіки та безпеки держави : постанова КМУ від 23.12.2004 р. № 1734 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1734–2004-%D0 %BF