Електронне наукове фахове видання "Державне управління: удосконалення та розвиток" включено до переліку наукових фахових видань України з питань державного управління (Наказ Міністерства освіти і науки України від 06.11.2014 № 1279)

ДЕРЖАВНЕ УПРАВЛІННЯ удосконалення та розвиток

Академія муніципального управління

Переглянути у форматі pdf

Р. В. Лук`янчук

УДК 351:316.77

Р. В. Лук`янчук,
здобувач Інституту законодавства Верховної Ради України, м. Київ

ДЕРЖАВНЕ УПРАВЛІННЯ КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ: ШЛЯХИ ВДОСКОНАЛЕННЯ В СУЧАСНИХ УМОВАХ

R. V. Lukianchuk,
Researcher, The Legislation Institute of the Verkhovna Rada of Ukraine, Kyiv

CYBER SECURITY GOVERNANCE: THE DIRECTIONS OF IMPROVEMENT IN MODERN CONDITIONS

У статті розкрито особливості формування системи державного управління кібербезпекою з урахуванням досвіду деяких зарубіжних країн. Проаналізовано акти законодавства України в яких окреслено перспективні напрями діяльності держави щодо розбудови національної системи кібербезпеки. Визначено проблемні питання державного регулювання та здійснення оцінки стану захищеності державних інформаційних ресурсів, захисту об'єктів вітчизняної критичної інформаційної інфраструктури. Деталізовано необхідні законодавчі ініціативи та напрями вдосконалення системи державного управління кібербезпекою в умовах «гібридної» війни.

In the article main features of formation of the system of cyber security governance using the experience of some foreign countries are considered. The acts of legislation of Ukraine which outlines the promising directions of state capacity in the aspects of development of the national system of cyber security are analyzed. Problem questions of state regulation and implementation of the evaluation of the security of state information resources, protection of objects of national critical information infrastructure are defined. The necessary legislative initiatives and directions of improvement of the system of cyber security governance in the conditions of the "hybrid" war are detailed.

Ключові слова: *державне управління кібернетичною безпекою, державні інформаційні ресурси, інформаційно-комунікаційні технології, гібридна війна, вітчизняний кібернетичний простір, національна система кібербезпеки, оцінка стану захищеності державних інформаційних ресурсів, об'єкти критичної інформаційної інфраструктури, кіберзлочинність, кібертероризм.*

Key words: *cyber security governance, the state information resources, information and communication technologies, hybrid war, domestic cyberspace, national system of cyber defense, assessment of the protection of the national information resources, objects of critical information infrastructure, cybercrime, cyber terrorism.*

Постановка проблеми. Україна відсвяткувала 24-у річницю Незалежності, проте ще й досі поза увагою державного апарату залишаються питання вдосконалення системи державного управління кібернетичною безпекою, хоча вже другий рік триває «інформаційна війна» з країною-агресором - Російською Федерацією, що потребує активізацію діяльності держави у напрямку розробки концептуальних засад забезпечення кібернетичної безпеки, визначення алгоритму здійснення заходів з метою захисту вітчизняного кібернетичного простору.

За таких умов формування і використання національних інформаційних ресурсів — одна з ключових проблем становлення та розвитку національного інформаційного простору України [1, с.94]. Загальновідомо, що саме інформаційні ресурси є важливою складовою стратегічних ресурсів держави, значення якої зростає із розвитком інформаційно-комунікаційних технологій та їх використанням в усіх сферах суспільного життя. Саме тому ефективне державне управління інформаційними ресурсами є важливою умовою забезпечення кібернетичної безпеки та реалізації виваженої державної політики у сфері інформатизації.

В умовах «гібридної» війни до останніх прикладів мережевих атак з боку РФ на вітчизняний сегмент кіберпростору та посягань на державні інформаційні ресурси можливо віднести несанкціоноване втручання в систему управління сайтом Львівської облдержадміністрації 18 лютого та 19 серпня 2015 року, коли хакери у першому випадку встановили на вказаному порталі відеопропаганду ідеології «ДНР», а у другому - розмістили на ньому фото президента та чиновників РФ з метою пропаганди «руського миру», приниження честі та гідності пересічених українців – користувачів мережі Інтернет, нівелювання авторитету органів державної влади, внаслідок чого правоохоронцями сайт було заблоковано [2].

Зазначене надає підстави стверджувати, що існуюча система державного управління кібернетичною безпекою має певні недоліки, не спроможна своєчасно реагувати на кіберзагрози, працювати на упередження мережевих кібернетичних атак на вітчизняний кібернетичний простір, особливо в умовах «гібридної» війни з РФ і потребує оптимізації.

Аналіз останніх досліджень і публікацій. Дослідження проблем забезпечення інформаційної безпеки держави досліджували: А.Марущак, В. Панченко, В.Петрик, В.Ліпкан та інші фахівці. Проблемні питання забезпечення кібернетичної безпеки розглядали у своїх працях: В. Бурячок, А. Бабенко, В. Бутузов, В. Гавловский, В. Голубєв, С. Гнатюк, Д. Дубов, О. Корченко, В. Номоконов, В. Петров, І. Рязанцева, В. Тулупов, В. Шеломенцев. Висвітлення проблемних питань підготовки фахівців у сфері забезпечення кібербезпеки певною мірою здійснювали: О. Баранов, В. Богуш, Ю. Онищенко, О. Орлов та інші. Проте визначення шляхів

вдосконалення системи державного управління кібернетичною безпекою в сучасних умовах жоден із вказаних фахівців не конкретизував, що посилює актуальність тематики обраного наукового дослідження.

Невирішені раніше частини загальної проблеми.

В умовах масового поширення інформаційно-комунікаційних технологій в масштабах світового інформаційного простору, необмежених можливостей інформаційного обміну, забезпечення кібербезпеки залишається одним із глобальних завдань світової спільноти. Враховуючи існуючі тенденції передових країн світу щодо пошуку оптимальної моделі забезпечення кібернетичної безпеки, протидії викликам та загрозам у кіберпросторі, більшість держав активно модернізують власні сектори безпеки та оборони, особливо в контексті можливого використання мережі Інтернет державою-супротивником з метою проведення військових спеціальних інформаційних операцій, спричинення шкоди державним інформаційним ресурсам на об'єктах критичної інформаційної інфраструктури, знищення та блокування систем життєзабезпечення у вітчизняному кібернетичному просторі.

В сучасних умовах кібератаки можуть бути здійснені з будь-якого місця, яке встановити та ідентифікувати є складним завданням: Інтернет-кафе, Wi-Fi системи або із застосуванням комп'ютерів третіх осіб [3, с. 101]. Вплив інформаційних загроз на структури державної влади, які відповідальні за підготовку і ухвалення рішень, реалізація яких безпосередньо впливає на безпеку країни, може призводити до виникнення надзвичайних ситуацій в державі і суспільстві, значним збиткам із-за порушення функціонування систем зв'язку, контролю і управління та просочування інформації, яка містить державну таємницю [4, с.231].

Виходячи із реалій сьогодення, кіберпростір все ще залишається не повністю нормативно врегульованим на міжнародному рівні, тому спецоперації, що здійснюються в ньому військовими чи розвідувальними підрозділами, не підпадають під визначення «акту війни». Фактично, йдеться про можливість забезпечити ефект військового втручання без подальших офіційних санкцій як з боку держави, що зазнала нападу, так і світового співтовариства.

З огляду на рівень проникнення ІКТ у всі критично важливі сфери життєдіяльності людини та держави, не виключається бажання деяких держав світу продемонструвати своє домінування у міжнародному кіберпросторі. Крім того, це призводить до необхідності чіткої регламентації засад державної політики більшості провідних держав в питанні контролю за власним кіберпростором, передбачає необхідність визначення пріоритетів державного управління кібербезпекою. Активність з боку провідних держав світу у кіберпросторі, формування потужних транснаціональних злочинних хакерських груп, що спеціалізуються на злочинах в кіберпросторі, обумовлюють необхідність вдосконалення вітчизняного безпекового сектору.

Щодо нашої держави, то в умовах «гібридної» війни з РФ, її сателітами «ДНР» та «ЛНР» триває протистояння в інформацій сфері, що вимагає від політичного керівництва, виходячи із зарубіжного досвіду, оперативного формування сучасної системи державного управління кібернетичною безпекою.

Мета публікації – визначити шляхи вдосконалення системи державного управління кібернетичною безпекою в контексті розбудови національної системи кібербезпеки та її складових.

Виклад основного матеріалу. Постійно зростаючий потенціал використання мережі Інтернет у військових цілях, провокує провідні країни світу - США, Японію, Францію, Великобританію, Росію, Китай протягом останніх років здійснити модернізацію власних секторів безпеки й, передусім, кібернетичної, віддаючи при цьому головну роль проблемі завоювання інформаційної переваги в управлінні військами (силами) і зброєю, а також удосконаленню нормативно-правової бази [5, с. 104].

У мережі Інтернет США, Китай та Російська Федерація залишаються лідерами за кількістю проведених кібератак. Кожної секунди у світі відбувається до 2500 тисяч DDoS-атак. З серпня 2014 року на сайті http://map.norsecorp.com розміщена онлайн карта хакерських спрямувань в режимі реального часу у глобальній мережі Інтернет.

Як свідчить зарубіжний досвід, процеси реформування сектору безпеки з метою вдосконалення державного управління системою кібернетичної безпеки передбачають активізацію діяльності держави за такими напрямами: розробка та затвердження нормативних документів, переважно стратегій, положення яких визначають напрямки діяльності держави у сфері забезпечення кібернетичної безпеки; безпосереднє реформування системи управління сектором безпеки, що передбачає створення спеціалізованих підрозділів, управлінських структур з метою оперативної протидії кіберзагрозам; збільшення чисельності підрозділів, задіяних у системі гарантування кіберзахисту; проведення роз'яснювальної роботи серед населення щодо визначення реальних та потенційних кіберзагроз; сприяння розвитку міжнародного співробітництва у сфері забезпечення транснаціональної кібернетичної безпеки.

Аналіз законодавства більшість держав світу дозволяє підсумкувати, що більшість з них мають фундаментальні акти законодавства - національні стратегії забезпечення кібербезпеки, положення яких визначають середньо- та довгострокові пріоритети діяльності уряду країни щодо розбудови системи захисту кіберпростору, деталізують завдання державних органів у вказаній сфері, визначають повноваження спеціальних підрозділів у складі військових формувань, які є відповідальними за гарантування захисту національного кіберпростору.

Слушно вказує О. Баранов, що практично всі національні стратегії щодо забезпечення кібербезпеки і переважна більшість експертів пов`язують проблематику кібербезпеки саме з використанням у процесі людської діяльності комп'ютерних систем і телекомунікаційних мереж (до останніх належить і мережа Інтернет) [6, с. 57].

Проте ще й досі Україна остаточно не визначилася із національною стратегією забезпечення кібернетичної безпеки, а стандарти НАТО у сфері гарантування кібернетичної безпеки, на жаль, не впроваджені в національне законодавство.

Побудова дієвої системи забезпечення кібернетичної безпеки вимагає від державних органів України чіткого визначення державної політики у цій сфері та випереджального реагування на динамічні зміни, що відбуваються у світі в сфері забезпечення кібернетичної безпеки. При цьому, вибір конкретних засобів і шляхів забезпечення кібернетичної безпеки України обумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам реальних та потенційних кібернетичних загроз життєво важливим інтересам людини і громадянина, суспільства і держави [7, с.300].

Останнє що було зроблено за вказаної проблематикою Урядом України – схвалення Кабінетом Міністрів України розпорядження від 05.11.2014 року №1135 «Про затвердження плану заходів щодо захисту державних інформаційних ресурсів» [8], яким визначено напрямки діяльності суб'єктів у сфері забезпечення кібербезпеки, створення захищеної інформаційної інфраструктури держави, дієвої системи протидії кіберзагрозам з урахуванням нових тенденцій, викликів і загроз у кіберпросторі протягом 2014 – 2016 років.

Зокрема у 2015 року з метою удосконалення правового регулювання сфери захисту державних інформаційних ресурсів передбачалося здійснити розробку проекту Указу Президента України «Про деякі заходи щодо захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах», забезпечити регламентацію процедури підтвердження відповідності засобів технічного захисту інформації; створити випробувальну лабораторію на базі Державного науково-дослідного інституту спеціального зв'язку та захисту інформації з метою сертифікації засобів захисту інформації.

Виходячи із аналізу вказаного нормативно-правового акта важливим завданням держави залишається забезпечення безпечного зберігання та сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті, зокрема Інтернет-ресурсів органів державної влади, з метою виявлення уразливих місць, їх аналізу та запобігання несанкціонованим діям з інформацією (знищення, блокування, порушення цілісності тощо).

На виконання зазначеного урядового нормативно-правового акта було прийнято наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 02 грудня 2015 року №660 «Про затвердження Порядку оцінки захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [9], відповідно до положень якого об'єктами оцінки стану захищеності виступають державні інформаційні ресурси, які обробляються в інформаційно-телекомунікаційних системах, незалежно від наявності в таких ІТС комплексної системи захисту інформації. Нормативно встановлено, що оцінка стану захищеності державних інформаційних ресурсів здійснюється Держспецзв'язку України з метою виявлення існуючих кіберзагроз.

Також на Адміністрацію Держспецзв'язку України покладено обов'язок протягом 2014 – 2015 років сформувати перелік об'єктів, що належать до критичної інформаційної інфраструктури держави, здійснити оцінку стану захищеності державних інформаційних ресурсів зазначених об'єктів, встановити порядок віднесення об'єктів до критичної інформаційної інфраструктури та перелік таких об'єктів [8].

В умовах «гібридної» війни об'єкти вітчизняної критичної інформаційної інфраструктури потребують першочергового захисту від можливих мережевих кібератак, у першу чергу, з боку сусідньої держави, проте зазначені заходи Адміністрацію Держспецзв'язку України остаточно ще й досі не реалізовані.

Авторитетно вказує В. Панченко, що основними етапами формування системи захисту національної інфраструктури від кіберзагроз є: 1) визначення основних понять та їх нормативне закріплення; 2) визначення критеріїв віднесення об'єктів до критично важливих; 3) укладання переліку таких об'єктів; 4) оцінка ризиків безпеки (здійснювалася або централізовано, або галузевими міністерствами відповідно до єдиної методики, розробленої науковими установами на замовлення державних органів); 5) планування заходів безпеки на основі результатів оцінювання ризиків із метою оптимізації витрат [10, с.96].

З метою вдосконалення системи державного управління кібербезпекою стратегічно важливим завданням для політичного керівництва нашої держави також залишається протидія сучасним кіберзагрозам, недопущення інформаційної експансії з боку інших держав з метою посягання на інформаційний суверенітет та вітчизняний кібернетичний простір, модернізація та вдосконалення програмного оснащення комплексів, що забезпечують роботу Команди реагування на комп'ютерні надзвичайні події України (CERT-UA). Потребує удосконалення спеціальна інформаційно-телекомунікаційна система функціонування органів виконавчої влади, у зв`язку з чим доцільним є створення комплексних систем захисту інформації з підтвердженою відповідністю в інформаційно-телекомунікаційних системах, на об'єктах інформаційної діяльності органів державної влади, підприємств, установ та організацій, що входять до сфери управління таких органів.

Окрім необхідності розробки стратегії забезпечення кібербезпеки, державна повинна прискорити розробку та впровадження новітніх конкурентоспроможних ІКТ в усіх сферах суспільного життя, посилити відповідальність в контексті 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; визначити напрямки розвитку національної інформаційної інфраструктури та її інтеграції до світової.

Висновки та пропозиції. В умовах «гібридної» війни для нашої держави важливим та необхідним залишається розробка й схвалення національної стратегії забезпечення кібербезпеки, створення захищеного національного сегменту кіберпростору; побудова ефективної та оперативної протидії будь-яким мережевим кібератакам, запобігання втручанню у внутрішні справи України і нейтралізація посягань на її інформаційні ресурси з боку інших держав, особливо РФ; посилення обороноздатності держави у кіберпросторі; зниження рівня уразливості об'єктів кіберзахисту; забезпечення повноправної участі України в загальноєвропейській та регіональних системах забезпечення кібербезпеки за участі НАТО; приєднання до міжнародної системи боротьби з кіберзлочинністю та кібертероризмом, забезпечення ефективної міжнародної співпраці у сфері забезпечення кібербезпеки, у тому числі із залученням фахівців Команди реагування (CERT-UA).

Враховуючи викладене, саме Уряд України є відповідальним за реалізацію виваженої державної політики у сфері забезпечення кібербезпеки, проте також необхідним є концентрація зусиль усіх державних органів, які опікуються питаннями захисту вітчизняного інформаційного простору.

Також вважається доцільним якнайшвидше здійснити розробку Національного плану забезпечення кібербезпеки на 2016-2020 роки, Концепції боротьби з кібертероризмом, прискорити створення державного реєстру об'єктів, що належать до критичної інформаційної інфраструктури, провести комплексну оцінку стану захищеності державних інформаційних ресурсів зазначених об'єктів, розробити порядок віднесення об'єктів до критичної інформаційної інфраструктури держави та визначити перелік таких об'єктів. Потребує удосконалення спеціальна інформаційно-телекомунікаційна система функціонування органів державної влади, у зв`язку з чим доцільним є створення комплексних систем захисту інформації з підтвердженою відповідністю в інформаційно-телекомунікаційних системах на об'єктах інформаційної діяльності органів державної влади, підприємств, установ та організацій, що входять до сфери управління таких органів.

Перспективи подальших досліджень.

В умовах «гібридної» війни не виключаються подальші спроби країни-агресора РФ та її сателітів «ДНР» та «ЛНР», інших країн світу, які розділяють політичний курс Кремля здійснювати мережеві кібератаки на державні інформаційні ресурси, створювати загрози національній системі кібербезпеки, що стимулює проведення подальших наукових досліджень з метою вдосконалення вітчизняної системи державного управління кібернетичною безпекою, визначення концептуальних засад забезпечення надійного захисту вітчизняного кібернетичного простору.

Література.

1. Нестеряк Ю.В. Державна інформаційна політика та управління національними інформаційними ресурсами / Ю.В. Нестеряк // Державне управління та місцеве самоврядування. — Збірник наукових праць. — Дніпропетровськ; ДРІДУ НАДУ. — 2013. — Вип. 1(16). — С. 94–104

2. Інформаційне повідомлення. Хакеры взломали сайт Львовской ОГА, разместив на нем фото Путина и чиновников РФ [Електронний ресурс]. – Режим доступу: http://www.unian.net/society/1113619-hakerskuyu-ataku-na-sayt-lvovskoy-oga-osuschestvili-iz-okkupirovannogo-kryima.html.

3. Савин Л.В. Сетецентричная и сетевая война. Введение в концепцию / Л.В. Савин – М.: «Евразийское движение» — 2011. – 130 с.

4. Орлов О.В. Державна політика підготовки кадрів з попередження кіберзлочинності в Україні / О.В. Орлов, Ю.М. Онищенко // Актуальні проблеми державного управління. - 2014. - № 1. - С. 230-236. - Режим доступу: http://nbuv.gov.ua/j-pdf/apdy_2014_1_32.pdf.

5. Бурячок В.Л. Кібернетична безпека — головний фактор сталого розвитку сучасного інформаційного суспільства / Бурячок В.Л. // Сучасна спеціальна техніка. — 2011. — № 3 (26). — С. 104-114.

6. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» / О.А. Баранов // Правова інформатика. – 2014. - №2 (42). – С.54- 62.

7. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). Науково-практичний журнал. – 2012. - №2 (28).-С.299-309.

8. Про затвердження плану заходів щодо захисту державних інформаційних ресурсів: Розпорядження Кабінету Міністрів України від 05 листопада 2014 року №1135 // Урядовий кур'єр, 06.12. 2014. №228.

9. Про затвердження Порядку оцінки захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах системах: Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 02 грудня 2015 року №660.

10. Панченко В.М. Зарубіжний досвід формування систем захисту критичної інфраструктури від кіберзагроз / Панченко В.М. // Інформаційна безпека людини, суспільства, держави. – 2012. - № 3 (10). – С. 91-100.

References.

1. Nesteryak Yu.V. *Derzhavna informatsiyna polityka ta upravlinnya natsional'nymy informatsiynymy resursamy* / Yu.V. Nesteryak // Derzhavne upravlinnya ta mistseve samovryaduvannya. — Zbirnyk naukovykh prats'. — Dnipropetrovs'k; DRIDU NADU. — 2013. — Vyp. 1(16). — S. 94–104

2. Informatsiyne povidomlennya. *Khakeri vzlomaly sayt L'vovskoy OHA, razmestyv na nem foto Putyna y chynovnykov RF* [Elektronnyy resurs]. – Rezhym dostupu: http://www.unian.net/society/1113619-hakerskuyu-ataku-na-sayt-lvovskoy-oga-osuschestvili-iz-okkupirovannogo-kryima.html.

3. Savyn L.V. *Setetsentrychnaya y setevaya voyna. Vvedenye v kontseptsyyu* / L.V. Savyn – M.: «Evrazyyskoe dvyzhenye» — 2011. – 130 s.

4. Orlov O.V. *Derzhavna polityka pidhotovky kadriv z poperedzhennya kiberzlochynnosti v Ukrayini* / O.V. Orlov, Yu.M. Onyshchenko // Aktual'ni problemy derzhavnoho upravlinnya. - 2014. - # 1. - S. 230-236. - Rezhym dostupu: http://nbuv.gov.ua/j-pdf/apdy_2014_1_32.pdf.

5. Buryachok V.L. *Kibernetychna bezpeka — holovnyy faktor staloho rozvytku suchasnoho informatsiynoho suspil'stva* / Buryachok V.L. // Suchasna spetsial'na tekhnika. — 2011. — # 3 (26). — S. 104-114.

6. Baranov O.A. *Pro tlumachennya ta vyznachennya ponyattya «kiberbezpeka»* / O.A. Baranov // Pravova informatyka. – 2014. - #2 (42). – S.54- 62.

7. Shelomentsev V.P. *Sutnist' orhanizatsiynoho zabezpechennya systemy kibernetychnoyi bezpeky Ukrayiny ta napryamy yoho udoskonalennya* / V.P. Shelomentsev // Borot'ba z orhanizovanoyu zlochynnistyu i koruptsiyeyu (teoriya i praktyka). Naukovo-praktychnyy zhurnal. – 2012. - #2 (28).-S.299-309.

8. *Pro zatverdzhennya planu zakhodiv shchodo zakhystu derzhavnykh informatsiynykh resursiv*: Rozporyadzhennya Kabinetu Ministriv Ukrayiny vid 05 lystopada 2014 roku #1135 // Uryadovyy kur"yer, 06.12. 2014. #228.

9. *Pro zatverdzhennya Poryadku otsinky zakhyshchenosti derzhavnykh informatsiynykh resursiv v informatsiynykh, telekomunikatsiynykh ta informatsiyno-telekomunikatsiynykh systemakh systemakh*: Nakaz Administratsiyi Derzhavnoyi sluzhby spetsial'noho zv"yazku ta zakhystu informatsiyi Ukrayiny vid 02 hrudnya 2015 roku #660.

10. Panchenko V.M. *Zarubizhnyy dosvid formuvannya system zakhystu krytychnoyi infrastruktury vid kiberzahroz* / Panchenko V.M. // Informatsiyna bezpeka lyudyny, suspil'stva, derzhavy. – 2012. - # 3 (10). – S. 91-100.

Стаття надійшла до редакції 08.09.2015 р.