УДК 621.396

Живило Є.О. (ВІТІ)
Черноног О.О. (ГШ ЗС України)

НАПРЯМИ СТВОРЕННЯ ТА РОЗБУДОВИ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ

У статті визначені пріоритети та шляхи вдосконалення державної політики забезпечення кібербезпеки України. Запропонована загальнодержавна модель побудови Національної системи кібербезпеки, визначені її функціональні елементи. З метою створення дієвої вертикалі органів державного управління у сфері кібербезпеки організаційно до моделі Національної системи кібербезпеки запропоновано включити перелік суб'єктів забезпечення кібербезпеки враховуючи діюче нормативно-правове поле.

Живило Є.О., Черноног О.О. Направления создания и развития национальной системы кибербезопасности. *В статье определены приоритеты и пути совершенствования государственной политики обеспечения кибербезопасности Украины. Предложенная общегосударственная модель построения Национальной системы кибербезопасности, определенны ее функциональные элементы. С целью создания результативной вертикали органов государственного управления в сфере кибербезопасности организационно к модели Национальной системы кибербезопасности предложено включить перечень субъектов обеспечения кибербезопасности учитывая действующее нормативно-правовое поле.*

E. Zhivilo, O. Chernonog Directions for the creation and development of a national cybersecurity system. *The article outlines priorities and ways to improve the state policy of ensuring cybersecurity of Ukraine. The proposed national model for building the National System of Cybersecurity, its functional elements are defined. In order to create an effective vertical of the state administration bodies in the field of cybersecurity, it is proposed to include the list of subjects of ensuring cybersecurity in the model of the National Cybersecurity System taking into account the current regulatory and legal framework.*

Ключові слова: *кібербезпека, суб'єкти забезпечення кібербезпеки, Національа система кібербезпеки.*

Постановка завдання в загальному вигляді

Останнім часом проблема забезпечення національної безпеки зміщується у бік не стільки декларованої, скільки реально розглядуваної.

Передусім, це обумовлено активізацією зовнішніх загроз безпечного розвитку України: посиленням мілітаризації держав у регіоні, використанням положення енергетичної та торговельно-економічної залежності нашої країни, посиленням економічного та інформаційного тиску на неї тощо.

Разом із тим, зовнішні загрози посилюються наявністю внутрішніх викликів національній безпеці, зокрема, йдеться про розбалансованість та незавершеність системних реформ, зниження обороноздатності держави, боєздатності Збройних сил України, незадовільний стан фінансування, складне економічне становище.

Слід констатувати, що сучасний стан системи національної безпеки [1], не забезпечує у повному обсязі нейтралізацію існуючих загроз і викликів. Національна безпека забезпечується проведенням єдиної державної політики у всіх сферах життєдіяльності, системою заходів економічного, політичного та організаційного характеру, адекватним загрозам і небезпекам життєво важливих інтересів особи, суспільства і держави.

Враховуючи той факт, що система національної безпеки є багатокомпонентною, звичайно постає потреба в існуванні спеціальної підсистеми, мета функціонування якої полягала б у забезпеченні функціонування та розвитку цієї системи, тобто у забезпеченні життєздатності її системостворюючих елементів, зокрема національних інтересів людини, суспільства, держави.

Такою системою і є система забезпечення національної безпеки [2], а також національна система кібербезпеки.

Ці та інші фактори і підтверджують висновок про ***актуальність*** даної статті.

Україна змушена у стислі строки сформувати цілісну позицію щодо кіберпростору як поля нового геополітичного протистояння, а державні зусилля у сфері зовнішньої політики природно мають бути спрямовані на досягнення „бажаного майбутнього", яке б найповніше відповідало її довгостроковим інтересам.

В умовах протистояння провідних країн світу у кіберпросторі, створення умов для безпечного функціонування кіберпростору України, його використання в інтересах особи, суспільства і держави, протидія випадкам кіберзлочинності є першочерговим заходом, на етапі створення національної системи кібербезпеки як складової системи забезпечення національної безпеки України [3].

Для забезпечення кібербезпеки України держава у партнерстві із суспільством та приватним сектором, а також громадянами, має підвищити ефективність державного управління у цій сфері, здійснити впорядкування нормативно-правового поля та забезпечити розвиток інфраструктури кібербезпеки.

Як показав ***аналіз літератури***, саме з впровадження сучасних інформаційних технологій в електронні системи управління урядового, оборонного, економічного та інших секторів провідних країн світу обумовив посилення залежності безпечного функціонування цих систем від зовнішнього кібернетичного впливу.

За таких обставин проблеми забезпечення кібернетичної безпеки будь-якої країни набувають важливого значення і вимагають від керівництва держави впровадження комплексу нормативно-правових та організаційних заходів, спрямованих на нарощування можливостей захисту національного кіберпростору [4, 5, 6].

Метою даної статті є надання пропозицій, щодо варіанту створення єдиної загальнодержавної моделі побудови Національної системи кібербезпеки [7], розробленої з урахуванням досвіду країн Європейського Союзу та НАТО.

Виклад основного матеріалу

Національна система кібербезпеки (НСКБ) – має об’єднати у форматі співробітництва центральні органи виконавчої влади, військові формування, правоохоронні органи, органи державного регулювання у сфері інформатизації, телекомунікацій та захисту інформації, органи місцевого самоврядування, наукові установи і організації, а також зацікавлені громадські організації, професійні асоціації, представництва міжнародних організацій в Україні, представників приватного сектору, а також підприємства, установи та організації незалежно від форм власності, які здійснюють діяльність, пов’язану із забезпеченням функціонування або безпеки національного сегмента кіберпростору, для своєчасного запобігання кіберзагрозам, забезпечення належного рівня обороноздатності та безпеки держави в кіберпросторі, оперативного виявлення, запобігання, протидії та розслідування злочинних проявів, заснованих на використанні інформаційних та інформаційно-комунікаційних технологій.

НСКБ (Рис. 1) має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об’єднань, а також підприємств, установ та організацій незалежно від форми власності, які проводять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об’єктів критичної інформаційної інфраструктури.

В рамках НСКБ пропонується передбачити такі функціональні елементи:

система моніторингу та реагування на кіберзагрози (моніторингу та оцінки загроз, реагування розслідування тощо) під час виявлення кібератак та кіберінцидентів на об’єктах інформаційної інфраструктури (передбачає швидку ідентифікацію зловмисників, вжиття заходів із локалізації шкоди, викликаної їх діями, та проведення розслідування кіберзлочинів);

система кібербезпеки у воєнній сфері та сфері оборони;

система кіберзахисту критичної інформаційної інфраструктури.

При формуванні вітчизняної моделі побудови НСКБ слід врахувати [7] такі особливості:

на сьогодні державні органи в секторах, які в європейських країнах належать до критичної інфраструктури, задіяні переважно для регулювання економічних і майнових

питань, у той час як невизначеними залишаються структури, які мають безпосередньо відповідати за питання кібербезпеки;

Рис. 1 Варіант єдиної загальнодержавної моделі побудови Національної системи кібербезпеки

забезпечення кібербезпеки у приватному секторі здійснюється на власний розсуд власника тієї чи іншої системи;

відсутність єдиного координаційного центру з питань забезпечення кібербезпеки суттєво ускладнює, уповільнює, а у деяких випадках й унеможливлює взаємодію органів державного управління та вжиття необхідних заходів з реагування на кібернетичні злочини та інциденти кібербезпеки, які відрізняються високим ступенем латентності;

важливими показниками ефективності НСКБ є: оперативність оцінки ситуації, термін прийняття відповідних рішень, час реагування, достатність вжитих заходів;

кібернетичний суверенітет і кібермогутність держави базуються на сукупності змістовних чинників, до яких належать [8, 9]: інноваційний потенціал країни та її здатність самостійно створювати новітні технології; ступінь розвитку ІТ-компаній, а де-факто – наявність національних ІТ-ТНК; ступінь розвитку внутрішнього ринку (передусім відповідної вимогам сучасності ІТ-інфраструктури); гуманітарний показник впливу культури країни на загальний контент мережі; військовий потенціал держави (передусім можливість здійснювати кібератаки та захищатися від них); зовнішньополітична компонента (включно з можливостями впливу на міжнародні структури, задіяні в управлінні Інтернетом).

Для створення дієвої вертикалі органів державного управління у сфері кібербезпеки [10] організаційно до НСКБ пропонується включити такі структурні елементи:

Орган стратегічного управління сферою кібербезпеки України – Рада національної безпеки і оборони України відповідно до Конституції України та у встановленому законом порядку має здійснювати координацію та контроль діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку України.

Орган оперативного управління сферою кібербезпеки України – Національний центр кібербезпеки при Президентові України (як центральний орган виконавчої влади зі спеціальним статусом у сфері кібербезпеки) [7];

Суб'єкти забезпечення кібербезпеки – органи державної влади та місцевого самоврядування, органи військового управління Збройних Сил України, інших військових формувань, правоохоронні органи, установи науково-методологічної підтримки, громадські

організації та професійні асоціації, створені за участю представників приватного сектору, а також об'єднання підприємств, установ та організацій незалежно від форми власності, які здійснюють діяльність, пов'язану із забезпеченням функціонування або безпеки національного сегмента кіберпростору. Основу національної системи кібербезпеки становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, на які мають бути покладені в установленому порядку такі основні завдання:

на Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції – здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснення військової співпраці з НАТО, пов'язаної з безпекою кіберпростору та сумісним захистом від кіберзагроз; забезпечення у взаємодії з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України кіберзахисту власної інформаційної інфраструктури;

на Державну службу спеціального зв'язку та захисту інформації України [11] – формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, державний контроль у цих сферах; координація діяльності інших суб'єктів кібербезпеки щодо кіберзахисту; здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків, інформування про кіберзагрози та відповідні методи захисту від них; забезпечення функціонування державного центру кіберзахисту; проведення аудиту захищеності об'єктів критичної інформаційної інфраструктури на вразливість;

на Службу безпеки України – попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством, а також щодо готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидія кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України; розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечення реагування на комп'ютерні інциденти у сфері державної безпеки;

на Національну поліцію України – забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі;

на Національний банк України – формування вимог щодо кіберзахисту критичної інформаційної інфраструктури у банківській сфері;

на розвідувальні органи України – здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.

Зі складу зазначених суб'єктів доцільно виділити суб'єкти забезпечення кібербезпеки постійної готовності – органи державної влади, сили та засоби яких спеціально виділені для перебування у постійній готовності до реагування на кіберзагрози та оперативного вирішення завдань забезпечення кібербезпеки.

До складу суб'єктів забезпечення кібербезпеки постійної готовності доцільно віднести:

РНБО України;

Національний центр кібербезпеки при Президентові України;

Міністерство внутрішніх справ України;

Службу безпеки України;

Міністерство оборони України;

Генеральний штаб Збройних сил України;

Державну службу спеціального зв'язку та захисту інформації України;

Головну професійну асоціацію (організацію) у сфері кібербезпеки приватного сектору держави.

До основних підрозділів суб'єктів забезпечення кібербезпеки постійної готовності слід віднести:

Центр за напрямком боротьби з кіберзлочинністю у складі Міністерства внутрішніх справ України;

Центр за напрямком боротьби з кібертероризмом у складі Служби безпеки України;

Центр за напрямком забезпечення захисту інформації та кібербезпеки у складі Збройних сил України;

Центр за напрямком реагування на комп'ютерні надзвичайні події (CERT-UA) у складі Державної служби спеціального зв'язку та захисту інформації України;

Недержавний центр за напрямком забезпечення кібернетичного захисту у складі Головної професійної асоціації (організації) у сфері кібербезпеки приватного сектору держави.

У центральних органах виконавчої влади та органах місцевого самоврядування доцільно створити відділи за напрямом забезпечення кібернетичного захисту інформаційної інфраструктури.

У складі підприємств, установ або організацій будь-яких форм власності, діяльність яких пов'язана із забезпеченням функціонування критичної інформаційної інфраструктури держави, доцільно створити відповідні відділи (відділення) за напрямком забезпечення кібернетичного захисту.

Об'єкти кіберзахисту.

До складу об'єктів кіберзахисту належать об'єкти інформаційної інфраструктури, інформаційні, телекомунікаційні та інформаційно-телекомунікаційні системи, в яких здійснюється обробка державних інформаційних ресурсів або інформації, вимога щодо кіберзахисту якої встановлена законом або власником системи.

За узгодженими з усіма суб'єктами кібербезпеки держави критеріями, зі складу об'єктів кіберзахисту доцільно виділити об'єкти критичної інформаційної інфраструктури (об'єкти, що потребують першочергового захисту від кібератак).

Мають бути створені умови для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інфраструктури, до забезпечення кібербезпеки України.

Зокрема, мають бути врегульовані питання щодо обов'язковості вжиття ними заходів із забезпечення захисту інформації та кіберзахисту відповідно до вимог законодавства, а також щодо сприяння ними державним органам у виконанні завдань із забезпечення кібербезпеки та кіберзахисту [12].

Держава повинна сприяти залученню наукових установ, навчальних закладів, організацій, громадських об'єднань і громадян до розробки та реалізації заходів із кібербезпеки і кіберзахисту.

Таким чином, кібербезпека стала пріоритетним питанням нормативно-правової бази органів інформаційно-комп'ютерного захисту, але на сьогоднішній день не існує уніфікованої моделі побудови національної системи кібербезеки.

Сьогодні для України актуальною є ціла низка проблемних питань створення та розбудови системи кібернетичної безпеки, розв'язання яких потребуватиме часу та певних зусиль як з боку держави, так і бізнесу/науково-дослідних установ.

Напрямки майбутніх досліджень

В умовах невизначеності кібербезпекової політики України та з урахуванням її знаходження на перетині інтересів основних геополітичних гравців такий стан речей

зумовлює необхідність якнайшвидшої розбудови усіх основних секторів держави за напрямом забезпечення кібербезпеки.

Тому з урахуванням досвіду провідних країн світу в статті запропоновано модель національної системи кібербезпеки та першочергові напрями діяльності державного та приватного секторів з розвитку її складових.

Впровадження одержаних результатів дасть можливість у найкоротші терміни розробити та впровадити ефективні організаційні заходи з підвищення рівня кібербезпеки України, що позитивно вплине на розвиток та стале функціонування усіх сфер діяльності держави.

Подальшими кроками з удосконалення сфери кібербезпеки держави мають стати пошук та вироблення науково-технічних рішень з удосконалення технічних складових національної системи кібербезпеки.

ЛІТЕРАТУРА

1. Стратегія кібербезпеки України від 15.03.2016 р. [Електронний ресурс]. – Режим доступу :http://zakon3.rada.gov.ua/laws/show/96/2016.

2. Концепція розвитку сектору безпеки і оборони України від14.03.2016 р. [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/92/2016.

3. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – Вип. 1. – С. 312 – 320.

4. Framework for Improving Critical Infrastructure Cybersecurity / 2012 / [Електронний ресурс]. – Режим доступу: http://www.nist.gov/cyberframework/ upload/cybersecurity-framework-021214-final.pdf.

5. National Cybersecurity Protection Act of 2014 [Електронний ресурс]. – Режим доступу: https://www.congress.gov/bill/113th-congress/senate-bill/2519/text.

6. Computer Security Incident Handling Guide. NIST Special Publication 800-61 Revision 2 / 2012 / [Електронний ресурс]. – Режим доступу: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

7. Положення про Національний координаційний центр кібербезпеки від 07.06.2016р. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/242/2016.

8. Стратегія національної безпеки України від 26.05.2015 р. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/555/2015.

9. Доктрина інформаційної безпеки України // http://www.president.gov.ua/documents/472017-21374.

10. Турчинов заявив про нові кіберзагрози з боку Росії, 11 липня 2016 р. [Електронний ресурс]. – Режим доступу: https://www.ukrinform.ua/rubric-politycs/2048633-turcinov-zaaviv-pro-novi-kiberzagrozi-z-boku-rosii.html.

11. Про Державну службу спеціального зв’язку та захисту інформації: Закон України від 23.02.2006р. [Електронний ресурс]. – Режим доступу :http://zakon2.rada.gov.ua/laws/show/3475-15.

12. Ткаченко В.І. Шляхи формування системи забезпечення національної безпеки / В. І. Ткаченко, Є.Б. Смірнов, О.О. Астахов // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2015. – № 2. – С. 3 – 8.