УДК 351.86:351/354+004.056

ДОРОНІН І.М., *кандидат юридичних наук, доцент*

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У РЕАЛІЗАЦІЇ ОКРЕМИХ ФУНКЦІЙ ДЕРЖАВИ

Анотація. *У статті на підставі аналізу документів стратегічного планування держави, актів законодавства та проектів законодавчих актів, досліджено питання реалізації окремих функцій держави у формі правового регулювання забезпечення кібербезпеки.*

Ключові слова: *кібербезпека, стратегічне планування, оборона, забезпечення державної безпеки, реалізація функції держави.*

Аннотация. *В статье на основании анализа документов стратегического планирования государства, актов законодательства и проектов законодательных актов, исследован вопрос реализации отдельных функций государства в форме правового регулирования обеспечения кибербезопасности.*

Ключевые слова: *кибербезопасность, стратегическое планирование, оборона, обеспечение государственной безопасности, реализация функции государства.*

Summary. *This article explores the issue of implementation of state functions by the legal regulation of cybersecurity based on the analysis of the state strategic planning documents, current legislation, draft laws in the field of cybersecurity.*

Keywords: *cybersecurity, strategic planning, defense, state security, the implementation of state functions.*

Постановка проблеми. У сучасних умовах фактичної гібридної війни, яка ведеться проти України, питання забезпечення кібербезпеки у нашій державі має надзвичайно велике значення. Ужиття заходів, визначених Стратегією національної безпеки України, затвердженою Указом Президента України від 26.05.15 р. № 287/2015 та Стратегією кібербезпеки, затвердженою Указом Президента України від 15.03.16 р. № 96/2016, зумовило необхідність змін у чинному законодавстві, насамперед з метою подальшого унормування суспільних відносин, пов’язаних з реалізацією таких функцій держави, як оборона та забезпечення державної безпеки.

На розвиток цього за останній рік було ухвалено низку доктринальних документів і підзаконних нормативно-правових актів, серед яких Концепція розвитку сектору безпеки і оборони України, затверджена Указом Президента України від 14.03.16 р. № 92/2016, Стратегічний оборонний бюлетень, уведений в дію Указом Президента України від 06.06.16 р. № 240, Положення про Національний координаційний центр кібербезпеки, затверджене Указом Президента України від 07.06.16 р. № 242/2016, Порядок формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави, затверджений постановою Кабінету Міністрів України від 23.08.16 р. № 563 та низка інших.

Як показує аналіз зазначених актів, переважна більшість з них встановлює загальні засади державної політики і визначає окремі підходи до унормування питань забезпечення кібербезпеки. Водночас, деякі заходи та стратегічні підходи не повною мірою базуються на науковому підґрунті, що неодмінно призведе до неналежного правового регулювання суспільних відносин, виникнення спірних питань стосовно застосування правових норм.

Аналіз основних досліджень і публікацій. Питання правової регламентації забезпечення кібербезпеки та її організаційних основ були предметом численних наукових публікацій за останні роки як вітчизняних [1 – 9], так і іноземних [10 – 14] дослідників. Водночас, практично відсутні публікації стосовно проблемних питань правого регулювання забезпечення кібербезпеки у контексті реалізації функцій держави. Крім цього, основний масив наукових напрацювань зосереджено навколо з’ясування термінологічної бази, визначення відповідних дефініцій або дослідження особливостей кримінальної відповідальності за вчинення злочинів з використанням інформаційно-телекомунікаційних систем.

Метою статті є проведення аналізу вітчизняної нормативно-правової бази, доктринальних документів та документів стратегічного планування держави останнього часу, дослідження впливу форм реалізації окремих функцій держави на стан правового регулювання, організацію і планування відповідних організаційних заходів.

Виклад основного матеріалу. Після ухвалення 20 грудня 2002 року Генеральною асамблеєю ООН резолюції 57/239 “Елементи для створення глобальної культури кібербезпеки” зазначений термін почав активно використовуватись у вітчизняній правовій термінології. Складніше було з імплементацією змісту резолюції. Зокрема, Генеральна асамблея ООН констатувала, що стрімкий розвиток інформаційної технології означає зміну підходів державних органів, організацій та індивідуальних користувачів до питання кібербезпеки.

За цих умов було визначено дев’ять взаємопов’язаних елементів, а саме:

- *обізнаність* (тобто учасники повинні бути обізнані щодо необхідності безпеки інформаційних систем та мереж, а також про те, що саме вони можуть здійснити для підвищення безпеки);
- *відповідальність* (учасники відповідають за безпеку мереж відповідно до власної ролі);
- *реагування* (учасники мають вживати своєчасних та спільних заходів щодо попередження інцидентів, які стосуються безпеки, їх виявлення та реагування, у тому числі обмінюватись інформацією і вводити процедури, які передбачають оперативне та ефективне співробітництво з метою попередження, виявлення та реагування таки інцидентів;
- *етика* (врахування законних інтересів інших);
- *демократія* (безпека повинна забезпечуватись таким чином, щоб це відповідало демократичним цінностям, включаючи свободу обміну думками та ідеями, вільний потік інформації, конфіденційність інформації, належний захист приватної інформації; відкритість та гласність);
- *оцінка ризиків* (учасники повинні здійснювати періодичну оцінку ризиків з метою виявлення загроз та факторів уразливості, мати належні технології та інструменти контролю для цього з урахуванням значущості інформації, яка захищається);
- *проектування та впровадження засобів забезпечення безпеки*;
- *переоцінка* (належні та своєчасні заходи з внесення змін у політику і практику забезпечення безпеки з урахуванням виникнення нових та зміни існуючих загроз).

У подальшому правове регулювання вжиття заходів з кібербезпеки (окрім деяких суто кримінально-правових аспектів) в Україні в основному було зумовлено вимогами євроатлантичної інтеграції держави і випливало з доктрин, стратегій та настанов НАТО і Євросоюзу.

Зокрема, у п. 2.8 Стратегії національної безпеки, затвердженої Указом Президента України від 12.02.07 р., стан безпеки інформаційно-комп’ютерних систем в галузі державного управління фінансової і банківської сфери, енергетики транспорту, внутрішніх та міжнародних комунікацій охарактеризовано як такий, що наближається до критичного. А у подальшому в п. 4.1 зазначеної Стратегії з метою реалізації державної політики було визнано за необхідне розробку та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами Конвенції про кіберзлочинність. Слід зазначити, що запропонований у першій редакції Стратегії національної безпеки підхід, який з одного боку передбачав пріоритет державного впливу на рівні національних стандартів та технічних регламентів, а з іншого – зумовлював вжиття заходів правового регулювання відповідно до вимог міжнародно-правових актів, взятих на себе міжнародних зобов’язань та вимог гармонізації законодавства до європейських стандартів, був цілком адекватним обстановці та повністю відповідав елементам для створення глобальної культури кібербезпеки, визначеним резолюцією Генеральної асамблеї ООН.

У подальшому Указом Президента України від 08.06.12 р. № 389/2012 було затверджено нову редакцію Стратегії національної безпеки України “Україна у світі, що змінюється”. Цей документ доктринального характеру, характеризуючи безпекове середовище, серед чинників впливу на національну безпеку визначав нездатність держави протистояти викликам, пов’язаним із застосуванням інформаційних технологій в умовах глобалізації, насамперед кіберзагрозам. Чинна на той час редакція ст. 8 Закону України “Про основи національної безпеки України” серед загроз в інформаційній сфері визначала:

- прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп’ютерна злочинність та комп’ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Таким чином, зазначені новітні виклики та загрози фактично не було визначено на рівні документів стратегічного планування, оскільки комп’ютерна злочинність та комп’ютерний тероризм далеко не повністю охоплюють такі загрози.

Серед завдань забезпечення інформаційної безпеки, окрім визначених у першій редакції Стратегії, додатково було зазначено:

- стимулювання впровадження новітніх інформаційних технологій і виробництва конкурентоспроможного національного інформаційного продукту, зокрема сучасних засобів і систем захисту інформаційних ресурсів;
- забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об’єктами критичної інфраструктури;
- створення національної системи кібербезпеки.

І нарешті, у чинній редакції Стратегії національної безпеки України, затвердженій Указом Президента України від 26.05.15 р. № 287/2015, серед загроз інформаційній безпеці визначено:

- ведення інформаційної війни проти України;
- відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства.

Загрозами кібербезпеці і безпеці інформаційних ресурсів є:

- уразливість об’єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак;
- фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

Отже, у чинній Стратегії національної безпеки України характеристику загроз кібербезпеці обмежено, а фактично зведено до кібератак та застарілості системи охорони інформації з обмеженим доступом. З іншого боку визначення як окремої загрози ведення інформаційної війни проти України розширило поле, яке характеризує загрози у кіберпросторі.

Формулюючи основні напрями державної політики щодо забезпечення кібербезпеки та інформаційної безпеки, внаслідок розділення цих сфер безпеки, не вдалося уникнути певного дуалізму і у формулюванні напрямів політики. Зокрема, створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них і моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації є багато у чому пов’язаними заходами. До того ж розвиток інформаційної інфраструктури держави стосується не тільки забезпечення кібербезпеки, а й інформаційної безпеки також.

У подальшому основні напрями державної політики забезпечення саме кібербезпеки було окреслено у Стратегії кібербезпеки України, яку затверджено Указом Президента України від 15.03.16 р. № 96/2016. Метою цієї Стратегії визначено створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Як показує аналіз пріоритетів та напрямів державної політики щодо забезпечення кібербезпеки, які визначені у розділі 4 Стратегії кібербезпеки, переважна більшість з них стосуються організаційних заходів, що є взаємопов’язаними і повинні складати відповідну систему забезпечення кібербезпеки. У питанні вжиття заходів правового регулювання забезпечення кібербезпеки Стратегією визнано за доцільне необхідність приведення вітчизняного законодавства у відповідність до вимог НАТО та ЄС, комплексне вдосконалення правової основи кіберзахисту об’єктів критичної інфраструктури, подальший розвиток кримінально-правової охорони суспільних відносин у цій сфері, боротьба з кіберзлочинністю.

На виконання Стратегії кібербезпеки України розпорядженням Кабінету Міністрів України від 24.06.16 р. № 440-р було затверджено план заходів на 2016 рік з реалізації зазначеної Стратегії. У цій статті неможливо провести аналіз стану здійснення державними органами положень зазначеного плану. Скоріше за все його виконання було незадовільним. Тому рішенням Ради національної безпеки і оборони України від 29.12.16 р., уведеним в дію Указом Президента України від 13.02.17 р. № 32/2017, акцентовано увагу на необхідності термінової підготовки законодавчих пропозицій щодо кіберзахисту об’єктів критичної інформаційної інфраструктури, посилення відповідальності за невиконання вимог законодавства стосовно захисту інформації в інформаційно-телекомунікаційних системах та законних вимог посадових осіб органів Державної служби спеціального зв’язку та захисту інформації України, а також щодо запровадження відповідальності за невиконання законних вимог посадових осіб Служби безпеки України розробки низки правових новел у сфері кібербезпеки.

Слід зазначити, що більшість з перелічених питань є предметом правового регулювання у проекті Закону України “Про основні засади забезпечення кібербезпеки України”, який було прийнято Верховною Радою України за основу 20.09.16 р. Проте, зазначений проект далекий від досконалого, на що справедливо було звернуто увагу науковцями [7, с. 26-27].

На нашу думку, характеризуючи стан справ у питанні розробки правових основ забезпечення кібербезпеки, слід звернути увагу на низку системних вад, що не береться до уваги при розробці фундаментальних документів стратегічного характеру.

По-перше, досить часто змішуються організаційні заходи, які можуть бути вирішені на рівні планування та впровадження державної політики або покращання ефективності виконання державними органами їх функціональних обов’язків, з правотворчою діяльністю, що викликає паралельну розробку нормативно-правових актів, які регламентують одне й те ж коло суспільних відносин у різних аспектах.

По-друге, при розробці законодавчих пропозицій поза увагою залишаються теоретичні питання, не в останню чергу питання розуміння правотворчої форми реалізації функцій держави, що проявляються у різних сферах людської діяльності. При цьому інформаційна сфера та сфера забезпечення кібербезпеки винятками у цьому не є.

Розглянемо, яким чином функції держави реалізуються у правотворчій формі в сфері регламентації кібербезпеки. Правотворча форма здійснення функції держави полягає у розробці, ухваленні та виданні нормативно-правових актів. Перелік функцій держави є предметом наукових дискусій і дослідити їх усі на рівні наукової статті не видається за можливе. Разом із цим вважається за доцільне дослідити ті функції держави, що є найбільш актуальними у сучасних умовах. До них слід віднести функцію оборони та функцію забезпечення державної безпеки.

Слід погодитись з висловленою у літературі точкою зору, що функція оборони держави полягає у цілеспрямованій діяльності держави щодо гарантування військової безпеки, цілісності території держави та непорушності кордонів шляхом застосування засобів військового характеру [15, с. 9]. На цей час застосування засобів військового характеру чинним законодавством прямо пов’язане зі станом війни. Проте гібридний характер сучасних війн, що зумовив появу неоголошених та невизнаних війн “де-факто”, вимагає перегляду підходів і у питанні правової регламентації застосування засобів військового характеру, що відомі як “кіберзброя”, застосування до суспільних відносин права війни та правових механізмів контролю за озброєнням [16, с. 54].

Безумовним є те, що функція забезпечення державної безпеки тісно пов’язана з функцією оборони, проте, водночас, вона має і свою специфіку. По-перше, загрози, що посягають на державний суверенітет, конституційний лад та територіальну цілісність держави, далеко не завжди є загрозами військового (збройного) характеру і не завжди виходять від інших держав-противників. По-друге, гібридність сучасних війн зумовлює і значне розширення суб’єктів військових дій, а також засобів, які ними обираються [17, с. 168-170; 18, с. 90]. За таких умов засоби та напрями державної політики, а також правової регламентації відрізняються від тих, що застосовуються при реалізації функції оборони держави.

На сьогодні можна стверджувати, що існує певна система законодавства, яке регламентує коло суспільних відносин, пов’язаних із реалізацією функції забезпечення державної безпеки. До цієї системи слід віднести законодавчі акти системного характеру, що ґрунтуються на положеннях Конституції України, законодавчі акти, що

визначають правовий статус окремих суб’єктів а також ті, що регламентують певну діяльність суб’єктів. Разом з цим суспільні відносини в інших сферах діяльності (насамперед в економічній) також перебувають під впливом правової регламентації відносин із забезпечення державної безпеки.

Таким чином, регламентація питання забезпечення державної безпеки у контексті вжиття заходів із кібербезпеки, повинна бути тісно пов’язана із правовою регламентацію компетенції відповідних державних органів. На жаль, розроблені останнім часом на виконання стратегічних настанов законодавчі пропозиції так і не дають відповіді на питання щодо визначення центрального органу виконавчої влади, який відповідає за проведення державної політики у сфері кібербезпеки. Далеко не у повному обсязі розробляється питання щодо регламентації відповідних повноважень державних органів, врахування при цьому прав і свобод людини і громадянина, особливостей захисту та відновлення порушених прав, дотримання при цьому вимог міжнародно-правових актів.

Слід зазначити, що повноваження з координації діяльності не повинні підміняти собою повноваження з реалізації державної політики у цій сфері. Практика європейських держав з цього приводу зводиться, як правило, до визначення (створення) уповноваженого державного органу виконавчої влади і наділення його відповідними повноваженнями. Наприклад, з прийняттям у липні 2015 року в Німеччині Закону “Про підвищення безпеки інформаційно-телекомунікаційних систем” (відомий як IT-Sicherheitsgesetz) розширені повноваження федерального відомства інформаційної безпеки (Bundesamt für Sicherheit in der Informationstechnik, BSI), у складі якого перебуває Національний центр кіберзахисту (Nationale Cyber-Abwehrzentrum (NCAZ). При цьому BSI, як федеральний орган, що знаходиться в підпорядкуванні МВС Німеччини, чітко наділений функціями і повноваженнями необхідними для їх виконання. Зазначена практика є досить розповсюдженою в європейських країнах (наприклад, Центр суспільної безпеки (NBU) Чехії має у своєму складі Суспільний центр кібербезпеки (NCKB) і є єдиним органом, що відповідає за державну політику в сфері кібербезпеки).

На жаль, в Україні інша ситуація. Як показує аналіз положень Стратегії кібербезпеки України, суб’єктами її забезпечення є мінімум 7 державних органів різного рівня, у тому числі підпорядкованих один одному. При цьому, під терміном “розвідувальні органи” згідно чинного законодавства може розумітись від 1 до 3 органів. Над усією цією системою з метою координації створено ще один орган – Національний координаційний центр кібербезпеки, до функцій якого згідно Положення про нього, затвердженого Указом Президента України від 07.06.16 р. № 242/2016, віднесено не тільки координуючі. При цьому, Державна служба спеціального зв’язку України (в структурі якої перебуває орган з функціями ідентичними німецькому NCAZ) є центральним органом виконавчої влади зі спеціальним статусом і не наділена функціями формування державної політики у сфері кібербезпеки, оскільки це суперечить положенням частини 2 статті 1 Закону України “Про центральні органи виконавчої влади”. Таким чином, слід констатувати, що формування державної політики з забезпечення кібербезпеки на жоден державний орган не покладено. Підготовлений проект законодавчого акту (проект Закону України “Про основні засади забезпечення кібербезпеки України”, який було прийнято Верховною Радою України за основу 20.09.16 р.) також оминає врегулювання цього питання.

На нашу думку, вирішення проблеми визначення статусу, функцій та наділення повноваженнями державного органу з формування та реалізації державної політики у сфері забезпечення кібербезпеки є основою для належної реалізації функцій оборони та забезпечення державної безпеки у сфері кібербезпеки.

Висновки.

1. Документи стратегічного планування у сфері забезпечення кібербезпеки визначають наявність низки загроз та викликів, встановлюють основні напрями державної політики у цій сфері, планують проведення організаційних заходів. Водночас, у питанні розробки нормативно-правових актів відсутній системний підхід та належне теоретичне підґрунтя.

2. На нашу думку доречним є сприйняття при законотворчості теоретико-правових конструкцій щодо розуміння правотворчої форми реалізації окремих функцій сучасної держави, насамперед, враховуючи умови гібридної війни проти України, мова йде про функцію оборони і забезпечення державної безпеки.

3. Основою для реалізації зазначених функцій держави має бути визначення статусу, функцій та наділення повноваженнями державного органу з формування та реалізації державної політики у сфері забезпечення кібербезпеки.

Використана література

1. Недільніченко В.Д. Розвиток інформаційних технологій і національна безпека України // Національна безпека : український вимір. – 2009. – № 3 (22). – С. 43-57.

2. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. – К. : НІСД, 2011. – 30 с.

3. Словник термінів з кібербезпеки ; уклад. Бутузов В.М., Гавловський В.Д., Довгань О.Д. [та ін.] ; за заг. ред. Копана О.В., Скулиша Є.Д. – К. : ВБ “Аванпост-Прим”, 2012.

4. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека : сутність, визначення, відмінності // Інформація і право. – 2012. – № 2. – С. 162-169.

5. Петров В.В. Щодо формування національної системи кібербезпеки України // Стратегічні пріоритети. – 2013. – № 4 (29). – С. 127-130.

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

7. Пилипчук В.Г. Забезпечення інформаційної безпеки України : сучасні тенденції та проблеми : матеріали наук.-практ. конф. [“Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти”], (Київ, 6 жовтня 2016 р.) / НТУУ “КПІ імені Ігоря Сікорського” ; упоряд. В.М. Фурашев. – К. : Вид-во “Політехніка”, 2016. – С. 24-28.

8. Грищук Р.В. Інформаційна та кібернетична безпека : роль та місце в умовах гібридної війни : матеріали всеукр. наук.- практ. конф. [“Кібербезпека в Україні : правові та організаційні питання”], (Одеса, 21 жовтня 2016 р.). – Одеса : ОДУВС, 2016. – С. 15-16.

9. Архипов А. Приставка кибер- : все ли очевидно? // Захист інформації. – 2016. – Т. 18. – № 3. – С. 203-209.

10. Безкоровайный М.М., Татузов А.Л. Кибербезопасность – подходы к определению понятия // Вопросы кибербезопасности. – 2014. – № 1(2) – С. 22-27.

11. Dunlop Charles. Perspectives for Cyber Strategists on Law for Cyberwar / Charles J. Dunlop // Strategis Studies. – 2011. – Spring Issue. – P. 81-99.

12. Finnemore M. Constructing Norms for Clobal Cybersecurity / M Finnemore, D. Hollis // American Journal Of International Law. – 2016. – Vol. 110[425] – P. 425-479.

13. Sabillon R. National Cyber Security Strategies : Global Trends in Cyberspace / R.Sabillon, V.Cavaller, J. Cano // International Journal Of Computer Science and Software Engineering. – 2016. – Vol. 5, Issue 5 – P. 67-80.

14. О кибербезопасности критической инфраструктуры государства / [М.А. Шнепс-Шнеппе, С.П. Селезнев, Д.Е. Намиот, В.П. Куприяновский] // International Journal of Open Information Technologies. – 2016. – Vol. 4. – № 7 – P. 22-31.

15. Волинець В. Правові аспекти реалізації оборонної функції сучасної держави // Юридична Україна. – 2013. – № 5. – С. 4-10.

16. Ford Christopher. The Trouble with Cyber Arms Control / Christopher A. Ford // The New Atlantis. – 2010. – № 29. – P. 52-67.

17. Chaudhry Rajeev. Violent Non-State Actors ; Contours, Challenges and Consequences / R.Chaudhry // CLAWS Journal. – 2013. – Winter Issue. – P. 167-187.

18. Mulford Joshua. Non-State Actors in the Russo-Ukrainian War / Joshua P. Mulford // Connections : The Quarterly Journal. – 2016. – № 2. – P. 89-107.

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