

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

СЛІПЧУК АНГЕЛІНА СЕРГІЇВНА

ДЕРЖАВНА ПОЛІТИКА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ
БЕЗПЕКИ УКРАЇНИ

Спеціальність: 281 Публічне управління та адміністрування

АВТОРЕФЕРАТ

магістерської роботи на здобуття наукового ступеня
магістра публічного управління

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми дослідження. На сучасному етапі, при стрімкому зростанні різноманітних інформаційних загроз постає питання недостатнього рівня дослідження проблем забезпечення інформаційної безпеки України.

Додатково актуальність проблеми забезпечення інформаційної безпеки України підкріплюється відсутністю дієвої системи забезпечення інформаційної безпеки, яка знаходиться на стадії розвитку. Складові цієї системи не завжди пов'язані між собою, а їх функції часто повторюються, що заважає їх ефективній діяльності. Для запобігання інформаційних загроз потрібні комплексні узгоджені дії всіх суб'єктів цієї системи.

За умов глобальних інформаційних загроз складність управління сферою інформаційної безпеки зумовлюється багатоманітністю вираження інформації та інформаційних процесів. Гібридна війна, частиною якої є інформаційні чинники, утворює довготривалі виклики для України. Перед державою постає необхідність в реформуванні системи національної безпеки і оборони, основним пріоритетом якої є інформаційна безпека.

При здійсненні державно-управлінських реформ в першу чергу необхідно вирішити проблему невідповідності існуючих зараз організаційно-правових механізмів в сфері забезпечення інформаційної безпеки тим загрозам, які постають перед Україною в процесі протистояння зовнішній агресії. Органи влади, на які покладено функції стосовно забезпечення інформаційної безпеки показали свою неефективність. В дійсності, попри наявність органів сектору безпеки та велику кількість документів, які так чи інакше регулюють інформаційну сферу, більша їх частина недієва при умовах реальних загроз інформаційній безпеці.

Постала потреба в науковому аналізі організаційно-правових норм формування та реалізації державної політики забезпечення інформаційної безпеки України, використання досвіду інших країн стосовно реагування на загрози інформаційній сфері, розробка пропозицій щодо вдосконалення цього процесу за умов інформаційної війни.

Під час написання магістерської роботи використовувались праці вітчизняних науковців з різних аспектів державного управління інформаційною безпекою. Дослідженню формування та забезпечення державної політики інформаційної безпеки присвячуються праці Степанова В. Ю., Розпутенка І. В., Данільян О. Г., Панова М. І., Богдановича В. Ю. та інших. Проблеми правового забезпечення регулювання інформаційних відносин, процесу інформатизації та захисту інформації розглядають в своїх працях Семенченко А. І., Ситник Г. П., Кулішко І. Б., Новицький Г. В., Євдоченко Л. О. та інші. Зв'язок між системами інформаційної та національної безпеки пояснюють російські вчені Левін А. А., Анохин П. К., Шагієв Р.В та інші. До джерельної бази дослідження також можна віднести офіційні документи й правові акти. Для даної роботи особливо корисним став Закон України «Про основи національної безпеки України».

Дослідження вище названих науковців забезпечили методологічну основу для вивчення питань в сфері державного забезпечення інформаційної безпеки. Після сукупного аналізу цього питання варто зауважити, що досліджуване питання є досить маловивченим. Залишаються невирішені проблеми формування та реалізації державної політики забезпечення інформаційної безпеки, які потребують подальшого вивчення.

Мета і завдання. Метою магістерської роботи є обґрунтування теоретичних положень та методологічних підходів, розробка практичних рекомендацій стосовно

вдосконалення процесу державного управління забезпеченням інформаційної безпеки України.

Для досягнення мети автор сформулював такі завдання:

- дослідити основні теоретико-методологічні підходи стосовно державної політики забезпечення інформаційної безпеки та визначити особливості її реалізації в умовах інформаційної війни;

- визначити основні проблеми державного забезпечення інформаційної безпеки;

- проаналізувати та узагальнити зарубіжний досвід державного забезпечення інформаційної безпеки та оцінити можливість його впровадження в систему державного управління України;

- розробити рекомендації щодо вдосконалення процесу державного управління забезпеченням інформаційної безпеки України.

Об'єктом дослідження є державна політика забезпечення інформаційної безпеки України.

Предмет дослідження – шляхи удосконалення процесу державного управління забезпеченням інформаційної безпеки України.

Методи дослідження. Дана робота ґрунтується на використанні комплексу загальнонаукових та спеціальних методів пізнання. Системний аналіз надав можливість комплексного дослідження проблем державного забезпечення інформаційної безпеки. Методи порівняння, індукції та аналогії дозволили визначити предмет, окремих елементів процесу формування та реалізації державної політики забезпечення інформаційної безпеки. Методологія структурно-функціонального методу дозволила охарактеризувати структуру та функції системи державного забезпечення інформаційної безпеки. Компаративний метод, метод спостереження та теоретичне узагальнення були використані при вивченні зарубіжного досвіду реагування на загрози інформаційній безпеці, його порівняння з вітчизняним та формування висновків та порад щодо вдосконалення.

Наукова новизна одержаних результатів магістерської роботи полягає в вирішенні актуального питання, яке полягає в науково-теоретичному обґрунтуванні напрямків вдосконалення державної політики забезпечення інформаційної безпеки України.

вперше:

- охарактеризовано шляхи удосконалення процесу державного управління забезпеченням інформаційної безпеки України;

удосконалено:

- організаційно-правові механізми формування та реалізації державної політики забезпечення інформаційної безпеки;

набули подальшого розвитку:

- тенденції, пов'язані з реформуванням системи національної безпеки і оборони, основним пріоритетом якої є інформаційна безпека.

Практичне значення полягає в тому, що дана робота може використовуватись як основа для подальших досліджень державного забезпечення інформаційної безпеки. Матеріали даної роботи мають певну цінність для вирішення наукових та практичних завдань з метою підвищення рівня державного забезпечення інформаційної безпеки України.

Апробації. Основні наукові результати роботи представлені під час Науково-практичної конференції «Лісабонський договір – 10 років після набуття чинності. Що змінилося у функціонуванні ЄС?».

Структура роботи. Загальний обсяг роботи – 87 сторінок, з яких 75 сторінок становить основний текст. Робота складається зі вступу, трьох розділів, восьми підрозділів, висновків, списку використаних джерел та додатків.

ОСНОВНИЙ ЗМІСТ МАГІСТЕРСЬКОЇ РОБОТИ

У вступі обґрунтовано актуальність теми магістерської роботи, визначено її мету, завдання, об'єкт, предмет, методи дослідження, розкрито наукову новизну одержаних результатів та їх практичне значення.

У першому розділі *«Теоретико-методологічні засади державної політики забезпечення інформаційної безпеки»* досліджено основні науково-методологічні підходи до державної політики забезпечення інформаційної безпеки, розкрито зміст політики інформаційної безпеки в контексті забезпечення національної безпеки, охарактеризовано особливості реалізації державної політики інформаційної безпеки України в сучасних умовах.

У підрозділі 1.1. «Теоретико-методологічні підходи щодо вивчення політики забезпечення інформаційної безпеки» охарактеризовано поняття «інформаційної безпеки» та «забезпечення інформаційної безпеки», розглянуто систему забезпечення інформаційної безпеки з точки зору структурно-функціонального, синергетичного та системного підходів.

У підрозділі 1.2. «Сутність державної політики забезпечення інформаційної безпеки» розглянуто різні підходи до поняття «державна політика» та завдяки узагальненню цих підходів дано цілісне визначення даного поняття. Визначено суб'єкти державної політики інформаційної безпеки.

Встановлено, що державне управління забезпечення інформаційної безпеки - одна з найважливіших функцій держави, його зміст в забезпеченні узгодженої національної стратегії на всіх рівнях державного управління. Для ефективного функціонування системи забезпечення інформаційної безпеки необхідне централізоване управління з відомчо-розпорядчими функціями, що забезпечуватимуть системний моніторинг та регулювання всіх складових національного інформаційного простору.

У підрозділі 1.3. «Реалізація державної політики забезпечення інформаційної безпеки України в сучасних умовах» досліджено специфіку реалізації сучасної державної політики забезпечення інформаційної безпеки.

Зроблено висновок, що до особливих умов реалізації державної політики забезпечення інформаційної безпеки відноситься: формування глобального інформаційного суспільства; політична, соціальна, інформаційна глобалізація; геополітична конкуренція в інформаційному просторі; інформаційно-психологічна війна як частина збройного конфлікту на Сході України.

У другому розділі *«Сучасний стан та перспективи розвитку державної політики забезпечення інформаційної безпеки України»* досліджено організаційно-правові механізми розробки державної політики у сфері інформаційної безпеки; проаналізовано керівні документи державної політики забезпечення інформаційної безпеки як механізм її формування; розглянуто зарубіжний досвід реалізації механізмів державного реагування та протидії сучасним викликам та загрозам інформаційній безпеці.

У підрозділі 2.1. «Організаційно-правові механізми формування та реалізації державної політики забезпечення інформаційної безпеки» встановлено, що організаційно-правові механізми державної політики забезпечення інформаційної безпеки складаються з

трьохкомпонентної системи, у котрій законодавчі органи визначають параметри безпеки інформаційної сфери, Президент вирішує питання стосовно визначення інструментів досягнення та забезпечення цих параметрів, а Кабінет міністрів виконує завдання щодо застосування обраного інструменту впливу на суспільні взаємовідносини та реалізації передбачених заходів.

У підрозділі 2.2. *«Керівні документи державної політики забезпечення інформаційної безпеки як механізм її формування та реалізації»* встановлено, що система забезпечення національної безпеки може бути ефективною, маючи надійну нормативно-правову базу, котра буде спрямовувати розвиток цієї системи. Цю базу складають керівні документи державної політики, які створюють фундамент стратегічного планування: закон, доктрина, концепція, стратегія, проекти і плани, які регулюють відносини в сфері національної безпеки. Одним з головних завдань, покладених на систему забезпечення національної безпеки, необхідно виділити розробку керівних документів щодо забезпечення інформаційної безпеки.

У підрозділі 2.3. *«Механізми реагування і протидії викликам та загрозам інформаційній безпеці: зарубіжний досвід»* було проаналізовано зарубіжний досвід реагування на загрози інформаційній безпеці та зроблено висновок що лідером в цій сфері є США. Вони не тільки ефективно реагують на існуючі загрози, а й прогнозують потенційне виникнення нових. Тому цей досвід можна використовувати в процесі реформування державного управління в інформаційній сфері України.

У третьому розділі *«Шляхи вдосконалення державного управління забезпеченням інформаційної безпеки України»* надано пропозиції стосовно вдосконалення державного управління забезпеченням інформаційної безпеки України.

У підрозділі 3.1. *«Теоретичні аспекти вдосконалення державного управління забезпеченням інформаційної безпеки України»* встановлено, що на сучасному етапі, для вдосконалення державного управління забезпеченням інформаційної безпеки необхідно: а) визначити перспективну модель системи забезпечення інформаційної безпеки в умовах ведення інформаційної війни. Варто зауважити, що вимоги до перспективної моделі системи забезпечення інформаційної безпеки передбачаються: суттєвим трансформуванням інформаційного та управлінського простору держави; сучасними тенденціями інформаційного протиборства; змінами в безпековому середовищі держави; б) розробити та впровадити в державно-управлінську практику рефлексивну модель організації системи державного управління забезпеченням інформаційної безпеки в умовах інформаційних протиборств, що надасть можливість системного впливу на інформаційну безпеку та забезпечить нестандартність поведінки суб'єктів інформаційної безпеки для попередження негативних інформаційних впливів; в) систематизувати законодавчі акти за трьома рівнями: доктринально-стратегічним, тактичним та функціонально-спеціальним; г) розгорнути широку та багатопрофільну підготовку фахівців з інформаційної боротьби.

У підрозділі 3.2. *«Рекомендації стосовно розробки та впровадження рефлексивної моделі організації системи державного управління забезпеченням інформаційної безпеки України»* запропоновано рефлексивну модель організації системи державного управління забезпеченням інформаційної безпеки, яка надає можливість вдосконалити нормативно-правову базу в сфері інформаційної безпеки та оптимізувати механізми забезпечення

інформаційної безпеки України, враховуючи сучасні загрози національним інтересам України в інформаційній сфері.

ВИСНОВКИ

В магістерській роботі представлено теоретичне узагальнення та запропоновано вирішення актуального наукового завдання, яке полягає у комплексному дослідженні та обґрунтуванні теоретичних та практичних засад організаційно-правових механізмів формування та реалізації державної політики забезпечення інформаційної безпеки України.

Отримані в процесі проведеного дослідження результати дають можливість зробити наступні висновки.

1. Узагальнено теоретико-методологічні підходи стосовно державної політики забезпечення інформаційної безпеки, яка може досліджуватись у рамках структурно-функціонального, синергетичного, системного та інших підходів.

З точки зору системного підходу доведено, що система забезпечення інформаційної безпеки є відкритою системою зі специфічними структурними елементами, котра має власні внутрішні взаємозв'язки та зв'язки з навколишнім середовищем, функціонує і розвивається під впливом різноманітних факторів, серед яких природні та соціальні.

Розкрито специфіку реалізації сучасної державної політики інформаційної безпеки, котра полягає у врахуванні, з одного боку, появи нових глобальних інформаційних викликів і загроз сучасного світу, геополітичної конкуренції в інформаційному просторі, відсутності міжнародного законодавства, що регулює зростання загроз міжнародній інформаційній безпеці, а з другого – національного виміру сучасних загроз, змістом яких є ведення проти України інформаційної війни РФ. Все це створює особливі умови реалізації державної політики інформаційної безпеки саме тому, що системою державного управління ще не вироблена ефективна система протидії вказаним викликам та загрозам.

2. Виявлено основні проблеми державного управління забезпеченням інформаційної безпеки України, до яких належать наступні: забезпечення життєво важливих потреб об'єктів інформаційної безпеки України за умов інформаційного протиборства, що зумовлені браком систематизованих знань про сучасні методи та форми інформаційного протиборства, аналітичної інформації та ресурсів, необхідних для ефективного реагування на загрози інформаційній безпеці; швидка адаптація нормативно-правової бази у сфері інформаційної безпеки з врахуванням появи нових викликів, загроз, небезпек інформаційного характеру, а також наявних розривів в організації діяльності суб'єктів забезпечення інформаційної безпеки України; оптимізація структури функцій системи забезпечення інформаційної безпеки; вдосконалення механізмів забезпечення інформаційної безпеки. На сьогоднішній день система державного управління забезпеченням інформаційної безпеки України залишається остаточно не сформованою.

Досліджено організаційно-правові механізми формування та реалізації державної політики забезпечення інформаційної безпеки у цілому.

Зроблено висновок, що суб'єкти формування державної політики інформаційної безпеки є частиною нормативно-правових механізмів забезпечення державної політики інформаційної безпеки, котрі виконують законодавчі функції стосовно вказаної сфери, а суб'єкти реалізації державної політики інформаційної безпеки являються частиною

організаційних механізмів забезпечення інформаційної безпеки, які здійснюють виконавчі функції. Нормативно-правові та організаційні механізми державної політики забезпечення інформаційної безпеки знаходяться на стадії розвитку.

Встановлено, що в цілому організаційно-правовий механізм державної політики інформаційної безпеки є впорядкованим комплексом інститутів держави, задіяних в процесі формування та реалізації політики інформаційної безпеки, внутрішні і зовнішні ролі й відносини якої регулюються системою правових норм та принципів. Цей організаційно-правовий механізм відповідно до зазначених напрямків реалізації політики інформаційної безпеки складається з трьох пов'язаних елементів.

По-перше, це сукупність державних інституцій (інститутів публічної влади та інститутів громадянського суспільства), задіяних в процесі формування і впровадження політики інформаційної безпеки.

По-друге, це сукупність ролей і відносин, яка включає правові відносини, що виникають у процесі реалізації політики інформаційної безпеки, та особливі ролі, форми і методи діяльності суб'єктів проведення політики інформаційної безпеки.

По-третє, це ієрархічна сукупність правових норм та принципів, що регулюють зміст і процес проведення політики інформаційної безпеки, тобто правовий механізм інформаційної безпеки, який становлять останні два елементи.

Зазначено, що ефективність захисту інформаційної безпеки держави залежить від ефективності кожної складової її механізму.

3. Проведено аналіз зарубіжного досвіду функціонування механізмів державного реагування на сучасні виклики та загрози інформаційній безпеці та можливості його застосування в державно-управлінській практиці України. Було з'ясовано, що європейський досвід має цінність для України, але не слід забувати про те, що за час ведення гібридної війни РФ проти України, були вироблені механізми протидії протидії інформаційній агресії в формі діяльності недержавних суб'єктів забезпечення інформаційної безпеки. Цей досвід може бути цінним для зарубіжних експертів в цій сфері.

Підсумовуючи вивчення зарубіжного досвіду реагування на загрози інформаційній безпеці можна сказати, що перші спроби розробки правових актів або хоча б характеристики інформаційних загроз, які постали перед суспільством в результаті розв'язаної Росією інформаційної війни спочатку проти України, а згодом в країнах ЄС та США, були зроблені в Україні. В Коаліційній угоді Верховної Ради України VIII скликання пріоритетним завданням зазначалось «створення взаємоузгодженої державної системи інформаційної безпеки та розроблення і прийняття Концепції інформаційної безпеки».

На сучасному етапі розбудови системи інформаційної безпеки ключове значення має зміцнення нормативно-правової бази функціонування інформаційної сфери та питань щодо забезпечення інформаційної безпеки. Динаміка відносин в інформаційній сфері випереджує розвиток правосвідомості суспільства. Недосконалість нормативно-правової бази дозволяє окремим зовнішнім та внутрішнім суб'єктам чинити протиправні дії щодо порушення цілісності державної системи забезпечення інформаційної безпеки.

4. Розроблено рекомендації стосовно вдосконалення процесу державного управління забезпеченням інформаційної безпеки за умов інформаційного протиборства, зокрема на сучасному етапі потрібно:

- надати інформаційній безпеці статус пріоритетного напрямку діяльності органів державної влади;
- впровадити в державно-управлінську практику рефлексивну модель організації системи державного управління забезпеченням інформаційної безпеки за умов інформаційного протиборства, що надасть можливість системно впливати на інформаційну безпеку України та забезпечити нестандартність поведінки суб'єктів інформаційної безпеки для запобігання зовнішнім негативним інформаційним впливам;
- створити комплекс системи підготовки фахівців з інформаційних операцій, що буде ґрунтуватись на європейських практиках та враховувати вітчизняний досвід, набутий під час проведення спеціальних операцій.

АНОТАЦІЯ

Сліпчук А. С. Державна політика забезпечення інформаційної безпеки України – На правах рукопису.

Магістерська робота на здобуття освітнього ступеню «магістр». Чорноморський національний університет імені Петра Могили. – Миколаїв, 2019.

В даній магістерській роботі розглянуто теоретико-методологічні засади дослідження державної політики інформаційної безпеки України.

Проаналізовано сучасні концепції та підходи до розуміння процесу становлення організаційно-правових механізмів формування та реалізації державної політики інформаційної безпеки України, роль та місце державної політики інформаційної безпеки у системі національної безпеки, а також можливе використання наукових здобутків у вигляді як загальних теорій національної безпеки, так і конкретних її елементів, кожен з яких пояснює окрему проблему і пропонує способи її вирішення.

Досліджено організаційно-правові механізми розробки державної політики забезпечення інформаційної безпеки, розробку керівних документів державної політики інформаційної безпеки як один з механізмів її формування, проаналізовано зарубіжний досвід стосовно механізмів державного реагування на сучасні виклики та загрози інформаційній безпеці.

Обґрунтовано пропозиції стосовно вдосконалення державного управління забезпеченням інформаційної безпеки України в сучасних умовах.

Ключові слова: державне управління, інформаційна безпека, система інформаційної безпеки, система забезпечення інформаційної безпеки, державне управління забезпеченням інформаційної безпеки.

SUMMARY

Slipchuk A. S. State policy of information security of Ukraine - Manuscript.

Graduate work for obtaining an educational degree «Master». Petro Mohyla Black Sea National University. – Mykolaiv, 2019.

This master's thesis deals with the theoretical and methodological principles of the analysis of public policy of information security. The nature of the state policy of information security of Ukraine is analyzed in the context of modern challenges and threats.

An analysis of current theories, concepts and approaches to understanding the genesis of organizational and legal mechanisms of formation and implementation of the state information security policy of Ukraine carried out to understand the role and place of the state of information security policy in the strategic national security system, and to possible use of accumulated scientific achievements, in the form of general national security theories and its specific

components, each of which explains the separate issues and offers its own means to decide them.

The institutional, organizational and legal mechanisms of the development of state policy in the field of information security are searched; the process of developing guidelines of the state information security policy is analyzed as one of mechanisms of its planning; foreign experience concerning the mechanisms of the state respond to modern challenges and threats to information security.

Theoretical and practical recommendations with respect to improvement of public administration of Ukraine in the sphere of information security.

Key words: public administration, information security, information security system, state security information security system.