ІНСТИТУТ ПІДГОТОВКИ КАДРІВ
ДЕРЖАВНОЇ СЛУЖБИ ЗАЙНЯТОСТІ УКРАЇНИ

ТУРЧАК АННА ВАСИЛІВНА

УДК 351:004.056.5

МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК СКЛАДОВОЇ ДЕРЖАВНОЇ БЕЗПЕКИ УКРАЇНИ

25.00.02 – механізми державного управління

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня
кандидата наук з державного управління

КИЇВ – 2020

Дисертацією є рукопис.

Робота виконана в Інституті підготовки кадрів державної служби зайнятості України.

Науковий консультант – доктор наук з державного управління, доцент **ВОРОНА Петро Васильович**, Інститут підготовки кадрів державної служби зайнятості України, перший проректор.

Офіційні опоненти: доктор наук з державного управління, професор, заслужений діяч науки і техніки України, **СЕМЕНЧЕНКО Андрій Іванович**, Національна академія державного управління при Президентові України, директор Інституту вищих керівних кадрів соціальної і гуманітарної політики, м. Київ;

кандидат наук з державного управління **ОЛЕКСЮК Лілія Віталіївна**, Всеукраїнська асоціація «Інформаційна безпека та інформаційні технології», Голова громадської організації.

Захист відбудеться *29 квітня 2020 року о 12-й годині* на засіданні спеціалізованої вченої ради Д 26.891.02 Інституту підготовки кадрів державної служби зайнятості України за адресою: 03038, м. Київ, вул. Нововокзальна, 17, ауд. 201.

Із дисертацією можна ознайомитись у бібліотеці Інституту підготовки кадрів державної служби зайнятості України за адресою: 03038, м. Київ, вул. Нововокзальна, 17.

Автореферат розісланий *26 березня 2020 року.*

Вчений секретар
спеціалізованої вченої ради М. З. Масик

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Сучасні умови суспільного розвитку характеризуються процесами глобалізації, що обумовило посилення боротьби між різними суб'єктами міжнародних відносин за панівний вплив на окремі соціальні групи та цілі народи. Інформаційна війна у цьому контексті стала важливим інструментом сучасних відносин між державами. На сьогодні Україна здійснює низку складних демократичних та соціально-економічних трансформацій, перебуваючи в зоні ризику забезпечення своєї інформаційної безпеки. Це пов'язано з тим, що тривалий час окресленій сфері не приділялась належна увага. Відповідно загострювалися протиріччя та конфліктні ситуації як внутрішнього, так і зовнішнього характеру. При цьому основним засобом здійснення негативного впливу на нашу країну були й залишаються інформаційно-комунікаційні технології. З метою ефективного забезпечення її інформаційної безпеки та кібербезпеки розробляється відповідна державна політика та здійснюється державне управління розвитком даного напряму.

Бурхливість розвитку інформаційних та інформаційно-комунікаційних технологій супроводжується підвищенням рівня традиційних і появою загроз принципово нового характеру для громадян, суспільства та держави, що актуалізує тематику дослідження.

Вивченню даного питання приділяли увагу багато науковців та дослідників. Зокрема, теоретичні аспекти забезпечення інформаційної безпеки розглядали такі науковці, як: В. Абакумов, В. Антонюк, В. Богуш, О. Юдін, І. Боднар, В. Брижко, М. Волошина, С. Гуцу, О. Дзьобань, К. Захарченко, Р. Калюжний, О. Литвиненко, В. Ліпкан, Л. Наливайко, В. Петрик, О. Рижук та ін. Зарубіжний досвід був проаналізований такими науковцями, як: О. Горелихина, Т. Михайлюк, О. Рябоконь, І. Чернухін, С. Шустенко, Є. Макаренко та ін. Ряд науковців зробили спробу виділити проблеми забезпечення інформаційної безпеки та запропонувати шляхи їх вирішення, зокрема: О. Горбатюк, У. Ільницька, В. Антонюк, Т. Ткачук, І. Беззуб, В. Горбулін, М. Еделєва та ін. Дисертаційні роботи виконали такі науковці, як: В.Гурковський, О. Довгань, В. Козубський, Є. Макаренко, О. Олійник, О. Петкова та ін.

Незважаючи на це розвиток механізмів забезпечення інформаційної безпеки потребує подальшої розробки та наукового обґрунтування шляхів їх модернізації, що зумовило вибір теми, мету та завдання наукового дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Дана дисертаційна робота виконувалася згідно з науково-дослідними роботами Інституту підготовки кадрів державної служби зайнятості України «Управління інноваційно-інвестиційним розвитком регіону в умовах децентралізації та регіональної демократії» (державний реєстраційний номер 0118U005266) та «Дослідження проблематики розвитку прямих форм

демократії в Україні в умовах децентралізації» (державний реєстраційний номер 0118U003560). Наукові напрацювання, отримані у результаті здійсненого дисертаційного дослідження на тему «Механізми забезпечення інформаційної безпеки як складової державної безпеки України», знайшли впровадження в програмах навчальних дисциплін професійної та практичної підготовки магістрів спеціальності 281 «Публічне управління та адміністрування» у модулі «Публічна комунікація та професійна іноземна мова в публічному управлінні».

Мета та завдання дослідження. *Метою* дисертаційної роботи є теоретико-методологічне обґрунтування формування та розвитку механізмів забезпечення інформаційної безпеки як складової державної безпеки України та розробка практичних рекомендацій органам влади щодо їх упровадження.

Для досягнення поставленої мети було визначено такі *завдання*:

– дослідити теоретичні засади державної політики інформаційної безпеки, удосконалити категорійно-понятійний апарат та запропонувати класифікацію механізмів забезпечення інформаційної безпеки;

– узагальнити зарубіжний досвід механізмів забезпечення реалізації державної політики інформаційної безпеки та сформувати на його основі пропозиції щодо вдосконалення національних механізмів;

– обґрунтувати теоретико-методологічний підхід щодо взаємодії державної політики інформаційної безпеки та державної політики у сфері кібербезпеки;

– проаналізувати наявні загрози національним інтересам в інформаційній сфері;

– проаналізувати можливості запровадження в Україні кращих міжнародних та національних практик формування та реалізації державної політики інформаційної безпеки;

– запропонувати перспективні напрями застосування механізмів реалізації державної політики інформаційної безпеки в Україні;

– окреслити коло відповідальних органів влади та шляхи удосконалення системи інформаційної безпеки України.

Об’єкт дослідження – суспільні відносини у сфері забезпечення інформаційної безпеки.

Предмет дослідження – розвиток механізмів забезпечення інформаційної безпеки як складової державної безпеки України.

Методи дослідження. Для виконання поставлених завдань дослідження використано загальнонаукові та спеціальні методи: аналізу та синтезу – для деталізації об’єкта дослідження; узагальнення – для розкриття теоретико-методологічних засад механізмів забезпечення інформаційної безпеки; порівняльний метод та систематизації – для вивчення нормативно-правового забезпечення інформаційної безпеки; системний метод – для розкриття концептуальних основ забезпечення інформаційної безпеки; логічний, діалектичний, метод узагальнення, комплексного і системного підходів – для вдосконалення понятійного апарату дослідження; порівняння

та узагальнення – при дослідженні особливостей забезпечення інформаційної безпеки; метод моделювання – для розроблення перспективних напрямів застосування механізмів реалізації державної політики інформаційної безпеки та можливих шляхів удосконалення системи інформаційної безпеки України; абстрактно-логічний метод – для теоретичного узагальнення й формулювання висновків та пропозицій. Методологічною базою дослідження є наукові праці вітчизняних і зарубіжних учених, зокрема офіційні публікації міжнародних організацій.

Інформаційна та емпірична база дослідження сформована нормативними документами органів державної та регіональної влади, статистичними й соціологічними даними, матеріалами, опублікованими в періодичних виданнях та мережі Інтернет.

Наукова новизна одержаних результатів полягає в теоретико-методологічному обґрунтуванні формування та розвитку механізмів забезпечення інформаційної безпеки як складової державної безпеки України та розробці практичних рекомендації органам влади щодо їх упровадження та вдосконалення. Найбільш значущі результати, що містять наукову новизну, конкретизовано в таких наукових положеннях:

уперше:

– запропоновано авторське визначення інформаційної безпеки - не тільки як стану захищеності інформаційного середовища й ресурсів, задоволення інформаційних потреб громадян, суспільства та держави, але й захищеності прав суб’єктів інформаційних правових відносин від негативних зовнішніх та внутрішніх факторів, що становлять загрозу конфіденційності, цілісності й доступності інформації, застосування якого сприятиме підвищенню рівня обґрунтованості державної політики інформаційної безпеки;

удосконалено:

– теоретико-методологічний підхід до розуміння сутності взаємодії державної політики інформаційної безпеки та державної політики у сфері кібербезпеки, який на відміну від наявного, формально визначеного в національному законодавстві, передбачає розгляд державної політики у сфері кібербезпеки як невід’ємної специфічної складової державної політики інформаційної безпеки, яка повинна включати низку напрямів - кіберзахист, кібероборону, кіберрозвідку, протидію кібершахрайству, кібертероризму, кібершпигунству, що сприятиме систематизації та упорядкуванню заходів із забезпечення державної політики інформаційної безпеки;

– пріоритетні напрями вдосконалення механізмів забезпечення інформаційної безпеки, а саме:

а) *правовий механізм,* у якому необхідно:

акцентувати увагу на забезпеченні консенсусу (згоди) в суспільних взаєминах, узгодженості поглядів та правомірній поведінці суб’єктів відносин інформаційного характеру, стосунків в інформаційному секторі; забезпеченні інформаційного суверенітету, незалежності України на

міжнародній арені; забезпеченні інформаційної безпеки людей, їх об'єднань, соціуму та країни в цілому; визнанні правомірної поведінки для кожного учасника інформаційного співробітництва в нашій країні;

захистити інформацію від несанкціонованих проникнень, злочинних дій (знищення, модифікація, спотворення, порушення приватності, конфіденційності тощо); гармонізувати національне законодавство з міжнародним, урахувавши особливості розвитку України; розробити інформаційний Кодекс з уточненням його першочергових завдань; внести зміни до Закону України «Про національну безпеку України» та Закону України «Про основні засади забезпечення кібербезпеки України» з метою розробки стратегії інформаційної безпеки замість Доктрини інформаційної безпеки України після затвердження Стратегії національної безпеки України, проведення з цією метою аналізу стану інформаційної безпеки, уточнення завдань та функцій складових системи забезпечення інформаційної безпеки;

б) *інституційний механізм,* включаючи:

створення ефективної багаторівневої державної системи підтримки інформаційного захисту із задіянням єдиних правових норм і механізмів, покликаних захистити інформаційні ресурси, інформаційно-телекомунікаційну інфраструктуру, об'єкти критичної інфраструктури й інформаційні права людей, ефективно координувати діяльність владних структур; розробку механізму взаємодії державних і місцевих органів влади у сфері підтримки інформаційної безпеки;

модернізацію, на відміну від наявного механізму інституційного забезпечення, Національного координаційного центру кібербезпеки України в Національний координаційний центр з питань інформаційної безпеки, з визначенням відповідальним за формування та реалізацію державної політики інформаційної безпеки Міністерства цифрових трансформацій, підпорядкувавши йому Державний комітет телебачення та радіомовлення, що дозволить комплексно вирішувати проблеми у сфері інформаційної безпеки як із питань засобів масових комунікацій, так і кібербезпеки;

в) *організаційно-технічний механізм,* до якого запропоновано внести кваліфікаційні вимоги до фахівців сфери кібербезпеки та розробити методики добору й оцінювання кадрів;

г) *інформаційний механізм,* при цьому: здійснити моніторинг інформаційної безпеки України; впровадити стандартизацію, сертифікацію та ліцензування діяльності у сфері забезпечення інформаційної безпеки України; удосконалити державну інформаційну інфраструктуру, враховуючи вимоги інформаційної безпеки України; удосконалити систему освіти, беручи до уваги потреби інформаційної безпеки України; розробити міжрегіональні, державні та міждержавні програми розвитку системи інформаційної безпеки України;

набули подальшого розвитку:

– перелік пріоритетних напрямів розвитку механізмів затвердження державної інформаційної політики шляхом уточнення переліку цих напрямів,

їх формулювання на основі міжнародного та національного досвіду, зокрема напрями підвищення охорони державної таємниці, а саме: визначення в законодавстві порядку створення та застосування інформаційно-телекомунікаційних систем, у яких зберігається, обробляється, розповсюджується, збирається інформація з обмеженим доступом, порядок створення та ліцензування програмно-апаратних комплексів інформації;

– аналіз та узагальнення кращого міжнародного досвіду, насамперед країн ЄС і США, щодо формування та реалізації механізмів забезпечення державної політики інформаційної безпеки, а також розроблення його пріоритетних напрямів розвитку, відповідних національних механізмів в Україні, в тому числі: забезпечення доступу до даних; створення національного інформаційного потенціалу; використання інформаційних ресурсів у національних інтересах; створення загальної системи охорони даних; сприяння міжнародній взаємодії у сфері комунікації та інформації; гарантування інформаційного державного суверенітету; розвиток інформаційної інфраструктури, що є доцільними при розробці (корегуванні) законодавства України у даній сфері, насамперед Стратегії кібербезпеки України та Закону України «Про основні засади забезпечення кібербезпеки в Україні»;

– перелік загроз інформаційній безпеці: монополізація інформаційної сфери національними та зарубіжними олігархічними структурами; блокування роботи державних ЗМІ щодо інформування українських та іноземних громадян; дефіцит професійних кадрів; неефективність механізмів забезпечення формування і реалізації державної політики інформаційної безпеки; несанкціонований доступ до інформації; негативний вплив на інформаційні ресурси та в цілому на інформаційну інфраструктуру; недостатність поінформованості населення за кордоном про ведення зовнішньополітичної та внутрішньополітичної діяльності країни; поширення неправдивої інформації про ведення зовнішньої і внутрішньої політики України; вплив інформаційного характеру, що здійснюють іноземні політичні, економічні, військові й інформаційні структури на розроблення і втілення засад зовнішнього та внутрішнього характеру політичного сегменту нашої держави; обмеження свобод, якого зазнають українські громадяни та юридичні особи в межах інформаційної сфери за кордоном.

Практичне значення отриманих результатів полягає в тому, що теоретичні положення, висновки та рекомендації, розроблені автором і запропоновані в дисертації, можуть бути використані для удосконалення механізмів забезпечення інформаційної безпеки як складової державної безпеки України, що сприятиме їх модернізації в умовах сучасного розвитку даної сфери та створенню безпечного інформаційного середовища на території нашої держави.

Наукові висновки та теоретичні положення дисертаційної роботи фактично доведені до рівня конкретних пропозицій і практичних

рекомендацій для використання в галузі науки державного управління. Зокрема, результати дослідження були використані в практичній діяльності:

– Департаменту інформаційно-комунікаційних технологій Київської міської державної адміністрації (довідка щодо впровадження від 19 липня 2019 року);

– Київської міської митниці Державної фіскальної служби України (довідка щодо впровадження від 13 вересня 2019 року);

– Міжрегіонального управління Національного агентства України з питань державної служби у м. Києві, Київській, Чернігівській та Черкаській областях (довідка щодо впровадження від 2 квітня 2019 року);

– Центру адаптації державної служби до стандартів ЄС (довідка щодо впровадження від 19 квітня 2019 року).

Отримані результати можуть бути застосовані для подальших науково-дослідних розробок теоретико-методологічних питань, пов'язаних із застосуванням механізмів забезпечення інформаційної безпеки як складової державної безпеки та удосконалення системи інформаційної безпеки України.

Особистий внесок здобувача. Основні теоретичні положення та розробки в межах дослідження, зокрема ті, що характеризують його наукову новизну і практичне значення результатів, отримані автором особисто.

Апробація результатів дисертації. Основні положення дисертаційної роботи були презентовані та обговорені на: науково-практичній конференції «Публічна служба в модерній державі», присвяченій 100-річчю державної служби України (м. Київ, 2018 р.), круглому столі «Проблематика процесу децентралізації надання послуг в об'єднаних територіальних громадах» (м. Київ, 2018 р.), VI Всеукраїнській науково-практичній конференції студентів та аспірантів «Організаційно-управлінські та психологічні аспекти сучасного ринку праці України» (м. Київ, 2017 р.), науково-практичній конференції «Форум прямої демократії» (м. Київ, 2018 р.), круглому столі «Трудова міграція в епоху глобалізації: виклики для України» (м. Київ, 2018 р.).

Публікації. Наукові результати дисертаційної роботи опубліковано в 13 наукових працях, зокрема: 1 монографія (у співавторстві); 7 статей у наукових фахових виданнях України з державного управління, з них 1 – в зарубіжному науково-періодичному виданні та 5 публікацій у збірниках матеріалів науково-практичних конференцій.

Структура та обсяг дисертації. Дисертаційна робота складається із вступу, трьох розділів, висновків, списку використаних джерел та додатків. Повний обсяг дисертації становить 233 сторінки, із них 210 сторінок основного тексту, включаючи 1 таблицю та 4 рисунки. Список використаних джерел налічує 202 найменування.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано вибір, актуальність і стан розроблення теми дисертаційної роботи, подано її загальну характеристику, вказано на зв'язок дисертації з науково-дослідними роботами, визначено мету, завдання, об'єкт, предмет, охарактеризовано методологічну базу, наукову новизну та практичну значущість одержаних результатів, наведено дані щодо апробації та опублікування результатів дослідження.

У **першому розділі** – *"Теоретико-методологічні засади публічної політики у сфері інформаційної безпеки"* – проаналізовано теоретичні засади державної політики інформаційної безпеки, подано класифікацію механізмів державного управління у сфері інформаційної безпеки та узагальнено зарубіжний досвід щодо механізмів забезпечення державної політики інформаційної безпеки.

Виокремлено чотири наукові напрямки аналізу термінологічної бази інформаційної безпеки, а саме:

– технічний – визначаються аспекти захисту даних технічного характеру в межах інформаційних систем і мереж та здатність учасників інформаційної безпеки до протидії злочинам інформаційного типу;

– правовий – розкривається правова сторона захисту інтересів людини, суспільства та держави в інформаційній галузі. Діяльність авторів у межах цього напрямку здебільшого зосереджується на правовому захисті даних, прогресу законодавчих норм та вдосконалювання практики в сфері інформації, інформаційних технологій і захисту даних;

– соціально-політичний – аналізуються аспекти політики щодо забезпечування інформаційної безпеки та вивчаються питання захисту суб'єктів інформаційної безпеки від негативних інформаційних впливів;

– організаційний – досліджується інформаційна безпека як складовий елемент національної безпеки.

На основі трактування різними авторами сутності поняття «інформаційна безпека» наведено власне його бачення – не лише як стану захищеності інформаційного середовища та ресурсів, задоволення інформаційних потреб громадян, суспільства та держави, але й захищеності прав суб'єктів інформаційних правових відносин від негативних зовнішніх та внутрішніх факторів, що становлять загрозу конфіденційності, цілісності та доступності інформації, застосування якого сприятиме підвищенню рівня обґрунтованості державної політики інформаційної безпеки.

Доведено, що основними механізмами у сфері інформаційної безпеки є: нормативно-правовий, інституційний, організаційно-технічний, інформаційний.

Встановлено, що нормативно-правовий механізм – це комплекс ієрархічних правових норм та принципів, які врегульовують зміст та процес здійснення політики інформаційної безпеки, тобто правовий механізм інформаційної безпеки, та комплекс ролей та взаємозв'язків, що містить

правовідносини, які утворюються під час проведення політики інформаційної безпеки та специфічної ролі, форми і методики діяльності суб'єктів здійснення політики інформаційної безпеки. Інституційним механізмом є комплекс державних інститутів, що задіяні у процесі створення і втілення політики інформаційної безпеки. Організаційно-технічний механізм – сукупність важелів та інструментів забезпечення інформаційної безпеки України. Інформаційний механізм ґрунтується на тому, що кожний суб'єкт інформаційного процесу повинен мати відповідну правову свідомість, бути законослухняним, добре уявляти наслідки свої дій для інших суб'єктів та міру відповідальності на випадок порушення їхніх життєво важливих інтересів.

Необхідність гарантування інформаційної безпеки зумовлюється потребою забезпечення державної безпеки України в цілому, існуванням таких загроз її інформаційній сфері, які здатні заподіяти значну шкоду загальнодержавним інтересам, ураховуючи те, що за допомогою інформації можна впливати на зміну свідомості та поведінку людей.

Протидія зовнішнім загрозам інформаційній безпеці України відбувається в умовах прогресування тенденції до переформатування сфер впливу у світовому просторі на тлі глобалізації політичних, соціально-економічних, культурних відносин. Виявлення та аналіз відповідних загроз ускладнюється низкою факторів: у частини населення відсутнє відчуття зовнішніх загроз країні; у Воєнній доктрині та Доктрині інформаційної безпеки немає чіткого визначення таких потенційних зовнішніх загроз, що призводить до відсутності відповідної їх класифікації й ранжування за ступенем важливості, порівняльної динаміки зростання, розуміння причин і джерел їх появи.

Рух України до інтеграційних процесів ЄС набув значення цивілізаційного вибору України. В системі зовнішньополітичних пріоритетів йому відводиться особливий статус. Угода про асоціацію з ЄС містить положення, реалізація яких має сприяти розвитку і зміцненню діалогу у різних сферах, у тому числі поступовій конвергенції позицій України з ЄС у сфері зовнішньої та безпекової політики. Крім того, Україна зацікавлена в залученні до роботи Агентства з питань мережевої та інформаційної безпеки Європейського Союзу (ENISA), до діяльності Європейського центру досліджень та компетенції з кібербезпеки, а також до тренінгів ЄС щодо координації механізмів спільного реагування ЄС і держав-членів на масштабні інциденти та кризові ситуації в галузі кібербезпеки. Активізацію євроінтеграційних процесів можна розглядати і в контексті інтенсивнішого включення України в міжнародну співпрацю з урегулювання конфліктів та протистояння загрозам у сфері безпеки.

На основі досвіду ЄС та його окремих країн у сфері формування та реалізації державної політики інформаційної безпеки з'ясовано, що головними напрямами державної політики інформаційної безпеки є: забезпечення доступу до даних; створення національного інформаційного потенціалу; використання інформаційних ресурсів у національних інтересах;

створення загальної системи охорони даних; сприяння міжнародній взаємодії у сфері комунікації та інформації; гарантування інформаційного державного суверенітету; розвиток інформаційної інфраструктури, а також доцільність урахування цього досвіду при розробці (корегуванні) законодавства України у даній сфері, насамперед Стратегії кібербезпеки України та Закону України «Про основні засади забезпечення кібербезпеки в Україні».

У **другому розділі** – "*Державна політика у сфері інформаційної безпеки*" – проаналізовано основні положення державної політики щодо забезпечення інформаційної безпеки, здійснено аналіз головних складових інформаційної безпеки держави, ключових засад позиціювання України щодо проблематики інформаційної безпеки та механізмів протидії інформаційним загрозам.

Визначено, що інформаційна безпека в контексті глобалізаційних процесів та міжнародної інтеграції стає особливо важливою. Держави, які мають потужний потенціал в інформаційному середовищі, можуть впливати на держави з незахищеним інформаційним та кіберпростором. Упродовж останніх трьох років Україна провела в межах інформаційного простору, Інтернету та кіберпростору більшу кількість заходів щодо забезпечення інформаційної безпеки, ніж за весь попередній період незалежності.

Дослідження питань державної інформаційної безпеки дає підстави стверджувати, що забезпечення інформаційної безпеки базується на інформаційній організації країни. Ця організація має гарантувати інформаційну безпеку держави та її суб'єктів під час глобалізаційних процесів та підвищення загрози, яку становить міжнародний тероризм. На жаль, в України є дуже багато чинників, які стають на заваді при створенні такої інформаційної організації, і тут не останню роль відіграє неузгодження роботи державних владних органів щодо забезпечення інформаційної безпеки.

Виокремлено основні завдання забезпечення інформаційної безпеки України, серед яких:

– забезпечення інформаційного суверенітету;

– удосконалення державного регулювання розвитку інформаційної сфери, створивши нормативно-правові та економічні передумови для того, щоб розвивалися національна інформаційна інфраструктура та ресурси, впроваджувалися новітні технології у цій галузі, внутрішній та світовий інформаційний простір наповнювався достовірними відомостями щодо України;

– активне залучення засобів масової інформації до процесу протидії корупції, зловживанню службовим становищем, іншим явищам, які становлять загрозу для національної та інформаційної безпеки України;

– забезпечення конституційного права людей на свободу слова, доступ до інформації, заборона державним органам неправомірно втручатися у роботу засобів масової інформації, не допущення дискримінації в інформаційній сфері та запобігання переслідуванню журналістів;

– застосування комплексних заходів для того, щоб захистити національний інформаційний простір та протидіяти монополії в інформаційній сфері України.

Доведено, що стабільний державний розвиток передбачає не тільки забезпечення економічної, військової, політичної безпеки, а й інформаційної, причому статусність останньої нині значно підвищується. Захист інформаційної сфери держави у всіх її виявах є гарантією збереження і розвитку держави. Наразі Україна, здійснюючи складні демократичні та соціально-економічні трансформації, перебуває в зоні ризику щодо інформаційної безпеки, адже ця сфера довго не мала належної уваги, що зумовило внутрішні протиріччя та конфлікти, інспіровані, зокрема, ззовні інформаційно-комунікаційними засобами.

Подано класифікацію інформаційних загроз, серед яких:

– несанкціонований доступ до інформаційних даних і вплив на інформаційні ресурси, інформаційну інфраструктуру владної вертикалі, що реалізує засади зовнішньої та внутрішньої політики держави, представників України та об’єднань на міжнародній арені та у межах міжнародних організацій;

– недостатність поінформованості населення за кордоном (в першу чергу, у сусідніх з Україною державах) про ведення зовнішньополітичної та внутрішньополітичної діяльності країни;

– поширювання неправдивої інформації про ведення зовнішньої та внутрішньої політики України;

– вплив зовнішніх чинників, на формування яких впливають іноземні політичні, економічні, військові і інформаційні структури;

– утиски свобод, що зазнають українські громадяни і юридичні особи в межах інформаційної сфери за кордоном.

З’ясовано, що механізмами протидії інформаційним загрозам є комплекс різних форм роботи, яка здійснюється органами державної та військової управлінської сфери, громадськими організаціями, політичними інституціями та ін., а також види їхньої взаємодії, що дозволяє оперативно впливати на загрози інформаційній безпеці або керувати ризиками з метою їх локалізації та нейтралізації. При оцінюванні механізмів спираються на: інформаційну державну політику, її вплив на характеристики безпеки; виявлення відхилень характеристик для стабільної роботи, що провадиться системою інформаційної безпеки; визначення зовнішніх умов, які сприяють відхиленням: посилення (за несприятливого зовнішньоекономічного середовища) або послаблення (за сприятливого зовнішнього середовища) загроз. Отже, механізмами протидії загрозам інформаційного характеру насамперед є ті, які базуються на принципах керування ризиками, дають змогу блокувати деструктивні елементи, властивості та процеси, що є руйнівниками системи інформаційної та державної безпеки в цілому, і стимулювати конструктивні елементи, властивості й процеси, які покращують їх функціонування та розвиток.

Захист інформаційної сфери держави у всіх її виявах є гарантією збереження і розвитку держави.

У **третьому розділі** – *"Шляхи модернізації механізмів реалізації інформаційної безпеки в Україні"* – запропоновано підходи запровадження в Україні кращих практик реалізації державної політики інформаційної безпеки, перспективні напрями застосування механізмів реалізації державної політики інформаційної безпеки та напрями вдосконалення системи інформаційної безпеки України.

Аналіз можливостей запровадження в Україні кращих практик реалізації державної політики інформаційної безпеки показав, що вони охоплюють такі сфери: економіка: просувати міжнародні стандарти й інноваційні відкриті ринки, що означає бути готовим до підтримання вільного ринкового оточення, захисту інтелектуальної власності та комерційної таємниці від викрадення, забезпечення верховенства сумісних і безпечних стандартів; захист вітчизняних кібернетичних мереж: сприяти дотриманню поведінкових нормативів у кіберсередовищі як у двосторонній спосіб, так і формуючи багатосторонні організації та багатонаціональне партнерство, що означає бути готовим до вжиття заходів щодо зменшення числа проникнень до власних мереж, забезпечення швидкої реакції на них та розширення можливостей оперативно відновити інформаційну інфраструктуру після нападів; галузь застосування права: розширити співробітництво і посилити силу законності.

Визначення шляхів удосконалення системи інформаційної безпеки України дало підстави сформувати функціональну систему інформаційної безпеки України як складової та інформаційного виміру національної безпеки. Захист та протистояння війнам інформаційного характеру повинні здійснюватися лише в межах розроблених стратегій, спрямованих на захист від інформаційної небезпеки та протистояння війнам інформаційного типу на території України. Така стратегія має забезпечувати як нормативно-правові, так і організаційні норми інформаційної безпеки в Українській державі.

Ефективну реалізацію стратегічних пріоритетів, головних положень і завдань державної політики щодо інформаційної безпеки можливо забезпечити через покращення інформаційного механізму управління інформаційною безпекою, його відповідного забезпечення інтелектуальними кадрами і ресурсами, в тому числі, покращення законодавчої системи щодо проблем національної безпеки, в першу чергу через:

– розвиток управлінських правових положень щодо національної безпеки через відповідні закони, концепції, доктрини, стратегії і програми, в тому числі, антикорупційне законодавство, Національні програми протистояння терористичним та екстремістським явищам, Концепції розвитку Воєнної організації держави, Національної стратегії формування інформаційного суспільства, Доктрини інноваційного та науково-технологічного розвитку тощо;

– розроблення та запровадження національних стандартів та технічних нормативів по застосуванню технологій інформаційно-комунікаційного

характеру, що гармонізовані відповідно до європейських стандартів, в тому числі щодо вимог, які ратифіковані Верховною Радою України у Конвенції про кіберзлочинність;

– розробка та запровадження загальної державної системи для окреслення та аналізу порогових значень даних (індикаторів), що можуть характеризувати рівень захисту інтересів нації у межах різних сфер та реальні загрози нацбезпеці.

Обгрунтовано перелік пріоритетних напрямів розвитку механізмів затвердження державної інформаційної політики шляхом уточнення переліку цих напрямів, їх формулювань на основі міжнародного та національного досвіду, зокрема напрями підвищення охорони державної таємниці, а саме: визначення в законодавстві порядку створення та застосування інформаційно-телекомунікаційних систем, у яких зберігається, обробляється, розповсюджується, збирається інформація з обмеженим доступом, порядок створення та ліцензування програмно-апаратних комплексів інформації. Варто наголосити на необхідності забезпечувати кіберзахист державним електронним інформаційним ресурсам, інформаційним даним, захищати які вимагає закон, а також інформаційній інфраструктурі, що перебуває в українській юрисдикції, оскільки погіршення її стабільної роботи негативно вплине на національну безпеку та оборону Української держави (явище критичної інформаційної інфраструктури) та ін. Конкретних зусиль треба докласти для підтримки дійового інструментарію у функціонуванні державної системи кібернетичної безпеки, зміцненні інформаційного захисту в межах національного, наднаціонального й міжнародного універсального рівня, беручи до уваги те, що проблематику порушено у глобальному вимірі.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальне наукове завдання, яке полягає в теоретико-методологічному обґрунтуванні формування та розвитку механізмів забезпечення інформаційної безпеки як складової державної безпеки України та розробці практичних рекомендацій органам влади щодо їх упровадження. Результати, отримані в процесі дослідження, підтверджують досягнення поставленої мети й вирішення завдань, дають підстави сформулювати наступні висновки і практичні рекомендації:

1. Визначено чотири наукові напрями дослідження терміносистеми у сфері інформаційної безпеки, а саме: технічний, правовий, суспільно-політичний та організаційний. Інформаційну безпеку запропоновано розуміти не лише як стан захищеності інформаційного середовища та ресурсів, задоволення інформаційних потреб громадян, суспільства і держави, але й захищеності прав суб’єктів інформаційних правових відносин від негативних зовнішніх та внутрішніх факторів, що становлять загрозу конфіденційності, цілісності й доступності інформації, застосування якого сприятиме підвищенню рівня обґрунтованості державної політики

інформаційної безпеки. З’ясовано, що у сфері забезпечення інформаційної безпеки України основними механізмами забезпечення державної політики інформаційної безпеки є: нормативно-правовий, організаційно-технічний, інституційний, інформаційний (інформаційний патронат, інформаційна кооперація, інформаційний захист).

2. Проаналізовано та узагальнено кращий міжнародний досвід, насамперед країн ЄС та США, щодо формування й реалізації механізмів забезпечення державної політики інформаційної безпеки, а також розроблення його пріоритетних напрямів розвитку, відповідних національних механізмів в Україні, а саме: забезпечення доступу до даних; створення національного інформаційного потенціалу; використання інформаційних ресурсів у національних інтересах; створення загальної системи охорони даних; сприяння міжнародній взаємодії у сфері комунікації та інформації; гарантування інформаційного державного суверенітету; розвиток інформаційної інфраструктури.

3. Доведено теоретико-методологічний підхід до розуміння сутності взаємодії державної політики інформаційної безпеки та державної політики у сфері кібербезпеки, який на відміну від наявного, формально визначеного в національному законодавстві, передбачає розгляд державної політики у сфері кібербезпеки як невід’ємної специфічної складової державної інформаційної безпеки, яка повинна включати низку напрямів, а саме: кіберзахист, кібероборону, кіберрозвідку, протидію кібершахрайству, кібертероризму, кібершпигунству, що сприятиме систематизації та упорядкуванню заходів із забезпечення державної політики інформаційної безпеки.

4. Обґрунтовано перелік загроз інформаційній безпеці: монополізація інформаційної сфери національними та зарубіжними олігархічними структурами; блокування роботи державних ЗМІ щодо інформування українських та іноземних громадян; дефіцит професійних кадрів; неефективність механізмів забезпечення формування і реалізації державної політики інформаційної безпеки; несанкціонований доступ до інформації; негативний вплив на інформаційні ресурси та в цілому на інформаційну інфраструктуру; недостатність поінформованості населення за кордоном про ведення зовнішньополітичної та внутрішньополітичної діяльності країни; поширення неправдивої інформації про ведення зовнішньої та внутрішньої політики України; вплив інформаційного характеру, що його здійснюють іноземні політичні, економічні, військові та інформаційні структури на розроблення і втілення засад зовнішнього та внутрішнього характеру політичного сегменту нашої держави; обмеження свобод, якого зазнають українські громадяни та юридичні особи в межах інформаційної сфери за кордоном.

5. Удосконалено перелік пріоритетних напрямів розвитку механізмів затвердження державної інформаційної політики шляхом уточнення переліку цих напрямів, їх формулювання на основі міжнародного та національного

досвіду, зокрема напрями підвищення охорони державної таємниці, а саме: визначення в законодавстві порядку створення та застосування інформаційно-телекомунікаційних систем, у яких зберігається, обробляється, розповсюджується, збирається інформація з обмеженим доступом, порядок створення та ліцензування програмно-апаратних комплексів інформації.

6. Запропоновано пріоритетні напрями удосконалення механізмів забезпечення інформаційної безпеки:

а) правового (визначити консенсус (згоду) в суспільних відносинах, узгодженість поглядів та застосувати юридичні норми, правомірну поведінку суб'єктів відносин інформаційного характеру, взаємин в інформаційному секторі; забезпечити інформаційний суверенітет, незалежність України на міжнародній арені, зокрема завдяки електронним телекомунікаціям; забезпечити інформаційну безпеку людей, їх об'єднань, соціуму та країни як складову українського національної безпеки; визначити правомірну поведінку для кожного учасника інформаційного співробітництва в нашій країні; захистити інформацію від несанкціонованих проникнень, злочинних дій (знищення, модифікація, спотворення, порушення приватності, конфіденційність тощо); гармонізувати національне законодавство з міжнародним, ураховуючи особливості розвитку України; розробити інформаційний Кодекс з уточненням його першочергових завдань; внести зміни до Закону України «Про національну безпеку України» та Закону України «Про основні засади забезпечення кібербезпеки України» стосовно необхідності розробки стратегії інформаційної безпеки замість Доктрини інформаційної безпеки України після затвердження Стратегії національної безпеки України, проведення з цією метою аналізу стану інформаційної безпеки, уточнення завдань та функцій складових системи забезпечення інформаційної безпеки);

б) інституційного (створити ефективну багаторівневу державну систему підтримки інформаційного захисту із задіянням єдиних правових норм і механізмів, покликаних захистити інформаційні ресурси, інформаційно-телекомунікаційну інфраструктуру й інформаційні права людей, ефективно координувати діяльність владних держструктур та управлінь; здійснити розробку механізму взаємодії державних і місцевих владних органів у сфері підтримки інформаційної безпеки; сформувати державну політику забезпечення регіонального інформаційного захисту, створити необхідні для втілення такої політики організаційні структури і нормативну правову базу; зміцнити співпрацю структур регіонального характеру та державних органів виконавчої влади при вирішенні проблем такої сфери, як інформаційна безпека; забезпечити ефективність державної політики інформаційної безпеки, у зв'язку з чим пропонуємо перетворити Національний координаційний центр кібербезпеки України в Національний координаційний центр з питань інформаційної безпеки, визначити відповідальним за формування та реалізацію державної політики

інформаційної безпеки Міністерство цифрових трансформацій, підпорядкувавши йому Державний комітет телебачення та радіомовлення, що дозволить комплексно вирішувати проблеми у сфері інформаційної безпеки як із питань засобів масових комунікацій, так і кібербезпеки);

в) організаційно-технічного (укомплектувати новостворені підрозділи кібернетичного захисту якісними кадрами та забезпечити їх подальше професійне удосконалення; теоретично обґрунтувати і практично визначити кваліфікаційні вимоги до фахівців сфери кіберзахисту, розробити методики добору кадрів з урахуванням особливостей сфери професійного характеру);

г) інформаційного (здійснити моніторинг інформаційної безпеки України; впровадити стандартизацію, сертифікацію та ліцензування діяльності у сфері забезпечення інформаційної безпеки України; удосконалити державну інформаційну інфраструктуру, враховуючи вимоги інформаційної безпеки України; удосконалити систему освіти, беручи до уваги потреби інформаційної безпеки України; розробити міжрегіональні, державні та міждержавні програми розвитку системи інформаційної безпеки України).

7. Окреслено шляхи вдосконалення системи інформаційної безпеки України, що дало підстави сформувати функціональну систему інформаційної безпеки України як складової та інформаційного виміру національної безпеки. При цьому Україні слід створити ефективну національну систему кібернетичної безпеки; посилити спроможності суб'єктів безпекової та оборонної галузей для підтримки дійової протидії воєнним кіберзагрозам, кібершпигунству, кібертероризму й кіберзлочинності, поглибити міжнародне співробітництво в даному секторі. Варто наголосити на необхідності забезпечити кіберзахист державним електронним інформаційним ресурсам, інформаційним даним, захистити які вимагає закон, а також інформаційній інфраструктурі, що перебуває в українській юрисдикції, оскільки погіршення її стабільної роботи негативно вплине на національну безпеку та оборону Української держави (явище критичної інформаційної інфраструктури) та ін. Конкретних зусиль треба докласти для підтримки дійового інструментарію у функціонуванні державної системи кібернетичної безпеки, зміцненні інформаційного захисту в межах національного, наднаціонального й міжнародного універсального рівня, беручи до уваги те, що проблематику порушено у глобальному вимірі.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Монографії

1. Турчак А.В. Механізми забезпечення політики інформаційної безпеки як складової державної безпеки України (підрозділ 4.7). *Публічне управління в умовах інституційних змін:* колективна монографія / за наук. ред. д. держ. упр. Р. В. Войтович та П.В. Ворони. К.: ІПК ДСЗУ, 2018. 475 с.

Праці, що відображають основні наукові результати дисертації

2. Турчак А.В. Сутність державної політики інформаційної безпеки. *Державно-управлінські студії*. 2018. № 5 (7). URL: http://box5800.temp.domains/~ipkeduua/sutnist-derzhavnoi-polityky-informatsiinoi-bezpeky/

3. Турчак А.В. Реалізація національних механізмів протидії інформаційним загрозам. *Державне управління та місцеве самоврядування*. 2019. Вип. 2 (41). С. 86-91.

4. Турчак А.В. Основні складові інформаційної безпеки держави. *Аспекти публічного управління*. 2019. №5. Т. 7. С. 44-56.

5. Турчак А.В. Основні засади державної політики забезпечення інформаційної безпеки в Україні. *Інвестиції: практика та досвід.* 2019. № 11. С. 123-127.

6. Турчак А.В. Перспективні напрямки застосування механізмів реалізації державної політики інформаційної безпеки в Україні. *Економіка та держава. Серія державне управління*. 2019. №4 (12). С. 114-117.

7. Турчак А. В. Особливості удосконалення системи інформаційної безпеки України. *Збірник наукових праць Донецького державного університету управління «Сучасні проблеми державного управління в умовах системних змін»*. Серія "Державне управління". Т. ХХ, вип. 310. Маріуполь, ДонДУУ, 2019. С. 105-112.

Статті в зарубіжних виданнях

8. Turchak A.V. Classification of mechanisms of public administration in the field of information security. *News of science and education*. 2019. № 2 (63). С.40-47.

Праці, що додатково відображають наукові результати дисертації

9. Турчак А. В. Взаємодія інформаційних структур інститутів громадянського суспільства та органів публічної влади в процесі розбудови правової держави. *Публічна служба в модерній державі*: матеріали міжнар. наук.-практ. конф., присвяченої 100-річчю державної служби України (м. Київ, 13 черв. 2018 р.). К.: ІПК ДСЗУ, 2018. С. 217.

10. Турчак А.В. Інформаційна публічність та прозорість – запорука демократичного розвитку країни в процесі децентралізації (на прикладі бюджетного процесу). *Проблематика процесу децентралізації надання послуг в об'єднаних територіальних громадах*: матеріали круглого столу (м. Київ, 18 квіт. 2018 р.). К.: ІПК ДСЗУ, 2018. С. 44.

11. Турчак А.В. Іформаційна безпека держави як невід'ємна складова національної безпеки. *Організаційно-управлінські та психологічні аспекти сучасного ринку праці України*: тези доповідей VI Всеукр. наук.-практ. конф.

студентів та аспірантів (м. Київ, 27 лист. 2017 р.). К.: ІПК ДСЗУ, 2017. Ч. ІІ. С. 93.

12. Турчак А.В. Електронні механізми прямої демократії як складова державно-громадської взаємодії. *Форум прямої демократії*: тези доповідей наук.-практ. конф. (м. Київ, 4 груд. 2018 р.). К.: ІПК ДСЗУ, 2018. Ч. 1. С. 230.

13. Турчак А.В. Глобальні зміни в структурі зайнятості як чинник трансформації міжнародного ринку праці. *Трудова міграція в епоху глобалізації: виклики для України:* тези доповідей круглого столу, м. Київ, 12 груд. 2018 р. / За заг. ред Черасова А. В. К.: ІПК ДСЗУ, 2019. – С. 126-129.

АНОТАЦІЯ

Турчак А. В. Механізми забезпечення інформаційної безпеки як складової державної безпеки України. Рукопис.

Дисертація на здобуття наукового ступеня кандидата наук з державного управління за спеціальністю 25.00.02 – механізми державного управління. – Інститут підготовки кадрів державної служби зайнятості України, Київ, 2020.

У дисертаційній роботі вирішено актуальне наукове завдання, яке полягає у теоретико-методологічному обґрунтуванні формування та розвитку механізмів забезпечення інформаційної безпеки як складової державної безпеки України та розробці практичних рекомендацій органам влади щодо їх упровадження.

Розкрито основні положення державної політики щодо забезпечення інформаційної безпеки та проаналізовано її головні складові. Державна інформаційна політика має низку цілей, зокрема – боротися з феноменом фейкових новин, використовуючи відповідні засоби, що обумовлює необхідність розробки урядової програми для того, аби школярі та менш захищені верстви (пенсіонери, інваліди) навчалися медіаграмотності. Головними складовими забезпечення інформаційної безпеки держави є: ідентифікація обсягу інформаційної продукції, яка виробляється на території держави; стійкість та цілісність мереж в умовах зростання інформаційного навантаження; здатність держави інтенсифікувати розвиток виробництва та поширення інформації; відкритість доступу до інформаційно-комунікаційних технологій для усіх верств населення.

Проаналізовано особливості позиціювання України щодо проблематики інформаційної безпеки, а також досліджено стан і проблеми нормативно-стратегічного та організаційного забезпечення національних механізмів протидії інформаційним загрозам.

Проаналізовано можливості запровадження в Україні кращих практик реалізації державної політики інформаційної безпеки та виявлено, що вони охоплюють такі сфери: економіка, захист вітчизняних кібернетичних мереж, галузь застосування права, збройні сили. Окреслено можливі шляхи вдосконалення системи інформаційної безпеки України. З’ясовано, що до пріоритетів у роботі має увійти вирішення таких завдань: створити мирну, безпечну, стійку й відкриту інформаційну сферу; сприяти відповідальній

поведінці країн; відповідними заходами зміцнити довіру й інформаційний обмін; нарощувати потенціал тощо. Таким чином, необхідна розробка глобальних поведінкових стандартів для кіберпростору, слід розширити можливості в міжнародно-правовій системі стосовно попередження й протидії кіберзлочинності; розвивати й заохочувати позитивний досвід щодо донесення інформації про надзвичайні події, створювати поведінкові стандарти для кіберпростору. Водночас, Україні треба створити ефективну національну систему кібернетичної безпеки; посилити спроможності суб'єктів безпекової та оборонної галузей для підтримки дійової протидії воєнним кіберзагрозам, кібершпигунству, кібертероризму і кіберзлочинності, поглибити міжнародне співробітництво в цьому секторі.

Ключові слова: державна політика, інформаційні технології, інформація, інформаційна безпека, кібербезпека, механізми державного управління, національна безпека.

ANNOTATION

Turchak A. V. Mechanisms for providing information security as a component of the state security of Ukraine. Manuscript.

Thesis for a Candidate Degree in Public Administration, specialty 25.00.02 - Mechanisms of Public Administration. - Institute for Personnel Training of the State Employment Service of Ukraine, Kyiv, 2020.

The thesis deals with the actual scientific problem, which consists in the theoretical and methodological substantiation of the formation and development of mechanisms for ensuring information security as a component of state security of Ukraine and the development of practical recommendations to the authorities on their implementation.

The main provisions of the state policy on ensuring information security are revealed and its main components analyzed. The state information policy has a number of goals, in particular, to combat the phenomenon of fake news, using appropriate means, which necessitates the development of a government program in order for students and less protected layers (pensioners, people with disabilities) to study media literacy. The main components of providing information security of the state are: identification of the volume of information products, which is produced on the territory of the state; stability and integrity of networks in the conditions of increasing information load; the state's ability to intensify production and dissemination of information; open access to information and communication technologies for all segments of the population.

The peculiarities of Ukraine's position on information security issues are analyzed, and the state and problems of regulatory, strategic and organizational support of national mechanisms for counteracting information threats are researched.

The possibilities of introduction of the best practices in implementation of the state policy of information security in Ukraine have been analyzed and they cover the following areas: economy, protection of domestic cybernetic networks,

sphere of application of law, armed forces. Possible ways of improving the information security system of Ukraine are outlined. It was clarified that the following tasks should be included in the priorities of work: to create a peaceful, safe, stable and open informational sphere; promote responsible behavior of countries; Relevant measures to strengthen trust and information exchange; to increase the capacity and so on. As a consequence, the development of global behavioral standards for cyberspace is necessary, it is necessary to expand the possibilities in the international legal system regarding the prevention and counteraction of cybercrime; develop and encourage positive experiences in reporting information on emergencies, and create behavioral standards for cyberspace. At the same time, Ukraine needs to work on creating an effective national cyber security system; strengthening the capabilities of security and defense industries to support effective counteraction to military cyber threats, cyber-espionage, cyber-terrorism and cybercrime, and deepening international cooperation in this sector.

The list of threats to information security is presented: monopolization of the information sphere by national and foreign oligarchic structures; blocking the work of state-owned media in informing Ukrainian and foreign citizens; shortage of professional staff; inefficiency of mechanisms for ensuring the formation and implementation of state information security policy; unauthorized access to information; negative impact on information resources and the information infrastructure in general; insufficient awareness of the population abroad about conducting foreign and domestic political activities of the country; dissemination of false information about Ukraine's foreign and domestic policy; the influence of the informational nature exercised by foreign political, economic, military and information structures on the development and implementation of the foundations of the external and internal character of the political segment of our country; restriction of freedoms experienced by Ukrainian citizens and legal entities within the information sphere abroad.

Key words: state policy, information technologies, information, information security, cybersecurity, mechanisms of state administration, national security.

PODSUMOWANIE

Turchak A. V. Mechanizmy zapewniające bezpieczeństwo informacji jako element bezpieczeństwa państwa Ukrainy. Rękopis.

Praca doktorska na stopień naukowy w administracji publicznej, specjalność 25.00.02 - mechanizmy administracji publicznej. - Instytut szkolenia Państwowej Służby Zatrudnienia Ukrainy, Kijów, 2020.

Praca dotyczy rzeczywistego problemu naukowego, polegającego na teoretycznym i metodologicznym uzasadnieniu tworzenia i rozwoju mechanizmów zapewniania bezpieczeństwa informacji jako elementu bezpieczeństwa państwa Ukrainy oraz opracowywania praktycznych zaleceń dla władz dotyczących ich wdrażania.

Ujawniono główne postanowienia polityki państwa w zakresie bezpieczeństwa informacji i analizowano jej główne elementy. Polityka informacji publicznej ma szereg celów, w szczególności - zwalczanie zjawiska fałszywych wiadomości, przy użyciu odpowiednich środków, co wymaga opracowania rządowego programu dla studentów i mniej chronionych grup (emerytów, osób niepełnosprawnych) do studiowania umiejętności korzystania z mediów. Głównymi elementami zapewniającymi bezpieczeństwo informacji państwa są: identyfikacja ilości produktów informacyjnych wytwarzanych na terytorium państwa; stabilność i integralność sieci w obliczu rosnącego obciążenia informacyjnego; zdolność państwa do zintensyfikowania rozwoju produkcji i rozpowszechniania informacji; otwarty dostęp do technologii informacyjnych i komunikacyjnych dla wszystkich grup ludności.

Analizowane są osobliwości pozycjonowania Ukrainy w kwestiach bezpieczeństwa informacji, a także status i problemy normatywno-strategicznego i organizacyjnego wsparcia krajowych mechanizmów przeciwdziałania zagrożeniom informacyjnym.

Analizowane są możliwości wprowadzenia najlepszych praktyk wdrażania polityki bezpieczeństwa informacji państwa na Ukrainie i okazuje się, że obejmują one następujące sfery: gospodarkę, ochronę krajowych sieci cybernetycznych, sferę stosowania prawa, siły zbrojne. Przedstawiono możliwe sposoby poprawy systemu bezpieczeństwa informacji Ukrainy. Stwierdzono, że priorytety w pracy powinny obejmować następujące zadania: stworzenie spokojnej, bezpiecznej, stabilnej i otwartej sfery informacyjnej; promować odpowiedzialne zachowanie kraju; wzmocnić zaufanie i wymianę informacji za pomocą odpowiednich środków; zwiększyć pojemność itp. W związku z tym konieczne jest opracowanie globalnych standardów zachowania w cyberprzestrzeni oraz rozszerzenie możliwości międzynarodowego systemu prawnego w zakresie zapobiegania cyberprzestępczości i zwalczania tego zjawiska; rozwijanie i promowanie pozytywnych doświadczeń w komunikowaniu o sytuacjach kryzysowych oraz tworzenie standardów zachowania w cyberprzestrzeni. Jednocześnie Ukraina musi pracować nad stworzeniem skutecznego krajowego systemu bezpieczeństwa cybernetycznego; zwiększanie zdolności podmiotów sektora bezpieczeństwa i obrony do wspierania skutecznego przeciwdziałania zagrożeniom cybernetycznym, szpiegostwu, cyberterroryzmowi i cyberprzestępczości oraz pogłębianie współpracy międzynarodowej w tym sektorze.

Słowa kluczowe: polityka publiczna, technologie informacyjne, informacja, bezpieczeństwo informacji, cyberbezpieczeństwo, mechanizmy administracji publicznej, bezpieczeństwo narodowe.

Підписано до друку 20.02.2020
Формат 148х210 мм. Обл.-вид.арк. 0,9.
Наклад 100 прим.

Свідоцтво серії ДК № 1805 від 25.05.2004
Віддруковано з оригінал-макета в Інституті підготовки кадрів державної служби зайнятості України
03038, м. Київ, вул. Нововокзальна, 17, тел. (044) 536 -14-85