ЧОРНОМОРСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ПЕТРА МОГИЛИ
ІНСТИТУТ ДЕРЖАВНОГО УПРАВЛІННЯ
Кафедра публічного управління та адміністрування

ГАРАЩЕНКО ЮЛІЯ ВАЛЕРІЇВНА

ДЕРЖАВНА ПОЛІТИКА У СФЕРІ КІБЕРБЕЗПЕКИ УКРАЇНИ

Спеціальність: 281 Публічне управління та адміністрування

АВТОРЕФЕРАТ

магістерської роботи на здобуття наукового ступеня
магістра публічного управління

Миколаїв – 2019

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. 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, вочевидь, малоефективні та залишаться такими ще тривалий час.

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

Джерелами для написання роботи є в перше чергу нормативно-правова база, а також спеціалізована юридична література, періодика та загальна наукова література, зокрема дослідження В. Богуша, В. Бурячка, Н. Винокурова, Д. Дубова, Г. Почепцова, В. Лисичкин. Особливості кібертероризму та кібербезпеки вивчають А.Щетілов, Г.Леваков, Г.Новіцький, Б. Кормич.

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

Для досягнення означеної мети було поставлено наступні завдання:

- розкрити історію становлення та визначити основні поняття і категорії дослідження державної політики у сфері кібербезпеки України;
- проаналізувати законодавчу та нормативно-правову базу дослідження;
- проаналізувати закордонний досвід реалізації державної політики у сфері кібербезпеки;
- проаналізувати особливості інформаційної доктрини України та розкрити основи зовнішньополітичної інформаційної політики, з огляду на

загрози;

- запропонувати рекомендації та визначити перспективи державної політики у сфері кібербезпеки України.

Об'єктом дослідження є сфера кібербезпеки України.

Предметом дослідження є особливості, проблеми та перспективи реалізації державної політики у сфері кібербезпеки України.

Методи дослідження. Для розв'язання поставлених завдань, автором застосовано комплекс загальнонаукових та спеціальних методів пізнання. Під час дослідження було використано такі методи: метод узагальнення використано для дослідження історії становлення кібербезпеки України і виявлення перспектив державної політики у сфері кібербезпеки України. Метод порівняння – використано у роботі під час дослідження закордонного досвіду реалізації державної політики у сфері кібербезпеки. Системний метод використано при аналізі перспективи оптимізації реалізації державної політики у сфері кібербезпеки України.

Крім того, в даному дослідженні були застосовані загальнонаукові методи аналізу і синтезу, індукції та дедукції.

Наукова новизна одержаних результатів обумовлена тим, що дане дослідження є спробою комплексного аналізу особливостей та перспектив реалізації державної політики у сфері кібербезпеки сучасної України та світових здобутків у цій сфері.

Практичне значення одержаних результатів Положення і висновки роботи можуть бути використані для подальшого науково-теоретичного дослідження реалізації державної політики у сфері кібербезпеки України, а також у навчальному процесі з підготовки фахівців з державного управління.

Апробація результатів дослідження. За результатами дослідження автор підготував та здав до друку наукову статтю, яка буде опублікована у фаховому виданні.

Структура магістерської роботи обумовлена зумовлена її метою та завданнями і складається зі вступу, трьох розділів, семи підрозділів,

висновків, списку використаних джерел (72 найменувань) та додатків. Повний обсяг роботи становить 103 сторінок, з яких 87 – основного тексту.

ОСНОВНИЙ ЗМІСТ МАГІСТЕРСЬКОЇ РОБОТИ

У вступі обґрунтовано актуальність теми, сформульовано мету та основні завдання, об’єкт і предмет, методи дослідження, висвітлено наукову новизну і практичне значення виконаної роботи. Наведено результати апробації основних положень та особистий внесок автора дослідження.

У першому розділі «*Теоретичні засади дослідження державної політики у сфері кібербезпеки України*» охарактеризовано проблематику та джерельну базу дослідження кібербезпеки в Україні.

Підрозділ 1.1. «Історія, основні поняття та категорії дослідження державної політики у сфері кібербезпеки України» Проаналізовано історію виникнення інформаційної безпеки, визначені основні поняття дослідження, проаналізовано стан наукової розробки проблеми у вітчизняній та зарубіжній науці.

З’ясовано, що кібернетична безпека (кібербезпека) - стан захищеності кібер простору країни в повних або окремих об'єктів його інфраструктури від ризику стороннього кібернетичного впливу, через якого гарантується їх стійке формування, а також крім того доречне виявлення, усунення та послаблення реальних і потенційних викликів, кібернетичних втручань і небезпек особистим, корпоративним та/або національним інтересам, відсутність якої може призвести до втрати політичної незалежності будь-якої держави світу, тобто до фактичного програшу нею війни невійськовими засобами та підпорядкування її національних інтересів інтересам протиборчої сторони.

Зроблено висновок, що на даний час кібербезпека України не сформувалася остаточно, оскільки з'являються нові загрози, у тому числі ті, що були спровоковані появою безпровідних методів передачі інформації.

У підрозділі 1.2. «Законодавчі та нормативно-правові засади дослідження» визначено, що правову основу забезпечення кібербезпеки

України становлять Конституція України, закони України щодо національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України. Зроблено висновок, що в Україні закладена достатньо міцна законодавча основа для формування глобального інформаційного простору.

У другому розділі «З*акордонний досвід реалізації державної політики у сфері кібербезпеки»* визначені основні напрями діяльності світового співтовариства щодо кібербезпеки.

У підрозділі 2.1. «Основи кібербезпеки у сучасному світі, глобальний інформаційний простір та боротьба з кібертероризмом» виявлено, що у середовищі, де постійно з'являються і еволюціонують кібер-загрози, країни при зустрічі з новими, глобальними загрозами отримають більшу вигоду від гнучких, оперативних стратегій кібербезпеки. Транскордонний характер загроз змушує країни вступати в тісну міжнародну взаємодію. Співпраця на глобальному рівні необхідна не тільки для ефективної підготовки до кібератаки, а й для своєчасної реакції на них. Комплексна державна стратегія кібербезпеки - перший крок на цьому шляху.

Основою боротьби з кібертероризмом в будь якій країні - є підрозділи інформаційно-військових сил, які відповідальні за проведення наступальних і оборонних операцій в глобальній Інтернет мережі. Щодо законодавчих моментів є всі підстави вважати, що деякі хитрі політичні діячі збираються покласти на кіберкомандування США далеко не військові обов'язки. На даний час, за прямої участі представників кіберкомандування, завершується впровадження низки законопроектів, які у майбутньому дозволять стати цій військовій організації повноцінним учасником американської військової машини. Зроблено висновок, що світове співтовариство доходить згоди у

тому, що мережева та інформаційна безпека стає ключовим фактором у розвитку інформаційного суспільства.

У підрозділі 2.2. «Інформаційні структури США та їх функціональність» встановлено, що однією з найрозвиненіших країн у питанні кібербезпеки на данний момент є США, кіберкомандування яких найближчим часом може стати найпотужнішою подібною структурою у світі. З урахуванням складної політичної обстановки в усьому світі, розвиток Сполученими Штатами своїх «кібервійськ» не повинен залишатися без уваги. Причому, слід не тільки мати на увазі це відомство, але й створювати свої організації з таким же призначенням.

У підрозділі 2.3 *«Інформаційний простір ЄС та боротьба з несанкціонованим контентом»* визначено, що Інформаційні технології міцно увійшли у повсякденне життя, тож створення нового законодавства актуально для вдосконалення регулювання і цієї сфери. На даний момент, одним з основних напрямів такої діяльності є боротьба з інтернет-піратством.

Зроблено висновок, що головні пріоритети політики Європи щодо кібербезпеки полягають у розробці засобів захисту інформаційно-комунікаційних технологій, розвитку правової основи інформаційної безпеки, та забезпеченні інформаційної обізнаності та безпеки громадян.

У третьому розділі *«Особливості, проблеми та перспективи оптимізації державної політики у сфері кібербезпеки України*» обґрунтовані правові основи і напрямки модернізації органів державного кіберзахисту. сформульовані конкретні пропозиції щодо оптимізації державної політики у сфері кібербезпеки України.

У підрозділі 3.1. «Інформаційна доктрина України та інституційне забезпечення кібербезпеки України» визначено, що за сучасних умов інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки, вона значною мірою впливає на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку, а тому безпосередньо стосується інформаційної

безпеки України. В Україні також була прийнята Доктрина інформаційної безпеки України є створення в Україні розвиненого національного інформаційного простору і захист її інформаційного суверенітету.

Зроблено висновок, що на сучасному етапі основними реальними та потенційними загрозами інформаційній безпеці України є:

- просування у світовому інформаційному просторі викривленої, невизначеної та упередженої інформації, що заподіяння шкоди національним інтересам України, та формує негативний імідж України, як ненадійного партнера для міжнародних відносин; низький рівень інтегрованості України у світовий інформаційний простір;
- низький рівень інтегрованості України у світовий інформаційний простір;
- прояви кіберзлочинності та кібертероризму, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем;
- зовнішні деструктивні інформаційні впливи на суспільну свідомість через засоби масової інформації, а крім того мережу Інтернет;
- застосування інформаційного простору для втручання у внутрішні справи України.

У підрозділі 3.2. «Рекомендації та перспективи державної політики у сфері кібербезпеки України» доведено, що для успішного розвитку України як суверенної, демократичної, правової та економічно стабільної держави також дуже важливо надання всебічної державної підтримки національним виробникам інформаційного продукту та телекомунікаційного обладнання, та забезпечити умови для їх успішної конкуренції на світовому та національному ринках інформаційних та телекомунікаційних послуг.

Зроблено висновок, що держава з метою забезпечення інформаційної безпеки має вживати таких заходів:

- вдосконалення інформаційного підтримки державної політики, діяльності українських громадських організацій та суб'єктів підприємницької діяльності за кордоном;
- організаційно-технічне, інформаційне та ресурсне сприяння держави вітчизняним засобам масової інформації, що формують у світовому інформаційному просторі позитивний імідж України;
- посилення інформаційно-просвітницької та просвітницької роботи щодо переваг для України від вступу 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, в тому числі з урахуванням перспективи повноправного членства в НАТО;
- об'єднання в міжнародні інформаційно-комунікаційні системи та організації на засадах рівноправності, економічної доцільності, кіберзахисту та збереження інформаційного суверенітету;
- сприяння створенню та додержанню міжнародних правил поведінки держав в інформаційному просторі; запобігання своєчасного виявлення зовнішніх загроз національному інформаційному суверенітету та їх нейтралізації, у тому числі з використанням технологій кібербезпеки;
- підвищення рівня міжнародного співробітництва у сфері забезпечення інформаційної безпеки на загальнодержавному та відомчому рівнях;
- поширення інформації у світовому інформаційному просторі, що створює позитивний імідж України, як надійного партнера для міжнародних відносин та пропагування позитивних надбань України.

ВИСНОВКИ

Відповідно до визначених у магістерської роботі мети і завдань отримані результати, які в сукупності вирішують важливе наукове завдання щодо забезпечення державної кібербезпеки в Україні. В узагальненому вигляді вони зводяться до таких теоретичних і практичних висновків:

1. На сьогодні кібербезпека ніяк не сформувалася повністю, так як з'являються нові загрози, у тому числі ті, що були спровоковані появою безпровідних методів передачі інформації. Проаналізовано історію появи інформаційної захищеності та визначено, що кібербезпека виявляє в ході власного розвитку шість етапів. Визначено, що кібернетична безпека (кібербезпека) - стан захищеності кіберпростору країни в цілому або окремих об'єктів його інфраструктури від ризику стороннього кібернетичного впливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним та/або національним інтересам, відсутність якої може відсутність якої може призвести до втрати політичної незалежності будь-якої держави світу, тобто до фактичного програшу нею війни невійськовими засобами та підпорядкування її національних інтересів інтересам нападника.

Основними критеріями, за якими у майбутньому будуть визначати стан кібербезпеки - є:

- всеохоплююче проникнення ІКТ;
- рівень безпеки в кіберпросторі;
- відповідальність за управління кіберпростором;
- джерела загроз кібербезпеці;
- цілі кібератак.

На даний час кібербезпека України не сформувалася остаточно, оскільки з'являються нові загрози, у тому числі ті, що були спровоковані появою безпровідних методів передачі інформації.

2. Правову базу забезпечення кібербезпеки України становлять Конституція України, закони України щодо національної безпеки, основ внутрішньої і зовнішньої політики, електронних комунікацій, охорони державних інформаційних ресурсів та інформації, умова щодо захисту якої встановлена законом, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов’язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

3. Сучасний стан законів більшості країн не відповідає ряду вимог, що виникли у зв'язку з широким розповсюдженням високих технологій. Для здійснення певних превентивних заходів у деяких країнах просто немає правової основи. На даний час, за прямої участі представників кіберкомандування, завершується впровадження низки законопроектів, які у майбутньому дозволять стати військовим організаціям повноцінним учасником військової об’єднаної коаліції.

4. В Україні розроблено велику правову базу для регулювання питань кібербезпеки. В основі правового забезпечення кібербезпеки України становлять Конституція України, також закони України відносно основ національної безпеки, також засад внутрішньої і зовнішньої політики, захисту державних інформаційних ресурсів та інформації, електронних комунікацій, Конвенція про кіберзлочинність, та інші міжнародні договори і внутрішні нормативно-правові акти. Згідно сучасних умов інформаційна безпека набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки, вона значною мірою впливає на темпи і рівень соціально-економічного, культурного розвитку і науково-технічного, а тому безпосередньо стосується національної безпеки України. В Україні також була прийнята Доктрина інформаційної безпеки, метою якої є створення в Україні розвиненого національного інформаційного простору і захист її інформаційного суверенітету.

Нині відбувається перетворення колишньої моделі підрозділів боротьби

з кіберзлочинністю на новітній орган правозахисного призначення, який за своїми технічними та професійними можливостями матиме змогу миттєвого реагування на кіберзагрози, а також відповідно до кращих європейських та світових стандартів проводитиме міжнародну співпрацю із знешкодження транснаціональних злочинних угруповань у цій галузі. Під час розроблення концепції з реформування підрозділів боротьби з кіберзлочинністю використано найкращий європейський та світовий досвід, а також враховані пропозиції міжнародних організацій.

Реальні та можливі небезпеки інформаційній безпеці України. На сучасному етапі головними дійсними і потенційними загрозами інформаційної захищеності України є:

- поширення у світовому інформаційному просторі викривленої, недостовірної 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 кіберзлочинності та кібертероризму, 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.

5. Держава з метою забезпечення інформаційної безпеки України має вживати таких заходів:

- вдосконалення інформаційного підтримки державної політики, діяльності українських громадських організацій та суб'єктів підприємницької діяльності за кордоном;

- організаційно-технічне, інформаційне та ресурсне сприяння держави вітчизняним засобам масової інформації, що формують у світовому інформаційному просторі позитивний імідж України;
- посилення інформаційно-просвітницької та просвітницької роботи щодо переваг для України від вступу 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, в тому числі з урахуванням перспективи повноправного членства в НАТО;
- об'єднання в міжнародні інформаційно-комунікаційні системи та організації на засадах рівноправності, економічної доцільності, кіберзахисту та збереження інформаційного суверенітету;
- сприяння створенню та додержанню міжнародних правил поведінки держав в інформаційному просторі; запобігання своєчасного виявлення зовнішніх загроз національному інформаційному суверенітету та їх нейтралізації, у тому числі з використанням технологій кібербезпеки;
- підвищення рівня міжнародного співробітництва у сфері забезпечення інформаційної безпеки на загальнодержавному та відомчому рівнях;
- поширення інформації у світовому інформаційному просторі, що створює позитивний імідж України, як надійного партнера для міжнародних відносин та пропагування позитивних надбань України.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ

1. Гаращенко Ю. В. Державна політика у сфері кібербезпеки України / Ю. В. Гаращенко // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Державне управління. − Том 30 (69). - № 1, 2019 р. (Прийнято науковою редакцією до друку, довідка).

АНОТАЦІЯ

Магістерська робота на тему «Державна політика у сфері кібербезпеки України» має науково-дослідницький характер. В ній подається характеристика теоретичних засад дослідження державної політики у сфері кібербезпеки України, включаючи нормативно-правові засади дослідження. Проаналізовано історію виникнення інформаційної безпеки та встановлено, що кібербезпека мала у процесі свого формування шість етапів. Визначено, що кібернетична безпека (кібербезпека) - стан захищеності кіберпростору держави в цілому або окремих об'єктів його інфраструктури від ризику стороннього кібернетичного впливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним та/або національним інтересам, відсутність якої тобто до фактичного програшу нею війни невійськовими засобами та підпорядкування її національних інтересів інтересам нападника. На даний час кібербезпека України не сформувалася остаточно, оскільки з'являються нові загрози, у тому числі ті, що були спровоковані появою безпровідних методів передачі інформації. Наведено закордонний досвід реалізації державної політики у сфері кібербезпеки, розглядаються особливості, проблеми та перспективи оптимізації державної політики у сфері кібербезпеки України, пропонуються рекомендації для її розвитку.

Ключові слова: Кібербезпека, державна політика, держава, безпека, кібертероризм, кіберпростір.

ANNOTATION

The subsequent militarization of cyberspace is becoming more apparent, and the efforts of individual states trying to prevent this process are obviously ineffective and will remain so long. Accordingly, the relevance of the study of this topic is due to the need to overcome the contradiction between the current state of rapid growth of the importance of cyber-security issues and the partial willingness

of the Ukrainian state to respond to the latest cyberbullying challenges. The purpose of the work is to analyze the peculiarities, problems and prospects of the study of the implementation of state policy in the field of cyber security of Ukraine. In the introduction the relevance and level of theme development are substantiated; the purpose and main tasks, object, subject and methods of research are determined; the scientific novelty is describes; the practical value of the obtained results of master’s work is established; one publication is indicated; the structure and scope of work are indicated. According to the goals and tasks defined in the master's thesis, results are obtained, which collectively solve an important scientific task of providing state cybersecurity in Ukraine. Today, cybersecurity has not come to the end, because there are new threats, including those that were provoked by the emergence of wireless methods of information transmission. The paper analyzes the history of information security emergence, identifies the main concepts of research, analyzes the state of scientific development of the problem in domestic and foreign science. It has been determined that cyber security (cybersecurity) is a state of protection of the cyberspace of the state as a whole or of individual objects of its infrastructure from the risk of extraneous cybernetic influence, which ensures their sustainable development, as well as timely detection, prevention and neutralization of real and potential challenges, cybernetic interventions and threats to personal, corporate and / or national interests, the absence of which may be lacking which could lead to the loss of political independence of any state of the world. At the current stage, the main real and potential threats to Ukraine's information security are: dissemination of distorted, inaccurate and biased information in the global information space that is detrimental to the national interests of Ukraine and creates a negative image of Ukraine as an unreliable partner for international relations; low level of integration of Ukraine into the world of information space; manifestations of cybercrime and cyberterrorism threatening the sustainable and safe functioning of national information and telecommunication systems; external destructive informational influences on public consciousness through the mass media, as well as the Internet;

use of information space for interference in internal affairs of Ukraine.

Keywords: Cyber security, state policy, state, security, cyberterrorism, cyberspace.

LIST OF PUBLISHED WORKS ON THE THEME

1.Garaschenko Yu.V. State policy in the sphere of cyber security of Ukraine / Yu.V. Garaschenko // Scientific Papers of the Taurida National University named after VI Vernadsky. Series: Public Administration. - Volume 30 (69). - No. 1, 2019 (accepted by the scientific editors to the press, the certificate).