

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

Петрова Тетяна Миколаївна

ДЕРЖАВНА ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Спеціальність: 074 Публічне управління та адміністрування

АВТОРЕФЕРАТ

магістерської роботи на здобуття наукового ступеня
магістра публічного управління

Миколаїв – 2019

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність дослідження. В сучасних умовах розвитку інформаційних технологій відбуваються зміни у всіх сферах суспільного життя України. Інформація стає вагомим продуктом, який впливає не тільки стан внутрішньої політики, а й забезпечує активну інтеграцію будь-якої країни на світову арену.

Захист національного інформаційного суверенітету та пошук нових ефективних моделей системи забезпечення інформаційної безпеки залишається актуальним завданням сьогодення. В першу чергу, це пов'язано з необхідністю протистояти протиправним втручанням в інформаційний простір України, захищати населення від негативного психологічного впливу, зберігати національні інформаційні ресурси, виготовляти власний інформаційний продукт.

Останні декілька років Україна активно реалізовує курс на євроінтеграцію, який є стратегічним пріоритетом національної зовнішньої політики. Для державної системи забезпечення інформаційної безпеки головним завданням є удосконалення нормативно-правової бази, яка б забезпечувала баланс між міжнародними стандартами та була максимально наближеною до сучасних українських реалій, забезпечувала виконання національних інтересів в інформаційній сфері. На законодавчій основі забезпечувалась і контролювалась робота з інформацією, її збереження, передача, розповсюдження, доступність та достовірність для забезпечення безпеки громадян України, всього суспільства в цілому та держави.

Поява нових викликів і загроз національній безпеці України досліджується як державними аналітичними центрами та і багатьма науковцями. Значний внесок у теоретичну розробку питань забезпечення інформаційної безпеки зробили як вітчизняні так і зарубіжні науковці. В роботах О. Білоруса, О. Бойченка, І. Валюшко, О. Гиркіної, В. Горбуліна, Р. Калюжного, Б. Кормича, В. Ліпкана, Ю. Лісовської, О. Марченко, Н. Нижника, О. Олійника, В. Семенова, О. Тихомирова, Т. Ткачука, В. Цимбалюка та інших предметом науково-теоретичних досліджень є з'ясування понять інформаційна безпека, інформаційний суверенітет, національний продукт, поняття та види загроз та небезпек для національних інтересів України та світу, становлення та розвиток інформаційного суспільства та багато інших.

Враховуючи викладене, для проведення ефективної державної політики в сфері забезпечення інформаційної безпеки, влада України та її державні органи мають визначити унікальну стратегію поведінки для забезпечення виконання національних інтересів України на основі проведених досліджень.

Мета та завдання дослідження. Мета дослідження полягає у з'ясуванні основ

державної політики України у сфері інформаційної безпеки. Завданнями дослідження є:

- розкрити теоретико-методологічні засади дослідження державної політики інформаційної безпеки в Україні;
- охарактеризувати основні механізми державної політики України щодо реалізації інформаційної безпеки;
- визначити сучасні виклики та загрози для інформаційної безпеки України;
- виділити напрямки державної політики щодо удосконалення інформаційної безпеки України як основи національної безпеки;
- надати висновки та рекомендації щодо подальших напрямів вивчення означеної проблематики дослідження та використання його результатів на прикладному рівні.

Об'єктом дослідження є державна політика України.

Предметом дослідження є державна політика інформаційної безпеки України.

Методи дослідження робота ґрунтується на використанні загальнонаукових (аналіз і синтез, збір, обробка та аналіз матеріалів з даної тематики, метод узагальнення та метод аналогії) та спеціальних методів (порівняльний, структурний та системний аналіз).

Порівняльний метод використовувався для дослідження різних підходів до визначення поняття інформаційна безпека, інформаційний суверенітет. Методи системного та структурного аналізу використовувались для дослідження нормативно-правової бази, при розгляді ризиків та небезпек для системи забезпечення інформаційної безпеки України.

Слід зазначити, що в роботі широко використовується комплексний підхід до методології дослідження, коли методи доповнюють один одного та дозволяють розглядати досліджувані процеси і явища в їх єдності і різноманітності.

Наукова новизна одержаних результатів полягає в тому, що в роботі цілісно виконано комплексне дослідження особливостей державної політики інформаційної безпеки України.

Наукова новизна магістерської роботи полягає у тому, що: здійснений докладний огляд загроз та небезпек інформаційній безпеці України, порівняні такі поняття як інформаційна війна, інформаційний тероризм та інформаційні злочини, визначений масштаб дії цих ризиків. Проаналізовані вірогідні кібератаки під час президентський виборів України 2019 року. Запропоновані шляхи вдосконалення нормативно-правової бази у сфері забезпечення інформаційної безпеки України, та адаптація безпекового законодавства до міжнародних стандартів.

Практичне значення одержаних результатів полягає в тому, що результати дослідження можуть бути використані для викладання курсів «Публічна політика»,

«Публічне управління». «Антикризове управління».

На практичному рівні результати дослідження можуть бути застосовані в роботі державних органів та позадержавних організацій, які забезпечують виконання законодавства України та здійснюють контроль в галузі інформаційної безпеки. Певні результати дослідження були впроваджені в роботі головного управління Пенсійного фонду України в Миколаївській області (довідка про провадження результатів магістерської роботи № 2199/02.02 від 19.03.2019).

Особистий внесок магістранта. Магістерська робота є самостійним завершеним дослідженням. Наукові положення, розробки, результати, висновки і рекомендації, одержані автором самостійно.

Апробація результатів дослідження. Результати дослідження були представлені у вигляді тез доповіді міжнародної науково-практичної конференції Ольвійський форум – 2019: стратегії країн Причорноморського регіону в геополітичному просторі (Миколаїв, 2019).

Структура роботи зумовлена її метою, та завданням і складається зі вступу, трьох розділів, що мають шість підрозділів, висновків та списку використаних джерел (89 найменувань). Загальний обсяг роботи становить 91 сторінку, з яких 80 основного тексту.

ОСНОВНИЙ ЗМІСТ МАГІСТЕРСЬКОЇ РОБОТИ

У **Вступі** доведено та обґрунтовано актуальність теми, сформульовано мету та завдання, визначено об'єкт та предмет дослідження, розкрито методологічну основу, окреслено наукову новизну, охарактеризовано практичне та теоретичне значення одержаних результатів, а також наведено результати апробації дослідження та особистий внесок автора.

У **першому розділі** *«Теоретико-методологічні засади дослідження державної політики інформаційної безпеки в Україні»* визначено основні концептуальні засади дослідження та окреслено основний категоріальний апарат, охарактеризовано підходи до визначення поняття «інформаційна безпека». Також охарактеризовано стан наукової розробки та методи дослідження державної політики інформаційної безпеки.

У підрозділі 1.1. *«Поняття інформаційної безпеки та методи її забезпечення»* розкрито основні теоретичні аспекти дефініції поняття «інформаційна безпека» та специфіку його використання.

В сучасному світі розвитку інформаційних технологій та комунікацій постає питання безпекового фактора, оскільки все більше інформація в сучасному постіндустріальному суспільстві стає реальною зброєю, новим джерелом національної могутності та відіграє

значущу роль у розвитку суспільства. Відповідно, якщо в традиційному суспільстві основна увага зосереджена на факторі сили, в індустріальному – на фінансових ресурсах, то сучасне постіндустріальне суспільство організовано навколо інформаційних потоків, де значну роль відіграють засоби масової інформації. Становлення інформаційного суспільства та розвиток інформаційних технологій докорінно змінює геополітичну ситуацію в світі, впливає на формування нових сфер життєдіяльності суспільства та на формування державної політики в сфері національної безпеки. До важливих компонентів інформаційної безпеки належить система технічних та інформаційних засобів комунікацій, нормативно-правова основа здійснення політики забезпечення інформаційної безпеки, комп'ютерна грамотність населення та швидкість реагування на загрози та небезпеки з боку держави. Взаємодія вказаних елементів виявляє ступінь ефективності державної політики в інформаційній та безпековій сфері.

Відсутність єдиних норм для визначення поняття інформаційної безпеки свідчить про складну та багатокомпонентну структуру державної політики. Більшість науковців сходяться на думці про актуальність даної тематики та важливість її вивчення для впровадження її результатів в державну політику національної безпеки. Швидкий розвиток інформаційної галузі сприяє виникненню нових небезпек, подолання яких напряму залежить від результатів наукових досліджень та їх застосування в державній політиці України. Вивчення досліджень зарубіжних науковців та досвіду іноземних країн в питаннях забезпечення інформаційної безпеки, співпраця зі світовими організаціями сприятиме більш ефективному розвитку галузі та вирішенню проблем забезпечення інформаційної безпеки України.

У підрозділі 1.2. *«Стан наукової розробки та методи дослідження державної політики інформаційної безпеки»* окреслено основні напрямки дослідження проблеми забезпечення системи інформаційної безпеки України. Обґрунтовано методологічний базис дослідження.

Основні теми, які розглядаються в багатьох монографічних дослідженнях вітчизняних науковців, стосуються питань інформаційного суспільства, національної та глобальної інформаційної безпеки, інформаційних війн, міжнародних інформаційних відносин тощо. Проблема захисту від нових видів загроз та небезпек, породжених інформатизацією, хвилює багатьох вчених сучасного суспільства. Серед найвідоміших з них дослідження О. Білоруса, О. Бойченка, І. Валюшко, О. Гиркіної, В. Горбуліна, Р. Калюжного, Б. Кормича, В. Ліпкана, Ю. Лісовської, О. Марченко, Н. Нижника, О. Олійника, В. Семенова, О. Тихомирова, Т. Ткачука, В. Цимбалюка та багато інших.

Основним завданням політики забезпечення інформаційної безпеки України є захист національних інформаційних ресурсів для використання їх окремими громадянами та

суспільством. Створення умов для зберігання, захисту, передачі, доступу до інформації, а також використання національного інформаційного продукту дозволяють забезпечити захист національних інтересів України.

Загалом, використання інноваційних технологій в будь-якій сфері, пов'язаний із застосуванням інформації вимагає швидкого реагування, тому державні органи та недержавні організації мають спиратись на вже існуючі результати досліджень та виступати ініціаторами для подальшої наукової розробки в галузі забезпечення інформаційної безпеки для проведення ефективної державної політики України.

Другий розділ *«Основні механізми державної політики України щодо реалізації інформаційної безпеки України»* присвячено вивченню особливостей формування нормативно-правової бази та концептуальних положень державної політики України в сфері інформаційної безпеки.

У підрозділі 2.1. *«Організаційно-правові механізми державної політики інформаційної безпеки України»* було охарактеризовано основні етапи розвитку нормативно-правової основи інформаційної політики та визначено концептуальні положення системи забезпечення інформаційної безпеки України.

Основні положення державної політики України в сфері інформаційної безпеки знайшли своє відображення в Концепції інформаційної безпеки України, яка була створена в 2015 році Експертною радою при Міністерстві інформаційної політики України. Головною метою Концепції визначалось вирішення нагальних питань в галузі національної безпеки та створення комфортних умов забезпечення інформаційної безпеки.

Вперше визначено та законодавчо закріплено поняття «інформаційний суверенітет України», наголошено на необхідності формування власної інформаційної інфраструктури. Концепція стала теоретичною основою для подальших законодавчих актів у цій сфері.

У ході проведеного дослідження зроблені висновки, що нормативно-правова база щодо забезпечення інформаційної безпеки України залишається недосконалою, деякі положення є суто теоретичними та декларативними, і на практиці не втілюються у життя. При подальшій розробці законодавчої бази з цих питань, вкрай важливим залишається баланс між демократією і безпекою. Отже, важливим завданням залишається організація нормативно-правового механізму державної політики інформаційної безпеки таким чином, щоб не допустити створення монопольного органу державної влади, що виконує контроль у сфері інформаційної безпеки.

У підрозділі 2.2. *«Доктрина інформаційної безпеки України»* було розкрито важливість прийняття Доктрини під час загострення україно-російських відносин. Головною метою впровадження Доктрини був захист українського суспільства від агресивного

інформаційного впливу Російської Федерації. Прописаний ряд заходів щодо зменшення агітаційного інформаційного продукту в медіа та кіберпросторі України. Наголошено на необхідності розвитку власного конкурентоспроможного інформаційного продукту. Отже, залишається питання подальшого реформування та удосконалення нормативної бази, необхідність пошуку нових механізмів для боротьби з пропагандою та законодавчого її закріплення.

Третій розділ *«Інформаційна безпека як складова національної безпеки України»* розкриває особливості співвідношення інформаційної та національної політики, залежність політики національної безпеки від інформаційних ризиків.

У підрозділі 3.1. *«Сучасні виклики та загрози інформаційній безпеці України»* визначено основні інформаційні виклики та небезпеки для країн в інформаційній сфері.

Серед актуальних з них для інформаційної безпеки України є інформаційні правопорушення, інформаційні війни та інформаційний тероризм. Саме вони становлять загрозу в інформаційній сфері для всіх країн світу. Більшість з них це протиправні дії, які виконуються за межами держави, але направлені безпосередньо для агресії всередину країни.

Але не слід забувати про існування внутрішніх викликів. Серед актуальніших з них для України є: критичний, відсталий стан в деяких державних галузях промисловості; несприятлива криміногенна ситуація; корумпованість державних органів та службовців; слабкий розвиток інститутів громадянського суспільства; недостатня координація діяльності публічних органів з формування і реалізації єдиної стратегії щодо державної політики в галузі забезпечення інформаційної безпеки України; слабе інформування суспільства про діяльність органів державної влади про надавання послуг; недостатня кількість кваліфікованих кадрів у галузі забезпечення інформаційної безпеки та низький технологічний рівень освіти громадян. Все це впливає на розвиток інформаційного потенціалу України та призводить до відставання від провідних країн світу за рівнем інформатизації.

У підрозділі 3.2. *«Напрямки державної політики щодо удосконалення інформаційної безпеки України як основи національної безпеки»* розкриваються особливості та перспективи державної політики щодо захисту інформаційних інтересів громадянина, суспільства і держави.

Захист інтересів громадянина, суспільства і всієї держави є головним завданням та найважливішою функцією політики національної безпеки України. За допомогою державних органів та позадержавного сегменту на основі нормативно-правової бази, наукових досліджень та світового досвіду відбувається розвиток нації, збереження та примноження її

духовних та матеріальних цінностей. Інформаційна безпека розглядається як важливий елемент національної безпеки, яка за допомогою роботи з інформацією втілює в життя функції держави. Основним завданням державної інформаційної політики України є виявлення, попередження та боротьба з різними видами загроз та небезпек, які можуть нанести шкоду національним інтересам України.

Зважаючи на високі темпи розвитку інформаційних технологій, появою кваліфікованих фахівців, глобальним процесом інформатизації та прогресі у сфері розвитку інформаційних технологій, серед потенційних загроз для національних інтересів будь-якої країни, в тому числі і України, з'являються такі як інформаційна війна, інформаційний тероризм та інформаційні злочини. Методи їх дій постійно зростають та урізноманітнюються. Інформаційні атаки в медіа- та кіберпросторі стають звичайним явищем.

ВИСНОВКИ

Дослідивши особливості проведення державної політики інформаційної безпеки України та спираючись на поставлені завдання можна зробити наступні висновки.

1. В науковій літературі та нормативних документах відсутні єдині критерії для визначення поняття інформаційна безпека. Це свідчить про складний та багатокomпонентний елемент даного поняття. Завдяки тому, що забезпечення інформаційної безпеки є актуальним у системі національної безпеки як однієї окремо взятої країни так і світу, в цілому, дослідженням цього питання займається ряд як вітчизняних так і закордонних дослідників та спеціалістів, а також велика кількість державних і недержавних наукових установ, дослідницьких та аналітичних центрів. Не зважаючи на різні підходи та визначення, більшість з них погоджуються з думкою, що інформаційна безпека – це особливий вид суспільних відносин, своєрідна взаємодія між суспільством і державою, стосовно створення, збереження, підтримки, охорони та захисту безпечних умов життєдіяльності для громадянина, суспільства та держави за допомогою інформації.

До важливих компонентів інформаційної безпеки належить система технічних та інформаційних засобів комунікацій, нормативно-правова основа здійснення політики забезпечення інформаційної безпеки, комп'ютерна грамотність населення та швидкість реагування на загрози та небезпеки з боку держави. Взаємодія вказаних елементів виявляє ступінь ефективності державної політики в інформаційній та безпековій сфері.

Основним завданням політики забезпечення інформаційної безпеки України є захист національних інформаційних ресурсів для використання їх окремими громадянами та

суспільством. Створення умов для зберігання, захисту, передачі, доступу до інформації, а також використання національного інформаційного продукту дозволяють забезпечити захист національних інтересів України.

Проаналізувавши стан наукових розробок, стає зрозуміло, що існує необхідність подальшого наукового дослідження проблем та перспектив в галузі інформаційної безпеки, що обґрунтовується високою динамікою розвитку міжнародних відносин та стрімким розвитком інформаційно-телекомунікаційних систем і технологій. Використання інновацій в будь-якій сфері, пов'язаній із застосуванням інформації вимагає швидкого реагування. Тому державні органи та недержавні організації мають спиратись на вже існуючі результати досліджень та виступати ініціаторами для подальшої наукової розробки в галузі забезпечення інформаційної безпеки для проведення ефективної державної політики України.

2. На сьогоднішній день, система інформаційного захисту України забезпечується великою кількістю нормативних документів, в яких визначені та утверджені інформаційний суверенітет України, основні національні інтереси, напрямки та пріоритети забезпечення інформаційної безпеки держави, особи і суспільства.

Основні положення державної політики України в сфері інформаційної безпеки знайшли своє відображення в Концепції інформаційної безпеки України, яка була створена в 2015 році Експертною радою при Міністерстві інформаційної політики України. Головною метою Концепції визначалось вирішення нагальних питань в галузі національної безпеки та створення комфортних умов забезпечення інформаційної безпеки. Концепція мала реалізувати вимоги Конституції України і бути визначальним елементом для подальшої розробки нормативно-правової бази у сфері інформаційної безпеки.

Прийняття Доктрини інформаційної безпеки України стало об'єктивним кроком з огляду на загострення україно-російських відносин, виникненню нових актуальних загроз національній безпеці. Цей документ мав визначати нові підходи до формування системи захисту та розвитку інформаційного простору в умовах гібридної війни. Однак, по своїй суті Доктрина стала декларативним документом, яка не вирішила глобальні питання захисту інформаційного простору.

На теперішній час існує безліч законів, які регулюють питання інформаційної безпеки, але їх перелік все одно не є досконалим, адже через стрімкий розвиток інформаційних технологій, з'являються нові виклики і загрози для національної безпеки України.

Основним завданням сьогодення залишається баланс між дієвим контролем державних органів та залученням недержавних організацій до системи інформаційної

безпеки України, недопущення порушень свободи слова та максимальний розвиток власного українського інформаційного продукту.

3. Серед найпоширеніших загроз та викликів для інформаційної безпеки України є інформаційні правопорушення, інформаційні війни та інформаційний тероризм. Саме вони становлять загрозу в інформаційній сфері для всіх країн світу. Більшість з них це протиправні дії, які виконуються за межами держави, але направлені безпосередньо для агресії всередину країни.

Різноманітність способів і методів використання інформації з метою дестабілізації ситуації в економічній, політичній, соціальній та культурній сферах становлять низку викликів в інформаційній сфері, а отже і сфері національної безпеки будь-якої країни. З розвитком інформаційних технологій та технічного процесу, масштабної комп'ютеризації та зростанням досвіду фахівців, з'являються нові форми інформаційних правопорушень. Завданням держави, за допомогою її політичної системи, системи державних органів та нормативно-правової бази ретельно стежити, виявляти, запобігати таким небезпекам для збереження власних національних інтересів.

4. За останні роки Україна декілька раз стикалась з інформаційними злочинами, що чітко вказувало на слабкі сторони в попередженні та боротьбі з ними. Недосконалість українського законодавства, відсутність розвиненої та захищеної інформаційної інфраструктури, слабкий розвиток національного інформаційного продукту та неналежне фінансування роблять систему забезпечення інформаційної безпеки недосконалою.

Отже, основними напрямками удосконалення інформаційної політики залишається подальша розробка та впровадження нормативно-правової бази, залучення світового досвіду, контроль над реальними та потенційними загрозами в галузі інформаційної безпеки, забезпечення ефективної діяльності органів публічної влади з інформування населення, освітня діяльність.

5. Для удосконалення політики інформаційної безпеки України як основи національної безпеки необхідно вжити наступні заходи:

- виявляти та попереджати різні види загроз та небезпек, які можуть нанести шкоду національним інтересам України, шляхом постійних науково-теоретичних досліджень та розробок;
- моніторинг світового правового поля з метою адаптації закордонних надбань до українського законодавства у сфері інформаційної безпеки;
- співпраця та обмін досвідом із організаціями, рішення яких відіграють важливу роль у формуванні системи забезпечення інформаційної безпеки як регіонального так і світового масштабу, для забезпечення власного інформаційного суверенітету;

- розвиток національного інформаційного продукту, належне його фінансування та підтримка;
- стежити за балансом між демократією і безпекою: не допускати порушення принципу свободи слова, використання жорсткої цензури.

Загалом, питання забезпечення системи інформаційної безпеки України є складним і багатокомпонентним. Тому для проведення ефективної державної політики у цьому напрямку вважаю необхідним проводити постійний контроль за розвитком інформаційних технологій та моніторинг за появами нових викликів для національної безпеки, контролювати здатність державних органів до швидкої адаптації в кризових ситуаціях та здатність їх вирішувати.

Подальша робота саме в цих напрямках допоможе забезпечити інформаційний суверенітет країни та стабільність в політиці національної безпеки України.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ

Петрова Т. Сучасні виклики та загрози інформаційній безпеці України / Лушагіна Т., Петрова Т. // Ольвійський форум – 2019: стратегії країн Причорноморського регіону в геополітичному просторі : матеріали міжнародної науково-практичної конференції. – Миколаїв : Вид-во ЧНУ ім. П.Могили, 2019.

АНОТАЦІЯ

Магістерську роботу присвячено дослідженню ефективності проведення державної політики інформаційної безпеки України на сучасному етапі. У вступі обґрунтовано актуальність і рівень розробленості обраної теми; визначено мету й основні завдання, об'єкт, предмет та методи дослідження; описано наукову новизну; встановлено практичне значення одержаних результатів магістерської роботи; зазначено структуру та обсяги роботи. На початку роботи розглянуто теоретико-методологічні засади дослідження державної політики інформаційної безпеки України. З'ясовано, що відсутні єдині критерії для визначення поняття інформаційна безпека у зв'язку із багатовекторністю та складністю цього поняття. Наведено різні погляди науковців на визначення поняття «інформаційна безпека», що свідчить про різноманітність поглядів та підходів щодо розуміння цієї категорії.

Основна частина роботи присвячена аналізу організаційно-правових механізмів державної політики інформаційної безпеки України. Розглянуті нормативно-правові документи, які регулюють вирішення питань інформаційної безпеки. Виявлено цілий ряд проблем, які залишаються поза увагою закону. Сформульовані основні види ризиків та

викликів, які торкаються інтересів національної безпеки України, запропоновані шляхи їх вирішення та контролю.

Зроблено висновок, що для проведення ефективної державної політики у напрямку інформаційної безпеки, необхідний постійний контроль за розвитком інформаційних технологій та моніторинг за появами нових викликів для національної безпеки, здатність державних органів до швидкої адаптації в кризових ситуаціях та здатність їх вирішити. Створення власного інформаційного продукту зміцнить позиції України у світовому інформаційному просторі.

Ключові слова: інформаційна безпека, національний інформаційний продукт, виклики та небезпеки національній безпеці України.

SUMMARY

The master's thesis is devoted to the research of the effectiveness of the state policy of information security of Ukraine at the present stage. The introduction substantiates the relevance and level of elaboration of the chosen theme; the purpose and main tasks, object, subject and methods of research are determined; described the scientific novelty; the practical value of the obtained results of master's work is established; The structure and scope of work are indicated. At the beginning of the paper the theoretical and methodological principles of the study of state policy of information security of Ukraine are considered. It is revealed that there are no common criteria for defining the concept of information security in connection with the multi-vectority and complexity of this concept. Different views of scientists on the definition of "information security" are presented, indicating a variety of views and approaches to understanding this category.

The main part of the work is devoted to the analysis of organizational and legal mechanisms of state policy of information security of Ukraine. The normative and legal documents regulating the decision of issues of information security are considered. A number of problems have been identified that are left out of the law. The main types of risks and challenges that affect the interests of Ukraine's national security are formulated, solutions for and control are proposed.

It is concluded that effective state policy in the direction of information security requires constant monitoring of the development of information technologies and monitoring of the emergence of new challenges for national security, the ability of state authorities to quickly adapt in crisis situations and the ability to solve them. Creation of own information product will strengthen the position of Ukraine in the world of information space.

Key words: information security, national information product, challenges and threats to the national security of Ukraine.