подолання проблем внутрішньо переміщених осіб в Україні, включаючи розробку прогнозів щодо використання потенціалу ВПО для формування нового громадянського суспільства та реалізації державної стратегії розвитку до 2020 року.

Література:

1. Офіційний сайт Міністерства соціальної політики України [Електронний ресурс]. – Режим доступу: http://www.mlsp.gov.ua/labour/control/uk/index
2. Аналітичний цент «CEDOS» [Електронний ресурс]. – Режим доступу: http://www.cedos.org.ua/uk/categories/migration/forced-migration-and-internally-displaced-person
3. Регіональне представництво УВКБ ООН у Білорусі, Молдові та Україні [Електронний ресурс]. – Режим доступу: http://www.unhcr.org.ua/idpprofile
4. Закон України «Про забезпечення прав і свобод внутрішньо переміщених осіб» 20.10.2014 № 1706-VII // Відомості Верховної Ради України. – 2015. – № 5. – Ст. 5. (Зі змін та допов.)
5. Численность населения на 1 января 2014 года и средняя численность за 2013 год [Електронний ресурс]. – Режим доступу: http://ukrstat.org/operativ/operativ2014/ds/kn/kn_r/kn0114_r.html
6. Вироблення політики щодо внутрішньо переміщених осіб в Україні [Електронний ресурс]. – Режим доступу: http://www.cedos.org.ua/uk/migration/vyroblennia-polityky-shchodo-vnutrishno-peremishchenykh-osib-v-ukraini
7. Kälin, Walter. Addressing Internal Displacement: A Framework for National Responsibility. Washington, DC: Brookings Institution – U of Bern Project on Internal Displacement, 2004.

УДК 323:351

ЄВРОПЕЙСЬКИЙ ДОСВІД ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

БАЛУЄВА О.В., д.е.н., доцент,
проректор з наукової роботи,
ОСТРОВИЙ О.В., здобувач,
Донецький державний університет управління (м. Маріуполь)

В статті розглянуто досвід зарубіжних країн в забезпеченні кібернетичної безпеки, актуалізовано необхідність прийняття національної стратегії забезпечення кібербезпеки, визначено принципи формування державної політики кібербезпеки.

Ключові слова: *державне управління, національна безпека, кібернетична загроза, кібернетична безпека, кібернетичний захист.*

В статье рассмотрен опыт зарубежных стран в обеспечении кибернетической безопасности, актуализирован необходимость

принятия национальной стратегии обеспечения кибербезопасности, определены принципы формирования государственной политики кибербезопасности.

Ключевые слова: *государственное управление, национальная безопасность, кибернетическая угроза, кибернетическая безопасность, кибернетическая защита.*

In the article the experience of foreign countries in ensuring cyber security Modified the need for a national strategy for cybersecurity, defined the principles of public policy cybersecurity.

Keywords: *public administration, national safety, cybernetic threat, cybernetic safety, cybernetic protection.*

Актуальність теми. Національна безпека України, її економічне процвітання та соціальне благополуччя все більше залежать від доступності, цілісності та конфіденційності інформаційних ресурсів, що забезпечуються інформаційними та комунікаційними технологіями, або в більш широкому розумінні – кіберпростором.

За оцінками експертів у сфері кібернетичної безпеки переважної більшості провідних країн світу відмічається стійка тенденція до значного зростання кількості та розширення спектра кібератак з метою порушення конфіденційності, цілісності і доступності державних інформаційних ресурсів, зокрема тих, що циркулюють на об'єктах критичної інформаційної інфраструктури [1].

На сьогодні, реальні прояви кібератак мало прогнозовані, а їх результатом є, як правило, значні фінансово-економічні збитки або непередбачувані наслідки порушень функціонування інформаційно-телекомунікаційних систем, які безпосередньо впливають на стан національної безпеки і оборони. У зв'язку з цим, існуючі загрози вимагають впровадження комплексних заходів, спрямованих на забезпечення кібербезпеки.

Кібернетична безпека все частіше розглядається, як стратегічна проблема, державного рівня та торкається всіх верств суспільства. Державна політика кібернетичної безпеки у світі виступає засобом посилення безпеки і надійності інформаційних систем держави. У стратегії до проблеми кібернетичної безпеки застосовується високорівневий: висувається ряд державних цілей і пріоритетів, які необхідно досягти за певний проміжок часу. Фактично, стратегія являє собою модель вирішення задачі кібернетичної безпеки всередині держави.

Аналіз останніх досліджень і публікацій, у яких розглянуто досвід, основні положення забезпечення кібернетичної безпеки, досягнення й пропозиції у сфері боротьбі з кіберзлочинністю свідчить про актуальність даної тематики. Дослідження з проблем підготовки фахівців з протидії злочинам у сфері кібербезпеки, що набуває особливої актуальності висвітлено в працях О. Бєлоусова, В. Голубєва, В. Козлова, Г. Маклакова, В. Поліванюка, М. Ожевана, В. Петрова, В. Пилипчука, В. Шеломенцева, В. Бутузова, О. Довганя та ін.

Мета дослідження. Виходячи з актуальності та широти проблематики, вельми доречним є розглянути зарубіжну практику організації і забезпечення кібернетичної безпеки з метою визначення можливостей її використання в Україні. Окреслення ключових стратегічних проблем в забезпечення кібернетичної безпеки і шляхів їх вирішення задля розбудови ефективних механізмів державного управління є нагальної потребою сьогодення, враховуючи ті соціально-політичні умови, в яких опинилась країна.

Виклад основного матеріалу дослідження. За останні десять років по всій Європі отримали поширення плани заходів та стратегії, покликані вирішити задачу

забезпечення кібернетичної безпеки. Так, у 2005 році Німеччина прийняла Державний план захисту інформаційної інфраструктури (National Plan for Information Infrastructure Protection – NPSI); у наступному році Швеція розробила Стратегію посилення безпеки Інтернету в Швеції (Strategy to improve Internet security in Sweden). Слідом за великої кібератакою в 2007 році Естонія стала однією з перших країн-членів Євросоюзу, що опублікувала в 2008 році державну стратегію кібернетичної безпеки. З тих пір в цій сфері на державному рівні була проведена велика робота, і в останні десять роки десять країн-членів Євросоюзу опублікували свої державні стратегії кібернетичної безпеки.

Слід зазначити, що Естонія надає особливого значення необхідності захисту кіберпростору в цілому і ставить в центр уваги безпеку інформаційних систем; рекомендовані заходи носять цивільний характер і ґрунтуються на правовому регулюванні, навчанні та співробітництво.

В фінській стратегії, в основі лежить розуміння кібернетичної безпеки як проблеми економічного характеру, тісно пов'язаної з розвитком фінського інформаційного суспільства.

В Словаччині забезпечення інформаційної безпеки розглядається як необхідна умова нормального функціонування і розвитку суспільства. Тому мета стратегії – служити міцним фундаментом для захисту інформації, стратегія спрямована як на запобігання загрозам, так і на забезпечення готовності і стійкості засобів їх запобігання.

Ключові цілі стратегії кібербезпеки Чехії включають в себе захист інформаційно-комунікаційних систем від вразливостей, яким ці системи піддані, і зменшення потенційного збитку від атак на системи. Основний фокус стратегії доводиться на проблеми вільного доступу до інформаційних сервісів, цілісності і конфіденційності даних в кіберпросторі Чеської Республіки. Стратегія достатньо інтегрована та узгоджується з іншими нормативно-правовими документами Чеської Республіки.

Франція орієнтується на те, щоб інформаційні системи були здатні протистояти подіям в кіберпросторі, які можуть негативно вплинути на доступність, цілісність і конфіденційність інформації. Франція робить упор на технічні засоби захисту інформації, боротьбу з кіберзлочинністю і встановлення кіберзахисту.

Стратегія Німеччини закладає основу для безпеки критично важливих інформаційних систем. Німеччина зосереджена на запобіганні і кримінальному переслідуванні кібератак, а також на запобігання виходу з ладу IT-обладнання, викликаного випадковими чинниками. Особливо останнє стосується критично важливих інформаційних систем. У стратегії аналізується, чи потрібно проводити додаткові дії (і якщо так, то де саме) щодо захисту IT-систем шляхом надання основних функцій безпеки, сертифікованих державою, а також підтримкою малого і середнього бізнесу за допомогою створення нової робочої групи.

Литва орієнтується на визначення цілей і заходів, спрямованих на розвиток обороту електронної інформації, а також забезпечення її конфіденційності, доступності та цілісності в кіберпросторі. Крім того, стратегія Литви спрямована на захист персональних даних, телекомунікаційних мереж, інформаційних систем і критично важливих інфраструктур від порушення безпеки і кібератак. У стратегії також визначені заходи, реалізація яких буде гарантувати повною безпеку роботи в кіберпросторі.

Усвідомлюючи вразливість інформаційно-комунікаційних технологій, стратегія Люксембургу стверджує, що найважливіше – громадська та економічна безпека. У стратегії також наголошується на важливості інформаційно-комунікаційних технологій для економічного зростання, окремих громадян і суспільства в цілому. Стратегія працює за п'ятьма напрямами: захист ключової інформаційної інфраструктури і

своєчасна реакція на інциденти безпеки; модернізація нормативно-правової бази, державне і міжнародне співробітництво; навчання та інформування; просування стандартів.

Голландія, з одного боку, прагне до безпечних і надійних інформаційно-комунікаційних систем, побоюючись серйозних порушень в цих системах, а з іншого боку, визнає необхідність свободи і відкритості Інтернет-простору. У стратегії дається визначення кібербезпеки, яку розуміють як захищеність від збоїв і неправильної експлуатації інформаційно-телекомунікаційних систем. Політика Великобританії спрямована на розвиток кібербезпеки і має інноваційну спрямованість. Її метою є виведення на перше місце країни з інновацій, інвестицій та якості сервісів у сфері інформаційно-телекомунікаційних технологій, і тим самим, в повній мірі скористатися всіма перевагами і достоїнствами кіберпростору [2-4].

У середовищі, де постійно з'являються і еволюціонують кібернетичні загрози, державна політика країн Євросоюзу ґрунтується на гнучких, оперативних стратегіях кібернетичної безпеки. Транскордонний характер загроз змушує країни вступати в тісну міжнародну взаємодію, така співпраця необхідна не тільки для ефективної підготовки до кібератак, а й для своєчасної реакції на них, вироблення узгоджених механізмів запобігання. Саме формування національної державної стратегії кібербезпеки є основою для вироблення ефективної державної політики.

Питання забезпечення кібернетичної безпеки є надзвичайно актуальними і для України. Однак, насьогодні відсутній єдиний документ, який би визначав

стратегічні підходи, механізми, інструменти, заходи з протидії викликам і загрозам у зазначеній сфері.

Формування пакету документів нормативно-правового характеру з даного питання дозволить, визначити правові та організаційні засади державної політики у цій сфері, основні принципи та напрями забезпечення кібербезпеки держави.

Основними напрямами забезпечення кібернетичної безпеки України сьогодні мають бути наступні:

розвиток інформаційної інфраструктури держави, забезпечення безпечного функціонування об'єктів критичної інформаційної інфраструктури;

розвиток міжнародного співробітництва у сфері кібербезпеки;

зосередження ресурсів і посилення координації діяльності правоохоронних, розвідувальних і контррозвідувальних органів України для боротьби з проявами кіберзлочинності та кібертероризму;

забезпечення ефективного застосування Збройних Сил України для адекватної відповіді реальним та потенційним кіберзагрозам національному сегменту кіберпростору;

розвиток пріоритетних напрямів науки і техніки як основи створення високих інформаційних технологій;

підтримка виробників продукції та послуг у сфері кібербезпеки на засадах стимулювання вітчизняних виробників;

адаптація законодавства України до норм ЄС, створення нормативно-правових та економічних передумов для розвитку інформаційної інфраструктури держави, підвищення її стійкості до кібератак, спроможності держави більш ефективно захищати національні інтереси у кіберпросторі;

забезпечення неухильного дотримання власниками об'єктів критичної інформаційної інфраструктури вимог законодавства у сфері захисту державних інформаційних ресурсів, криптографічного та технічного захисту інформації, захисту персональних даних;

підвищення рівня обізнаності суспільства щодо ризиків, викликів і загроз у кіберпросторі.

Конвенція про кіберзлочинність ділить її на наступні категорії:

– правопорушення проти конфіденційності, цілісності і доступності комп'ютерних систем;

– правопорушення, пов'язані з комп'ютерами;

– правопорушення, пов'язані з дитячою порнографією;

– правопорушення, пов'язані з порушенням авторських прав [5].

Серйозною перешкодою в питанні забезпечення безпеки «в мережі» є відсутність єдиного центру прийняття рішень та реалізації політики держави. За фактом, відповідальність в питанні кібернетичної безпеки розділяється між декількома структурами, які сьогодні діють не достатньо узгоджено.

В державній стратегії кібернетичної безпеки мають бути розглянуті та висвітлені положення, що стосуються наступного:

побудова принципової державної моделі, спрямованої на забезпечення кібербезпеки;

визначення відповідного державного механізму, що дозволяє приватним і державним зацікавленим сторонам обговорювати і затверджувати заходи, пов'язані з проблемою кібербезпеки;

планування та визначення необхідної політики і регулюючих механізмів, чітке позначення ролей, прав і відповідальності для приватного і державного сектора;

розробка системного та інтегрованого підходу до державного управління ризиками;

визначення і позначення цілей інформаційних програм, покликаних прищепити користувачам нові моделі поведінки і моделі роботи.

доказ необхідності нової програми освіти, що робить упор на навчання ІТ-фахівців і професіоналів у сфері кібербезпеки.

Принципами, на яких має ґрунтуватись та здійснюватися державна політика забезпечення кібернетичної безпеки України мають бути наступні:

верховенство права, законності та пріоритету додержання прав і свобод

людини і громадянина;

невідворотність відповідальності за вчинення кібернетичних злочинів;

пріоритетність запобіжних заходів;

комплексне здійснення правових, організаційних, технічних, криптографічних, інформаційних та інших заходів;

партнерство держави та приватного сектору з метою вироблення нових,

більш оптимальних рішень;

пріоритетний розвиток та підтримка вітчизняної науково-інноваційної сфери;

відповідальність суб'єктів забезпечення кібернетичної безпеки за захист національної інформаційної інфраструктури;

дієвість, комплексність і постійність заходів забезпечення кібернетичної безпеки держави;

участь інституцій громадянського суспільства у забезпеченні кібернетичної безпеки держави;

співпраця на міжнародному рівні, з метою вироблення єдиних підходів та ефективної взаємодопомоги протидії кіберзагрозам.

Висновки та напрями подальших досліджень. Слід констатувати, що в Україні механізми державного забезпечення кібербезпеки, все ще знаходяться на етапах становлення. Деякі з них потребують вдосконалення, однак для розробки більшості та їхніх окремих елементів передусім бракує концептуального обґрунтування. Крім того, в

Україні досі відсутні критично важливі елементи національної системи кібернетичної безпеки.

Забезпечення кібернетичної безпеки України має відбуватись із врахуванням існуючої нормативно-правової бази, а саме: положень Конституції, Закону України «Про основні засади внутрішньої та зовнішньої політики», Закону України «Про основи національно безпеки», Стратегії національної безпеки України та Доктрини інформаційної безпеки України.

Вкрай необхідним є формування дієвих механізмів державного управління забезпеченням єдиної системи кібернетичного захисту, яка б пов'язувала роботу різних структур і підрозділів і стала центром політики держави в сфері кібернетичної безпеки країни.

Список використаних джерел:

1. Дубов Д.В. Кібербезпека : світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. –К. : НІСД, 2011. – 30 с.
2. H. Luiijf, K. Besseling, M. Spoelstra, P. de Graaf, Ten National Cyber Security Strategies: a comparison, CRITIS 2011 – 6th International Conference on Critical information infrastructures Security, September 2011.
3. Европейское агентство по сетевой информационной безопасности (ENISA), 201 [Електрон. ресурс]. – Режим доступу: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss
4. ROADMAP: Proposal on a European Strategy for Internet Security http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf
5. Конвенція про кіберзлочинність / Рада Європи; Конвенція, Міжнародний документ від 23.11.2001 р. [Електрон. ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_575

In article the experience of foreign countries in providing of cybernetic safety is considered. The need of national strategy of ensuring cyber-safety acceptance is actual. The main principles of the state policy in the cyber-safety formation are defined.

Relevance of the subject. The national security of Ukraine, its economic prosperity and social wellbeing more and more depend on availability, integrity and confidentiality of the information resources provided with information and communication technologies, or in a broader sense – cyber-spaces.

It should be noted that providing mechanisms of the state cyber-safety in Ukraine are still at a formation stage. Some of them have to be improved; however first of all for the development of the majority of them as well as their separate parts there isn't appropriate conceptual substantiation. Besides, there aren’t crucial elements of national system of cybernetic safety still in Ukraine.

Ensuring of Ukrainian cybernetic safety has to occur taking into account the existing standard and legal base, namely: Constitution provisions, the Law of Ukraine "About the basic principles of domestic and foreign policy", the Law of Ukraine "About National safety", Strategy of national security of Ukraine and the Doctrine of information security of Ukraine.

Formation of effective mechanisms of public administration by providing uniform system of cybernetic protection which connected work of various structures and divisions are extremely necessary and became the main policy of the state in the sphere of cybernetic safety of the country.