УДК 351/354

Гаращенко Ю.В.
Чорноморський національний університет імені Петра Могили

ДЕРЖАВНА ПОЛІТИКА У СФЕРІ КІБЕРБЕЗПЕКИ В УКРАЇНІ

У статті проаналізовано історію становлення й основні поняття та категорії державної політики у сфері кібербезпеки України, законодавчу та нормативно-правову базу для розуміння проблем, які наявні на цьому етапі розвитку української держави. Зважаючи на загрози та з досвіду інших країн, установлено та доведено, що нагальною є необхідність подолання суперечності між зростанням важливості кібербезпекової проблематики та лише часткової готовності України відповісти на новітні кібербезпекові виклики.

Ключові слова: *державна політика, кібербезпека, інформаційний простір, соціум, електрозв'язок, радіозв'язок, гідроакустичний засіб, інформація.*

Постановка проблеми. За останні 5–7 років глобальний кіберпростір усе більше розглядається всіма державами світу як один із найважливіших безпекових пріоритетів, оскільки його функціонування стає визначальним чинником розвитку економіки, військового, соціального та інших секторів. Стає очевиднішою і подальша мілітаризація кіберпростору, а зусилля окремих держав, що намагаються попередити цей процес, є малоефективними та залишаться такими ще тривалий час.

Так, актуальність дослідження цієї теми зумовлена необхідністю подолання суперечності між наявним станом стрімкого зростання важливості кібербезпекової проблематики та лише часткової готовності української держави відповісти на новітні кібербезпекові виклики.

Аналіз останніх досліджень та публікацій. Проблемі кібербезпеки в Україні присвячено роботи багатьох дослідників, зокрема розгляд кібербезпеки та захист критичної інформаційної інфраструктури вивчають В.Л. Бурячок, В.М. Богуш; особливості кібертероризму та кібербезпеки – В.К. Харченко, О.Г. Корченко, Ю.П. Травніков, О.М. Климчик, Р.В. Кравченко, Є.С. Старостіна, Д.М. Поллард; кібертероризм як загрозу інформаційному суверенітету держави аналізують О.Д. Довгань, В.Г. Хлань; організаційно-правові засади побудови системи захисту критичної інфраструктури від кібернетичних атак визначають О.Д. Довгань, І.О. Чернухін.

Постановка завдання. Мета статті полягає в аналізі особливостей, проблем і перспектив реалізації дослідження державної політики у сфері кібербезпеки України.

Виклад основного матеріалу дослідження. За умов швидкого формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору спостерігається активізація використання інформаційно-комунікаційних технологій у всіх сферах життя, набувають загрозливих наслідків для країни проблеми інформаційної безпеки.

У результаті відсутності дієвої системи забезпечення інформаційної безпеки у національному інформаційному просторі України спостерігається велика кількість негативних явищ, які створюють реальні та приховані загрози інформаційній безпеці громадянина, суспільству та державі.

Це відбувається на тлі масованого й агресивного інформаційного наступу російської пропаганди, яка (всупереч європейським стандартам у сфері засобів масової інформації) розпалює в Україні міжнаціональну ворожнечу та сепаратистські настрої, посягає на державний суверенітет і територіальну цілісність України.

Натепер інформаційний складник стає одним із найважливіших елементів забезпечення національної безпеки. Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значно впливають на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку. Саме рівень розвитку та безпека інформаційного простору, які є системоутворювальними факторами у всіх сферах національної безпеки, активно впливають на стан економічного, політичного, оборонного та інших складників національної безпеки України [8, с. 307].

Унаслідок унікального геополітичного розташування, багатства духовної та історичної спадщини

українського народу, Україна має стати інформаційно розвиненою державою, повноправним і впливовим учасником європейського життя, посісти гідне місце у глобалізованому світі, забезпечивши при цьому захист власного інформаційного простору від небажаного інформаційного впливу; захист національних, зокрема державних інформаційних ресурсів; безпечне функціонування інформаційних та телекомунікаційних систем, зокрема тих, що функціонують в інтересах управління державою; захист інформації, що циркулює в них.

Основною метою реалізації положень принципів інформаційної безпеки України є створення в Україні розвиненого національного інформаційного простору і захист її інформаційного суверенітету. Забезпечення інформаційної безпеки України ґрунтується на таких принципах:

- законності, верховенства права та пріоритету додержання прав і свобод людини і громадянина;
- адекватності та своєчасності заходів захисту національних інтересів України від зовнішніх і внутрішніх загроз в інформаційній сфері;
- невідворотність відповідальності за вчинення злочинів та правопорушень в інформаційній сфері і забезпечення відновлення порушених прав і законних інтересів, відшкодування збитків, шкоди, завданої цими злочинами;
- безперервності і комплексності заходів у сфері забезпечення інформаційної безпеки і захисту інформації;
- пріоритетності запобіжних заходів;
- взаємодії органів державної влади та чіткого розмежування повноважень у вирішенні питань забезпечення інформаційної безпеки;
- партнерства держави та приватного сектора у виробленні нових, оптимальних рішень у сфері інформаційної безпеки та участі інституцій громадянського суспільства у забезпеченні інформаційної безпеки держави;
- дієвості, комплексності і постійності заходів із захисту інформації та інформаційних ресурсів в інформаційному просторі;
- пріоритетності національної інформаційної продукції;
- зниження рівня технічної анонімності з одночасним підвищенням захисту персональних даних [1, с. 432].

Саме тому необхідною є державна підтримка вітчизняного виробника інформаційної продукції, інформаційно-телекомунікаційного обладнання, національних операторів телекомунікацій, засобів захисту інформації, кібербезпеки та структур забезпечення інформаційної безпеки, зокрема шляхом створення нормативно-правових, фіскальних, фінансових та інших передумов для підвищення конкурентоспроможності на світовому та національному ринках інформаційних та телекомунікаційних послуг.

На сучасному етапі основними реальними та потенційними загрозами інформаційній безпеці України є:

у зовнішньополітичній сфері:

- поширення у світовому інформаційному просторі недостовірної, викривленої та упередженої інформації, що завдає шкоди національним інтересам України та створює негативний імідж України (як ненадійного партнера для міжнародних відносин); низький рівень інтегрованості України у світовий інформаційний простір;
- прояви кібертероризму та кіберзлочинності, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем, зовнішні деструктивні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет, використання інформаційного простору для втручання у внутрішні справи України [4, с. 31–37].

Напрями державної політики у сфері інформаційної безпеки України. Діяльність органів виконавчої влади у сфері забезпечення інформаційної безпеки України має бути зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства і людини за чотирма головними напрямами:

- інформаційно-психологічному – забезпечення конституційних прав і свобод людини і громадянина, створення сприятливого психологічного клімату в національному інформаційному просторі для утвердження загальнолюдських та національних моральних цінностей;
- технологічного розвитку, зокрема щодо розбудови та інноваційного оновлення національних інформаційних ресурсів, запровадження новітніх технологій;
- захисту інформації щодо забезпечення її конфіденційності, доступності та цілісності в національних інформаційних ресурсах від кібернетичних атак шляхом створення в інформаційно-телекомунікаційних системах комплексних систем захисту інформації з підкріплювальною відповідністю;
- прискорення розвитку інформаційних технологій, збільшення спроможностей держави щодо захисту від інформаційних атак із боку інших держав, а також проведення інформаційних операцій [5, с. 264].

Україна для забезпечення інформаційної безпеки має вживати низку заходів:

У зовнішньополітичній сфері:

- удосконалення інформаційного супроводу державної політики, діяльності українських громадських організацій та суб'єктів підприємницької діяльності;
- організаційно-технічне, ресурсне та інформаційне сприяння держави вітчизняним засобам масової інформації, які формують в інформаційному просторі позитивний імідж України;
- посилення просвітницької та інформаційно-просвітницької роботи щодо переваг для України від вступу в ЄС, удосконалення практичної взаємодії з НАТО, іншими міжнародними організаціями та державами-партнерами в галузі безпеки, а також щодо ефективних шляхів зміцнення національної безпеки України, зокрема з урахуванням перспективи повноправного членства в НАТО;
- інтеграція в міжнародні інформаційно-комунікаційні системи економічної доцільності та організації на засадах рівноправності, кіберзахисту та збереження інформаційного суверенітету;
- гарантування своєчасного виявлення зовнішніх загроз національному інформаційному суверенітету та нейтралізації, зокрема з використанням технологій кібербезпеки;
- допомога створенню та додержанню міжнародних правил поведінки держав в інформаційному просторі;
- підвищення рівня міжнародного співробітництва у сфері забезпечення інформаційної безпеки на загальнодержавному та відомчому рівнях;
- популяризація у світовому інформаційному просторі інформації, що створює позитивний імідж України як надійного партнера для міжнародних відносин та пропагування позитивних надбань України;
- підтримка вже наявних навчань із протидії інформаційним загрозам стосовно приватної та державної інформаційної інфраструктури та ініціювання нових видів таких навчань;
- реалізація засобів захисту від зовнішніх інформаційних впливів, зокрема шляхом підвищення якості національного культурного та інформаційного продукту;
- уживання комплексних та дієвих заходів для поширення за кордоном об'єктивної інформації про Україну, а також для протидії загрозам інформаційній безпеці, зокрема шляхом оперативного та обґрунтованого спростування у світовому інформаційному просторі дезінформації щодо України та руйнування нав'язаних світовій спільноті негативних стереотипів щодо України [6, с. 25–29].

Таким чином, інформаційна безпека є невід'ємним складником кожної зі сфер національної безпеки. Інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки, яка характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз, є сукупністю інформаційно-психологічної (психофізичної) та інформаційно-технологічної безпеки держави.

Саме через це розвиток України (як суверенної, демократичної, правової та економічно стабільної держави) можливий тільки за умов забезпечення належного рівня її інформаційної безпеки, надання всеосяжної державної підтримки національним виробникам інформаційного продукту та телекомунікаційного обладнання, створення нормативно-правових, фінансових та інших передумов, необхідних для успішної конкуренції на світовому та національному ринках інформаційних та телекомунікаційних послуг.

Щодо зовнішньої політики, то це інтеграція до інформаційного простору ЄС, а також інтеграції до структур НАТО, яка дає фізичний, матеріальний і психологічний аспект перспективним противникам України не шкодити нашому кіберпростору та інформаційному полю [7, с. 439].

Сьогодні триває процес розбудови національної системи кібербезпеки і кіберзахисту, формування її організаційно-технічної моделі, здатної забезпечити оперативне й адекватне реагування на потенційні та реальні кіберзагрози. Проте в Україні лише розпочинає формуватися розуміння масштабів та наслідків сучасних кіберзагроз, необхідності забезпечення максимально захищеного кіберпростору.

Опанування розбудови систем кібернетичної безпеки в провідних державах світу свідчить про те, що основними тенденціями у цій сфері є проведення відповідної системи реорганізації сектора безпеки та створення спеціалізованих органів із захисту національних інтересів у кіберпросторі.

Розглядаючи напрями розвитку національної системи кібербезбеки як складники системи національної безпеки України, як пріоритети, що постійно розвиваються у розробленій стратегії та місії, необхідно враховувати тенденції конкретного сегмента кіберпростору України, спираючись на ефективне використання наявних ресурсів.

Необхідно виокремлювати наявні кіберзагрози для інформаційної інфраструктури та визначати ефективні заходи протидії, створювати та вдосконалювати ефективні системи захисту критичної інфраструктури від зовнішніх і внутрішніх загроз

кібернетичного характеру, що також має на меті підвищення якості підготовки фахівців новітньої генерації галузі інформаційної та кібернетичної безпеки в процесі формування нових стандартів та партнерства. Визначаючи особливу роль вищої освіти як визначальної сили для формування фахівців із кібербезпеки та зважаючи на те, що потреба у фахівцях із кібербезпеки є актуальною (а з подальшим розвитком високотехнологічного суспільства буде ще більше зростати), розвиток якісної університетської освіти й науки потребує узгодженого вирішення конкретних практичних завдань для захисту кіберпростору [2, с. 119–148].

За умов протистояння зовнішній агресії, становлення України, прагнення щодо вступу до європейських та євроатлантичних структур, кількість та якість загроз і небезпек, спрямованих проти України, суттєво збільшуються. Тому проблематика національної безпеки стає особливо актуальною та загострює питання про «розвиток системи підготовки кадрів для потреб органів сектора безпеки й оборони України та розвиток науково-виробничого потенціалу такої системи».

Таким чином, вважаємо за доцільне таке:

1) виокремити головні вимоги до ліцензування освітніх послуг у сфері інформаційних технологій;

2) нормалізувати сталі інтеграційні зв'язки з провідними світовими ІТ-корпораціями та університетськими центрами. Для цього необхідним є:

- створення на базі консорціумів ВНЗ робочих груп із міжнародної взаємодії з провідними ІТ-корпораціями та університетськими центрами;
- розробка програм підготовки ІТ-спеціалістів міжнародного рівня;

3) удосконалити програми міжнародної співпраці в частині академічного обміну викладачами, освітніми програмами і практичними технологіями з ІТ-тематики;

4) покращити стратегії розвитку підготовки фахівців із кібербезпеки, яка дозволить університетам розвивати власне освітнє середовище для забезпечення якості підготовки майбутніх фахівців та науково-педагогічних працівників у галузі інформаційних технологій, що базується на максимальному паритетному врахуванні вимог та потреб інфраструктури регіонального сектора [9, с. 119–127];

5) стале вдосконалення та забезпечення якості освіти, що має за мету зміцнення позиції навчального закладу в галузі інформаційних технологій та кібернетичної безпеки, вдосконалення викладання та здійснення наукових досліджень у цій сфері, що дає можливість стати найважливішим засобом гарантування надійності університету стосовно споживача його послуг, зокрема бакалавра, магістра, здобувача ступеня доктора філософії та доктора наук [1, с. 432].

Наявні проблеми розвитку української системи університетської освіти і науки потребують невідкладного вирішення шляхом упровадження таких стратегій:

- системний підхід, що спирається на довгострокове співробітництво між університетами та правоохоронними органами, органами державної влади та провідними установами, що реалізується за допомогою участі здобувачів вищої освіти і викладачів у процесі обміну досвідом та знаннями, створення різних форм довгострокового партнерства в інституційній сфері освіти, упровадження інституційного та програмного типів мобільності на основі різних навчальних інструментів;
- розширення можливостей, які заохочують отримання підвищення кваліфікації викладачів певної галузі у вітчизняних ЗВО та провідних навчальних закладів Європи, які є партнерами та які реалізують спільні освітні програми, що надасть можливість здобувачам вищої освіти отримати подвійні дипломи;
- забезпечення якості освітніх послуг, що створює постійне вдосконалення різних сфер діяльності ЗВО, зокрема підвищує конкурентоспроможність випускників на внутрішньому та зовнішньому ринках праці та задоволення роботодавців результатами підготовки фахівців;
- розширює спектр освітніх послуг, що надаються, та підтримує високу якість, зміцнюючи позиції навчального закладу на ринку освітніх послуг;
- поліпшує організацію роботи та компетентність професорсько-викладацького складу і допоміжного персоналу, результативність, ефективність роботи закладу вищої освіти в цілому [3, с. 22–30].

Зважаючи на вищезазначені проблеми, можна запропонувати конкретні шляхи подальшого розвитку освіти і науки в сучасному університеті в контексті міжнародного співробітництва, а саме:

- упровадження та створення регіональної системи забезпечення кіберзахисту;
- розробка стратегічного плану кадрового забезпечення підприємств, організацій та установ області фахівцями з кібернетичної безпеки, виходячи з реального запиту ринку праці та перспектив розвитку міста й регіону;
- створення умов для сприяння розвитку університетської спільноти, зокрема викладачів, здобувачів вищої освіти, співробітників, що поєднує нові методи і принципи створення новітніх систем кіберзахисту [9, с. 119–127];

- заходи щодо комерціалізації наукової діяльності провідних учених університету в співпраці з підприємствами та організаціями в галузі інформаційної та кібернетичної безпеки;

- системне підвищення якості освіти на основі розробки та впровадження сучасного інформаційно-комунікативного та науково-методичного супроводу навчально-виховного процесу, активізацію практико-орієнтованих досліджень із залученням провідних фахівців міста й області з кібернетичної та інформаційної безпеки;

- розвиток зв'язків із правоохоронними органами, органами місцевої влади, провідними установами, вітчизняними та закордонними університетами, вивчення позитивного досвіду щодо захисту кібернетичного простору з метою його подальшого впровадження у практику професійної підготовки вищих навчальних закладів;

- продовжити роботу з оновлення змісту й підвищення якості освітніх професійних програм із галузі інформаційних технологій, відкриття нових спеціалізацій з орієнтацією на найбільш значущі напрями для регіону і країни з урахування запитів ринку праці і можливостей освітніх установ;

- здійснювати підготовку професійних кадрів із кібербезпеки із застосуванням сучасних інформаційних технологій у навчанні як важливих складників розвитку світового освітнього процесу та урізноманітнення системи моніторингу навчального процесу [10, с. 43].

Висновки. Боротьба з кібертероризмом у тій чи іншій країні належить до функціональних обов'язків підрозділів інформаційно-військових сил, яка має на меті проведення наступальних та оборонних операцій в мережі Інтернет. Проблема полягає у тому, що сучасний стан законодавства в більшості країн не відповідає низці вимог, що виникли у зв'язку з поширенням високих технологій. Часто з'ясовується, що для здійснення певних заходів подекуди немає правової основи. Натепер, за прямої участі представників кіберкомандування, завершується впровадження низки законопроектів, які у майбутньому дозволять стати таким військовим організаціям повноцінним учасником широкомасштабного об'єднаного міжнародного кіберзахисту.

Інформаційні технології швидко ввійшли у повсякденне життя суспільства, тому саме створення нового законодавства актуальне для вдосконалення регулювання і цієї сфери. Натепер одним з основних напрямів такої діяльності є боротьба з інтернет-піратством.

Тому для кібербезпеки наша країна (з метою забезпечення інформаційного захисту та супроводу) має вживати таких заходів, як:

- удосконалення діяльності українських громадських організацій та суб'єктів підприємницької діяльності за кордоном як інформаційного супроводу державної політики;

- інформаційне, організаційно-технічне та ресурсне сприяння держави вітчизняним засобам масової інформації, що формують у світовому інформаційному просторі позитивний імідж України;

- посилення просвітницької та інформаційно-просвітницької роботи щодо вступу України в ЄС, поглиблення практичної взаємодії з НАТО, іншими міжнародними організаціями та державами-партнерами в галузі безпеки, а також щодо ефективних шляхів зміцнення національної безпеки України, зокрема з урахуванням перспективи повноправного членства в НАТО;

- інтеграція в міжнародні інформаційно-комунікаційні системи та організації на засадах рівноправності, економічної доцільності, збереження інформаційного суверенітету та кіберзахисту;

- гарантування своєчасного виявлення зовнішніх загроз національному інформаційному суверенітету та нейтралізації, зокрема з використанням технологій кібербезпеки;

- сприяння створенню та додержанню міжнародних правил поведінки держав в інформаційному просторі;

- підвищення рівня міжнародного співробітництва у сфері забезпечення інформаційної безпеки на загальнодержавному та відомчому рівнях;

- розширення у світовому інформаційному просторі інформації, яка буде створювати позитивний такий імідж України, як надійного партнера для міжнародних відносин та пропагування позитивних надбань України.

Список літератури:

1. Богуш В.М. Інформаційна безпека держави. Київ: МК-Прес, 2005. С. 432.
2. Бурячок В.Л., Богуш В.М. Кібербезпека та захист критичної інформаційної інфраструктури. *Ukrainian Scientific Journal of Information Security.* 2014. № 2. С. 119–148.
3. Бачило И.Л. Методология решения правовых проблем в области информационной безопасности. *Информатика и вычислительная техника.* 1992. № 2. С. 22–30.

4. Брижко В. До питання застосування у правотворчості понять «інформація» та «дані». *Правова інформатика.* 2005. № 4. С. 31–37.

5. Брыжко В.М., Цимбалюк В.С., Орехов А.А., Гальченко О.Н. Э-будущее и информационное право; под ред. Р.А. Калюжного, М.Я. Швеца. 2002. 264 с.

6. Бортко Г.Н. Национальные стратегии информационного общества: преимущества и условия реализации в Украине. *Информационное общество.* 2004. № 2. С. 25–29.

7. Богуш В., Юдін О. Основи інформаційної безпеки держави: Вступ до спеціальності. Харків: Консум. 2004. С. 439.

8. Башмаков А.И., Башмаков И.А. Интеллектуальные информационные технологии. МГТУ имени Н. Э. Баумана, 2005. С. 307.

9. Дубов. Д. В. Стратегічні аспекти кібербезпеки України. *Стратегічні пріоритети.* 2013. № 4. С. 119–127.

10. Власенко Н.А., Зорько С.В., Сиротич М.Р. Україна на шляху до інформаційного суспільства: проблеми та здобутки. *Інформаційно-аналітичний огляд Національного інституту стратегічних досліджень.* 1995. № 5. С. 43.

ГОСУДАРСТВЕННАЯ ПОЛИТИКА В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ В УКРАИНЕ

В статье проанализирована история становления и основные понятия и категории государственной политики в сфере кибербезопасности Украины, законодательная и нормативно-правовая база для понимания проблем, имеющиеся на данном этапе развития украинского государства. Учитывая угрозы и из опыта других стран, установлено и доказано, что насущной является необходимость преодоления противоречия между ростом важности проблематики кибербезопасности и только частичной готовностью Украины ответить на новые вызовы кибербезопасности.

Ключевые слова: *государственная политика, кибербезопасность, информационное пространство, социум, электросвязь, радиосвязь, гидроакустическое средство, информация.*

STATE POLICY ON CYBERSECURITY IN UKRAINE

The article analyzes the history of the formation and the basic concepts and categories of state policy in the field of cybersecurity of Ukraine, the legislative and regulatory framework for understanding the problems existing at this stage of development of the Ukrainian state. Taking into account the threats and from the experience of other countries, it has been established and proved that the need to overcome the contradiction between the growing importance of cyber security and only partial readiness of Ukraine to respond to new cyber security challenges is urgent.

Key words: *public policy, cyber security, information space, society, telecommunications, radio communications, hydroacoustic equipment, information.*