МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ
ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

«До захисту допущено»
Завідувач кафедри УІКБ
_____ С.В.Легомінова
(підпис)
“___”_____20__ р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

на тему: **«НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ»**

Студент групи УБЗМ-71 Бородін Ростислав Русланович _____
(підпис)

Науковий керівник: к.е.н., доцент Мордас Ірина Василівна _____
(підпис)

Нормоконтроль: к.в.н., доц. Якименко Юрій Михайлович _____
(підпис)

Київ – 2020

Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою

«Затверджую»
Завідувач кафедри УІКБ
_____ С.В.Легомінова
(підпис)
“___”_____20__ р.

ЗАВДАННЯ
на магістерську атестаційну роботу
студенту Бородіну Ростиславу Руслановичу

1. Тема роботи: «НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ» затверджена наказом ректора від «___» _____ 20__ р. № __.

2. Термін здачі студентом оформленої роботи: «___» _____ 20__ р.

3. Об’єкт дослідження: інформаційна безпека держави.

4. Предмет дослідження: нормативно-правове забезпечення інформаційної безпеки держави.

5. Мета дослідження: розробка пропозицій щодо покращення системи нормативно-правового забезпечення інформаційної безпеки держави.

6. Перелік питань, які мають бути розроблені:
1. Теоретичні засади забезпечення інформаційної безпеки держави.
2. Нормативно-правова основа забезпечення інформаційної безпеки України.
3. Пропозиції щодо покращення державної політики та нормативно-правового забезпечення у сфері інформаційної безпеки держави.

7. Дата видачі завдання: «___» _____ 20__ р.

Науковий керівник: Мордас І. В.

Завдання прийнято до виконання: Бородін Р. Р.

Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою

КАЛЕНДАРНИЙ ПЛАН

виконання магістерської атестаційної роботи
студентом Бородіним Ростиславом Руслановичем

Дата видачі завдання: «__» _____ 20__ р.

№ з/п	Етапи виконання магістерської атестаційної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	11.03.2020	
2.	Збір та аналіз літератури.	18.03.2020	
3.	Написання 1-го розділу роботи.	01.04.2020	
4.	Написання 2-го розділу роботи.	15.04.2020	
5.	Написання 3-го розділу роботи.	29.04.2020	
6.	Формулювання висновків за результатами проведеного дослідження.	06.05.2020	
7.	Оформлення роботи.	12.05.2020	
8.	Оформлення презентації.	14.05.2020	
9.	Отримання рецензії на роботу.	20.05.2020	
10.	Захист в ДЕК.	__.06.2020	

Студент групи УБЗМ-71 Бородін Ростислав Русланович _____
(підпис)

Науковий керівник: к.е.н., доцент Мордас Ірина Василівна _____
(підпис)

Нормоконтроль: к.в.н., доц. Якименко Юрій Михайлович _____
(підпис)

РЕФЕРАТ

Робота містить вступ, три розділи з підрозділами, висновки та список використаних джерел. Загальний обсяг роботи – 66 сторінок.

Об’єкт дослідження – інформаційна безпека держави.

Предмет дослідження – нормативно-правове забезпечення інформаційної безпеки держави.

Мета дослідження – розробка пропозицій щодо покращення системи нормативно-правового забезпечення інформаційної безпеки держави.

У магістерській атестаційній роботі досліджено теоретичні засади забезпечення інформаційної безпеки держави; проаналізовано нормативно-правову основу забезпечення інформаційної безпеки України; розроблено пропозиції щодо покращення державної політики та нормативно-правового забезпечення у сфері інформаційної безпеки держави.

БЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

ЗМІСТ

ВСТУП

Актуальність теми. На початку третього тисячоліття народилося суспільство нового типу – інформаційне, у якому основними стратегічними ресурсами виступають інформаційні ресурси. Потужний вплив інформаційних процесів, які протікають у світі, на усі сфери життєдіяльності суспільства, посилює та актуалізує найважливіші проблеми соціального життя, у тому числі питання інформаційного обміну й взаємодії, включаючи протидію інформаційним загрозам різноо роду та боротьбу за інформаційний простір загалом.

Інформаційна безпека держави посідає одне із провідних місць серед складових системи забезпечення важливих життєвих інтересів всіх країн й, безумовно, і України. Це зумовлено, передусім, нагальною потребою у створенні розвинутого інформаційного українського середовища суспільства, але найчастіше саме через таке середовище відбуваються загрози національній безпеці всіх країн.

У сучасних умовах вся сформована система забезпечення інформаційної безпеки в Україні, що раніше склалася, уже не спроможна відповідати новим принципам та закономірностям забезпечення інформаційної безпеки й не спроможна ефективно протидіяти виникаючим інформаційним загрозам. Тому сьогодні у сучасний період розвитку в Україні гостро постає питання визначення пріоритетів держави в сфері забезпечення її інформаційної безпеки та зосередження й концентрація зусиль на найважливіших ділянках реальних й потенційних загроз.

Мета і завдання дослідження. Мета роботи – розробка пропозицій щодо покращення системи нормативно-правового забезпечення інформаційної безпеки держави.

Для досягнення цієї мети в роботі необхідно вирішити такі *завдання*:

1. Дослідити теоретичні засади забезпечення інформаційної безпеки держави.

2. Проаналізувати нормативно-правову основу забезпечення інформаційної безпеки України.

3. Розробити пропозиції щодо покращення державної політики та нормативно-правового забезпечення у сфері інформаційної безпеки держави.

Об'єкт дослідження – інформаційна безпека держави.

Предмет дослідження – нормативно-правове забезпечення інформаційної безпеки держави.

Методи дослідження. У роботі були використані загальнонаукові методи пізнання – аналіз, синтез, абстрагування, аналогії, теоретичного узагальнення та ін.

Практичне значення одержаних результатів. Результати роботи можуть бути використані для покращення системи забезпечення інформаційної безпеки держави.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

1.1. Поняття інформаційної безпеки держави

Інформаційна безпека визначається це ступінь захисту систем зберігання і обробки інформаційних данних, за якого зберігається конфіденційність, цілісність і доступність інформації, або комплекс певних заходів, що спрямовані на забезпечення захисту інформації від оприлюднення, використання, руйнування, ознайомлення, внесення змін, запису, перевірки, знищення або несанкціонованого доступу (хоча у цьому значенні використовується частіше поняття захисту інформації) .

Інформаційна безпека держави визначається як ступінь захисту важливих життєвих інтересів, держави, суспільства і людини, за якого відбувається запобігання нанесенню шкоди через: невчасність, невірогідність неповноту інформації, яка використовується; негативні наслідки використання інформаційних технологій; негативний інформаційний вплив; несанкціоноване використання чи розповсюдження інформації; порушення цілісності, доступності або конфіденційності.

З одного боку, термін інформаційної безпеки містить у собі забезпечення вільного доступу людей до різного роду джерел інформації та якісне інформування громадян, а з другого – контроль за нерозповсюдженням таємної інформації, захисту від інформаційних негативних впливів, сприяння цілісності суспільства тощо. Рішення такої комплексної проблеми допоможе як захистити інтереси людей, держави і суспільства, так і сприяти реалізації прав людей на отримання якісної та всебічної інформації.

Стратегічним головним завданням інформаційної безпеки в Україні є створення потужного інформаційного національного простору як головного аспекта присутності держави у інформаційному світовому просторі. Окрім

того, це стратегічне завдання включає формування системи запобігання інформаційним загрозам, а також захист інформаційних ресурсів держави, інформаційної інфраструктури та інформаційного власного простору.

Загалом, задачами забезпечення інформаційної безпеки держави сьогодні можна вважати таке:

– виявлення, прогнозування та оцінка поведінки існуючих джерел загроз й ризиків інформаційній безпеці, які здійснюються через оперативний моніторинг інформаційної обстановки в державі;

– формування та експлуатація систем забезпечення інформаційної безпеки;

– вироблення, введення та координація єдиної державної політики в забезпечення інформаційної безпеки;

– розробка, запровадження та координація єдиної державної політики в забезпеченні інформаційних міжнародних відносин, зокрема в напрямку створення іміджу держави.

Згідно з українським законодавством, забезпечуючи ІБ держави, вирішення проблем інформаційної безпеки варто здійснювати шляхом:

– формування інформаційної повнофункціональної інфраструктури держави та системи забезпечення захищенності її критичних елементів;

– удосконалення нормативно-правової основи стосовно забезпечення інформаційної безпеки, а саме захисту інформаційних ресурсів, захисту персональних даних, протидії комп'ютерній злочинності, а також стосовно правоохоронної діяльності у інформаційній сфері;

– підвищення рівня координування діяльності державних органів стосовно виявлення, прогнозування і оцінки загроз і ризиків інформаційній безпеці, протидія таким загрозам, забезпечення ліквідації наслідків загроз і ризиків, здійснення міжнародного співробітництва стосовно цих питань;

– розвитку і розгортання Національної системи конфіденційного зв’язку у напрямі сучасної захищеної транспортної платформи, що здатна

здійснювати інтегрування територіально розподілених інформаційних систем, у яких оброблюється конфіденційна інформація [5].

Інформаційна безпека кожної держави характеризується станом захисту й, отже, стійкістю усіх основних сфер життєдіяльності (техносфери, економіки, науки, сфери управління, суспільної свідомості, військової справи і т. ін.) по відношенню до загрозливих небезпечних (деструктивних, дестабілізуючих, суперечуючим інтересам держави тощо) інформаційних впливів, причому і як до вилучення, і до впровадження інформації.

Проблеми ефективного забезпечення безпеки інформації у кожній державі повинні передбачати вирішення таких масштабних завдань як:

– створення системи органів, що відповідатимуть за безпеку та захист інформації;

– розробка теоретичних основ забезпечення безпеки та захисту інформації;

– вирішення проблем керування захистом й безпекою інформації й її автоматизацією;

– створення нормативно-правової основи, що регламентувала б вирішення усіх задач забезпечення захисту й безпеки інформації;

– організація підготовки відповідних фахівців, налагодження виробництв засобів захисту інформації і т. ін.

В комплекс питань стосовно інформаційної безпеки кожної держави включені такі сфери діяльності держави як:

– захист інформаційної інфраструктури країни;

– захист й безпека обігу інформації;

– захист інформаційного національного ринку;

– безпека функціонування інформаційної сфери країни;

– попередження інформаційних війн й інформаційного тероризму.

Так, система інформаційної безпеки кожної держави є невід’ємною частиною всієї системи безпеки кожної держави світу. А проблеми інформаційної безпеки обумовлені специфікою сьогоднішнього етапу

функціонування науково-технічного прогресу у світі, інформатизацією і глобалізацією загалом. Проте вирішення цих надто важливих проблем потребує грунтовного й ефективного нормативно-правового забезпечення та підготовленої теоретичної бази, що на даний момент не є досконалими. Відсутність єдиних підходів до розуміння понять та чітко визначеної термінології в цілому гальмують вирішення проблемних задач у цій галузі й вимагають суттєвого доопрацювання.

1.2. Структура управління інформаційною безпекою держави

Виокремимо два аспекти аналізу інформаційної безпеки у контексті всієї національної безпеки. З однієї сторони, це є самостійнии складовим елементом національної безпеки країн, а з іншої – інтегрована складова частина будь-якого іншого виду безпеки: економічної, політичної, військової та ін.

Серед головних складових елементів інформаційної безпеки держав виокремлюють [3]: обсяг інформаційних послуг і продуктів, що виробляються у державі й державою; можливість держави здійснювати керування розвитком вироблення й розповсюдженням інформації; здатність існуючих мереж витримати постійно зростаюче інформаційне навантаження; можливість доступу населення держави до всіх існуючих інформаційних джерел та відкритість й доступність більшості із них.

Здійснивши аналіз праць вітчизняних дослідників, головні цілі політики щодо інформаційної безпеки країн можна сформулювати наступним чином [4, с. 129]: реалізація конституційного права на інформацію з боку держави, громадян та суспільства; захищеність інформаційного суверенітету країни, зокрема, інформаційного національного ресурсу й систем формування свідомості суспільства; забезпечення певного рівня достатності інформації для прийняття необхідних рішень громадянами, державними

підприємствам й установами; належна присутність країни в інформаційному просторі світу.

Оскільки інформаційний національний ресурс став сьогодні одним із головних джерел для економічної потужності держави й її суб'єктів господарювання, то необхідним буде визначити державні інтереси, загрози і фактори у інформаційній сфері; аналіз ефективності наявної системи безпеки й можливих шляхів її вдосконалення.

Отже, вирішення найважливіших проблем інформаційної безпеки держав повинно відбуватися на основі політики держави, при цьому, у відповідності до вищеназваних положень й принципів забезпечення інформаційної безпеки держав, потрібне сьогодні вирішення нижчеперерахованих ключових проблем:

– формування нормативно-правової (законодавчої) бази забезпечення інформаційної безпеки держав, в тому числі, розробка реєстрів інформаційних національних ресурсів, регламентів інформаційного обміну для державних органів влади та державних підприємств, юридичного закріплення відповідальності громадян й посадових осіб за недодержання вимог інформаційної безпеки;

– створення механізмів реалізації права громадян на інформацію в державі;

– розвиток наукових та практичних засад інформаційної безпеки держав, що відповідають геополітичній ситуації сучасного світу й умовам політичного, соціально та економічного розвитку держав;

– формування систем інформаційної безпеки, які є складовими частинами загальних систем національної безпеки країн;

– розробка сучасних технічних засобів й методів, які забезпечують комплексність рішення задач щодо захисту інформації;

– створення критеріїв й методів оцінки ефективності наявних систем й засобів інформаційної безпеки та їхня сертифікація при необхідності;

– дослідження способів й форм цивілізованого впливу держав на формування свідомості суспільства;

– комплексне дослідження роботи персоналу інформаційних систем, в тому числі способів і методів підвищення їхньої мотивації, психологічно-моральної стійкості й соціальної захищеності працівників, що мають справу із конфіденційними або секретними видами інформації.

На загальнонаціональному рівні інформаційну безпеку держав розглядають як систему заходів, що спрямовані на недопущення несанкціонованого доступу будь-кого до інформації, порушення її цілісності та її модифікації. Вона включає:

- захист громадських, політичних й державних інтересів;

- заборона тих видів інформації, що містять ідеї дискримінації, насилля, посягання на права людей або агресії війни;

- захист моральних цінностей людей.

Інформаційний простір розуміється як певне середовище, в якому проходить формування, збереження, опрацювання, поширення й збирання інформації, та на яке поширюється юрисдикція тих чи інших держав. Треба наголосити і на тому, що інформаційні технології будь-якого виду складаються із наступних елементів: виробництво інформації, зберігання інформації, обробка інформації та її споживання. З врахуванням без пекового моменту, необхідно забезпечити також і надійність роботи усіх складових елементів цієї системи. Досліджуючи проблему у такому ракурсі, слід окреслити і головну мету інформаційної діяльності – формування відкритого повноцінного інформаційного простору.

Важливим елементом інформаційного простору країни є засоби масової інформації. Важливими чинниками для даного сектору інформаційного простору є законодавче забезпечення їхньої діяльності, умови їхнього функціонування в країні та стан захищеності журналістів. У країнах, які розвиваються, ЗМІ відіграють ключову роль для усього суспільства, адже вони дозволяють, за відсутності законодавчих засобів й методів стримування,

маніпулювати думкою суспільства та надавати не завжди коректну інформацію. А це є суттєвим порушенням стану інформаційної національної безпеки. В системі національної безпеки держав дедалі більше значення набуває інформація, що заповнює вільний час людей та формує настрій всієї нації. Саме такою інформацією й забезпечують ЗМІ суспільство разом з іншими системами формування масової свідомості в державі.

Ще більше значення набуває і довгостроковий вплив ЗМІ, що є одним із основних джерел для формування систем соціально-політичних стереотипів й настанов. Відсутність певних відомостей, їх переважно чи виключно негативний характер в сьогоднішньому світі впливає на зовнішню економічну й політичну діяльностя як держав у цілому, так й на окремих їх громадян та їхні організації. Саме тому, ця проблема має сьогодні загальнонаціональне значення, а у випадку нехтування її створює загрозу національній безпеці держав. Саме тому, формування потрібних умов для розширення інформаційної присутності держав в інформаційному просторі світу є найважливішим завданням політики інформаційної безпеки держави.

Одним з основних складових елементів реалізації політики держави у інформаційній сфері є нині інформаційна інфраструктура, яка є невід'ємною частиною інформаційних стратегічних ресурсів й має ключове значення для забезпечення обороноздатності держави та інформаційного ринку держави.

Під інформаційною інфраструктурою пропонуємо розуміти єдність наступних компонентів: система виробництва інформаційних послуг і продуктів, система доставки їх до споживача, система виробництва засобів виробництва інформаційних послуг і продуктів й їх доставки, система виробництва інформаційних технологій, система накопичення й збереження інформаційних послуг і продуктів (або інформаційного ресурсу), тобто системи сервісу та обслуговування елементів інфраструктури, а також системи підготовки відповідних кадрів.

Процес удосконалення суспільних відносин суттєвою мірою залежить від розвитку інформаційних національних ресурсів, що є основними для

формування ефективних моделей у системах державного управління. Отже, такий вид ресурсів водночас є предметом діяльності системи державної влади й її інститутів та об’єктом управління.

Інформаційні ресурси являють собою інформаційну інфраструктуру та циркулюючу у ній продукцію інформаційної діяльності, що дає змогу вирішити відповідні завдання [9]. При цьому, найважливішим є розуміння того, що обидві складові інформаційних ресурсів одна одну доповнюють й не можуть окремо бути використані. Темпи економічного й науково-технічного розвитку країн багато в чому можна визначити такими факторами як якість й доступність інформаційного забезпечення країн. А рівень забезпеченості інформацією також визначає успіх суспільства, держави і громадян у цілому. Важлива проблема, що виникає, це – налагодження процесів збирання, ефективного використання й аналізу науково-технічної інформації іншомовного походження, а доступ до неї є однією із критичних умов забезпечення будь-якого прогресу. Ключове значення у сучасних умовах надається і інформаційному забезпеченню політичної діяльності в державах.

Перша складова системи покликана забезпити оперативне керівництво в державах, інтереси другої складової зосереджені на оперативному рівні управління, а третя складова здійснює стратегічне планування зовнішньої політичної діяльності. При дослідженні проблем інформаційної безпеки в державах важливим кроком є виокремлення загроз інформаційній безпеці й також аналіз технологій захисту від цих загроз.

Під загрозами інформаційній безпеці розуміються явища, дії негативних факторів або процесів, через які об’єкти інформаційної безпеки держав частково чи повністю втрачають можливості реалізації своїх інтересів у інформаційній сфері держав; а також відбувається порушення нормального функціонування, відбувається руйнація чи стримується розвиток технічних (технологічних) об’єктів інформаційної безпеки держав. Як правило, виокремлюють такі типи інформаційних загроз: суспільні, політичні, економічні, військові й науково-технічні [1, с. 106].

У суспільній сфері це:

– системи ЗМК;

– загрози для систем формування громадської думки;

– структури політичних партій, релігійних організацій, громадських рухів;

– структури забезпечення основних свобод і прав людей.

У політичній сфері це:

– телекомунікаційні системи спеціального призначення;

– виборчі системи;

– системи державного управління;

– системи підготовки для прийняття політичних рішень.

В економічній сфері це:

– банківська інфраструктура;

– системи прийняття рішень;

– управління економічним становищем в умовах надзвичайних ситуацій;

– промисловий шпіонаж й корпоративні війни;

– управління державними комунікаціями, що мають економічний характер.

В військовій сфері:

– системи управління військами;

– інформаційні ресурси збройних сил країн;

– системи постійного спостереження й контролю;

– канали надходження інформації розвідувального, оперативного й стратегічного характеру.

У науково-технічній сфері:

– об’єкти інтелектуальної власності;

– системи накопичення ноу-хау;

– структури прикладних й фундаментальних;

– структури прогнозування й аналізу тенденцій в даній сфері;

– банки й бази даних конфіденційного характеру.

Українські експерти [10] як правило, загрози інформаційній безпеці України за своєю загальною спрямованістю, поділяють на такі види:

– загрози конституційним правам і свободам людини і громадянина у сфері духовного життя й інформаційної діяльності, індивідуальній, груповій і суспільній свідомості, духовному відродженню України;

– загрози інформаційному забезпеченню державної політики України;

– загрози розвиткові вітчизняної індустрії інформації, включаючи індустрію засобів інформатизації, телекомунікацій і зв'язку;

– загрози безпеці інформаційно-телекомунікаційних систем на території України, як діючих, так і тих, що створюються. Серед загроз інформаційному забезпеченню державної політики України виділяють наступні: монополізація інформаційного ринку України, його окремих секторів вітчизняними і закордонними інформаційними структурами;

– блокування діяльності державних засобів масової інформації з інформування української і закордонної аудиторій;

– низька ефективність інформаційного забезпечення державної політики України внаслідок дефіциту кваліфікованих кадрів, відсутність системи формування і реалізації державної інформаційної політики.

Загрозами для безпеки інформаційно-телекомунікаційних систем на території України, як діючих, так і тих, що створюються, можуть бути:

– протиправні збирання та використання інформації;

– порушення технології обробки інформації;

– впровадження в апаратні і програмні вироби компонентів, що реалізують функції, не передбачені документацією на ці вироби;

– розробка і поширення програм, що порушують нормальне функціонування інформаційно-телекомунікаційних систем, зокрема систем захисту інформації;

– знищення, пошкодження, радіоелектронне придушення або руйнування засобів і систем обробки інформації, телекомунікацій і зв'язку;

– вплив на парольно-ключові системи захисту автоматизованих систем обробки і передачі інформації;

– компрометація ключів і засобів криптографічного захисту інформації; витік інформації по технічних каналах;

– впровадження електронних пристроїв для перехоплення інформації в технічні засоби обробки, збереження та передачі інформації, а також у службові приміщення органів державної влади, підприємств, установ і організацій незалежно від форми власності;

– знищення, пошкодження, руйнування або розкрадання машинних та інших носіїв інформації;

– перехоплення інформації в мережах передачі даних і на лініях зв'язку, дешифрування цієї інформації і нав'язування помилкової інформації;

– використання несертифікованих вітчизняних і закордонних інформаційних технологій, засобів захисту інформації, засобів інформатизації, телекомунікації і зв'язку під час створення й розвитку української інформаційної інфраструктури;

– несанкціонований доступ до інформації, що знаходиться в банках і базах даних; порушення законних обмежень на поширення інформації [10].

Розглядаючи проблему інформаційних загроз неможливо обминути поняття джерел загроз інформаційній безпеці. Експерти розрізняють внутрішні та зовнішні джерела загроз [13, с. 211].

Під внутрішніми джерелами розуміють відсутність історичного, політичного та соціального досвіду життя у правовій державі, що торкається процесу практичної реалізації конституційних прав та свобод громадян, в тому числі в інформаційній сфері, а також посилення організованої злочинності та збільшення кількості комп'ютерних злочинів, зниження рівня освіченості громадян, що суттєво ускладнює підготовку трудових ресурсів для використання новітніх технологій, в тому числі інформаційних. Недостатню координацію діяльності вищого державного керівництва, органів влади та військових формувань в реалізації єдиної державної політики

забезпечення національної безпеки теж можна вважати таким джерелом. До цього слід додати і відставання України від розвинутих країн за рівнем інформаизації органів державної влади, юридично-фінансової сфери, промисловості та побуту громадян.

До зовнішніх джерел належать діяльність іноземних політичних, військових, економічних та розвідувальних структур в інформаційній сфері; політика домінування деяких країн в інформаційній сфері; діяльність міжнародних терористичних груп; розробка концепцій інформаційних війн будь-якими структурами; культурна експансія у відношенні до конкретної країни. В наш час стало очевидним, що під впливом інформації зростає потенційна вразливість суспільних процесів від інформаційного впливу. Інформація стала чинником, здатним призвести до велико-масштабних аварій, військових конфліктів, дезорганізації державного управління тощо.

Враховуючи цілі та завдання політики інформаційної безпеки України, як правило, виділяють такі основні напрями забезпечення інформаційної безпеки: забезпечення інформаційної достатності для прийняття рішень; захист інформації, тобто захист інформаційного ресурсу; захист та контроль національного інформаційного простору, тобто систем формування масової свідомості; присутність у світовому інформаційному просторі.

Головним завданням заходів із забезпечення інформаційної безпеки є мінімізація шкоди через неповноту, несвоєчасність або недостовірність інформації чи негативного інформаційного впливу через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації [15].

Загалом, основні напрямки діяльності по забезпеченню інформаційної безпеки держави являють собою величезний комплекс заходів, до яких відносяться:

– розвиток науково-практичних основ інформаційної безпеки;

– розвиток законодавчої і нормативно-правової бази забезпечення інформаційної безпеки;

– розробка нормативно-правових і організаційно-методичних документів; розробка концепції інформаційної безпеки, спеціальних правових і організаційних заходів, що забезпечують збереження і розвиток інформаційних ресурсів;

– формування правового статусу суб'єктів системи інформаційної безпеки; розробка законодавчих і нормативних актів, що регулюють порядок ліквідації наслідків загроз інформаційній безпеці;

– відновлення порушеного права і ресурсів, реалізації компенсаційних мір; вдосконалення організації форм і методів запобігання і нейтралізації загроз інформаційній безпеці;

– розвиток сучасних методів забезпечення інформаційної безпеки [6].

Розвиток науково-практичних основ інформаційної безпеки включає в себе:

– розробку стратегії забезпечення інформаційної безпеки країни;

– обґрунтування державної політики в умовах глобалізації інформаційних процесів, формування світових інформаційних мереж, прагнення деяких країн до домінування в розвитку і використанні світового інформаційного простору;

– розробку науковопрактичних основ формування і проведення державної політики в області забезпечення інформаційної безпеки;

– обґрунтування пріоритетів національної безпеки, що відповідають довгостроковим інтересам суспільного розвитку.

Розвиток законодавчої і нормативно-правової бази забезпечення інформаційної безпеки означає визначення порядку розробки законодавчих і нормативно-правових актів, а також механізмів практичної реалізації прийнятого законодавства.

Розробка нормативно-правових і організаційно-методичних документів включає розробку документів, що регламентують:

– діяльність в області інформаційної безпеки органів державної влади;

– взаємини суб'єктів інформаційної діяльності для забезпечення інформаційної безпеки;

– регулювання державою процесів функціонування і розвитку ринку засобів інформації, інформаційних продуктів і послуг;

– інформаційні відносини в суспільстві і державі в умовах ринкової економіки тощо.

Під розвитком сучасних методів забезпечення інформаційної безпеки мається на увазі:

– розробка форм і способів цивілізованого впливу держави на формування суспільної свідомості і практичних рекомендацій з реалізації їх на практиці;

– розробка методів комплексного дослідження діяльності персоналу інформаційних систем, у тому числі методів підвищення мотивації, морально-психологічній стійкості і соціальної захищеності людей, що працюють із секретною і конфіденційною інформацією;

– розробка практичних рекомендацій зі збереження і зміцнення політичної стабільності в суспільстві;

– забезпеченню прав і свобод громадян;

– зміцненню законності і правопорядку методами інформаційної безпеки;

– формування шляхів і способів забезпечення органів державної влади, підприємств і громадян достовірною, повною і своєчасною інформацією;

– розробка основних напрямків діяльності із запобігання негативних інформаційних впливів на індивідуальну, групову і суспільну свідомість;

– розробка цивілізованих, демократичних форм і методів впливу на засоби масової інформації;

– розробка механізмів розвитку інформаційних відносин у сфері підприємництва і включення інформаційного ресурсу у господарські відношення;

– дослідження основних шляхів послаблення криміногенної обстановки, зниження числа комп'ютерних злочинів, у першу чергу у кредитно-фінансовій сфері;

– розробка методів і практичних рекомендацій із контролю над експортом вітчизняних наукомістких технологій; обґрунтування напрямків протидії інформаційній зброї;

– удосконалення способів контролю за персоналом у захищених інформаційних системах.

1.3. Особливості нормативно-правового забезпечення в сфері інформаційної безпеки

В сучасних доробках стосовно проблеми функціонування інститутів суспільства, а також можливостей застосування інституціонального підходу при дослідженні державного управління хочемо виоремити роботи таких науковців як В.В.Цвєтков, О. Оболенський, О. Лазор, В. Дементьєв, О. Бєляєв, Л. Кирилов, І. Кох та ін.

Сам інституціональний підхід зародився у США ще в період початку XX ст. Тоді виник класичний інституціоналізм, що був новим підходом до аналізу економічних явищ й процесів. Основоположником його вважають Т. Веблена, а послідовниками інституціоналізму – Р. Коуза, Дж. Гелбрейта, Д. Норта та ін.

Усі представники вищезазначеного підходу вважали, що сама поведінка економічної людини здійснюється головним чином під впливом соціальних колективів й груп і в певних рамках.

У змісті інститутів Д. Норт виокремлює три головних елементів:

– сукупність формальних правил (норми права, закони, конституції тощо);

– сукупність неформальних обмежень (угоди, домовленості, звичаї, традиції тощо);

– сукупність механізмів примусу, що забезпечують додержання правил (суди, правоохоронні органи тощо).

Аналіз та дослідження законодавства в сфері забезпечення інформаційної безпеки країн дозволяє дійти до висновку про те, що діюче законодавство в сфері забезпечення національної інформаційної безпеки України знаходиться на етапі становлення і формування. На цих етапах дані процеси характеризуються суттєвою кількістю колізій і прогалин. Одним з напрямів виходу із цієї ситуації є, на нашу думку, здійснення систематизації норм адміністративного права (передусім, шляхом його кодифікації). Саме відсутність принципу системності у підходах до кодифікації норм інформаційного законодавства є сьогодні однією із значних проблем реформування українського законодавства в сфері забезпечення національної інформаційної безпеки.

В той самий час, треба зазначити, що створення нових суспільних відносин у інформаційному будь-якому суспільстві передбачає формування відповідного комплексу юридичного забезпечення. Сьогодні у світі проводиться робота над удосконаленням (реформуванням) існуючого законодавства, розробкою нових нормативно-правових (юридичних) актів в сфері регулювання національних інформаційних відносин й забезпечення національної інформаційної безпеки. Усі елементи життя суспільства, що мають зв’язок із забезпеченням національної інформаційної безпеки, мають бути достатньо унормовані й урегульовані законодавством (чітко установленими правилами поведінки).

Отже, інституціоналізація на сьогодні виступає основним соціальним механізмом побудови й функціонування системи національної інформаційної безпеки. Створення інституційного середовища для управління інформаційною безпекою виступає основною стратегією для досягнення стабільності у будь-яких суспільствах. При цьому, слід виокремити той факт, що суспільна інституційна система, обслуговуючи увесь спектр суспільних відносин, є формою реалізації свієї системи інтересів суспільства. Ефективна

інституційна система, що реалізує громадські інтереси, гармонізує та організовує їх в напрямку забезпечення інтересів національних вищого порядку. Завдяки цьому досягається ефективність всього розвитку суспільства й країни, її всебічний й повний (тобто достатній) захист.

Висновки до першого розділу

Термін інформаційної безпеки містить у собі забезпечення вільного доступу людей до різного роду джерел інформації та якісне інформування громадян, а з другого – контроль за нерозповсюдженням таємної інформації, захисту від інформаційних негативних впливів, сприяння цілісності суспільства тощо.

Інформаційна безпека кожної держави характеризується станом захисту й, отже, стійкістю усіх основних сфер життєдіяльності (техносфери, економіки, науки, сфери управління, суспільної свідомості, військової справи і т. ін.) по відношенню до загрозливих небезпечних (деструктивних, дестабілізуючих, суперечуючим інтересам держави тощо) інформаційних впливів, причому і як до вилучення, і до впровадження інформації.

РОЗДІЛ 2. НОРМАТИВНО-ПРАВОВА ОСНОВА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Нормативні акти, які закріплюють концептуальні положення інформаційної безпеки України

Нормативна платформа інформаційної безпеки у першу чергу повинна виконувати такі три основні функції:

1. Нормативне забезпечення дій суб'єктів інформаційної безпеки держав на усіх рівнях, зокрема –суспільства, держави, людини.

2. Регулювання взаємовідносин між суб'єктами інформаційної безпеки держав, визначення їх права, відповідальності та обов'язків.

3. Встановлення порядку застосування різних засобів і сил забезпечення інформаційної безпеки держав.

Найактуальнішим завданням в сфері забезпечення національної інформаційної безпеки держав на сьогодні є створення відповідних положень інформаційного національного законодавства стосовно правового забезпечення діяльності відповідних суб'єктів у інформаційній сфері, в першу чергу державних органів влади, на які покладено державою виконання функцій, пов'язаних з цим.

Протягом років незалежності в Україні було закладено законодавчі основи для створення системи забезпечення національної інформаційної безпеки, було напрацьовано, зокрема, суттєву кількість нормативно-правових актів, що визначають основні повноваження державних органів влади у інформаційній сфері. Документи національного законодавства, що здійснюють регламентацію діяльності державних органів, громадян й організацій у інформаційній сфері, установлюють також і повноваження державних органів влади стосовно забезпечення інформаційної національної безпеки країни.

Виходячи з викладеного, нормативну базу України стосовно забезпечення її національної безпеки у інформаційній сфері слід розглядати із врахуванням існуючої ієрархії нормативно-правових документів.

На найвищому рівні слід розглядати норми Конституції України, в яких закріплюються концептуальні положення національної безпеки у всіх сферах існування України. Документи (найвищого рівня) враховують основні положення міжнародних угод й договорів, які Україна ратифікувала і які стосуються національної безпеки держави.

На другому рівні слід розглядати закони конститутивного напряму, що визначають важливі положення стосовно забезпечення безпеки в національній інформаційній сфері.

На третьому рівні слід розглядати закони інституційного рівня, в яких закріплено основні форми діяльності органів влади у державі в процесі забезпечення безпеки в національній інформаційній й інших сферах життя й діяяльності суспільства, держави та особи.

Значну роль в системі законодавства України стосовно питань національної безпеки грають акти директивного й нормативного характеру органів влади місцевого самоврядування – рішення стосовно питань процесу забезпечення національної безпеки (про підтримку громадського порядку, про боротьбу із наслідками техногенних катастроф і аварій, стихійних лих, із епідеміями, тощо), що є обов’язковими для виконання для всіх установ, організацій й підприємств, а також усіма громадянами й посадовими особами на території, що підпорядкована цьому органові влади.

Суттєвим кроком на шляху формування системи нормативно-правового (юридичного) регулювання процесу забезпечення національної інформаційної безпеки країни стало прийняття Конституції України 28.06.1996 р. Верховною Радою України. У ній є, зокрема, норми, які стосуються забезпечення інформаційної національної безпеки та які є основоположними для побудови системи національної інформаційної безпеки.

Верховна Рада України в січні 1997 р. прийняла “Концепцію (основи державної політики) національної безпеки України”. Концепція нормативно закріпила принципи та загальні положення забезпечення національної безпеки країни, загрози національній безпеці й національні інтереси, ключові напрямки політики національної безпеки держави, систему її забезпечення й перелік повноважень основних суб’єктів цієї системи. Основними принципами її забезпечення Концепція називає верховенство права, пріоритет прав людей й демократичний цивільний контроль над військовою сферою і іншими подібними структурами у всій системі процесу забезпечення національної безпеки.

Разим із іншими ймовірними загрозами національній безпеці в Концепції зазначаються і загрози у інформаційній сфері: витік інформації, яка становить державну й іншу таємницю, передбачену законом, конфіденційної інформації, яка є власністю держави; інформаційна експансія зі сторони інших держав.

Серед основних напрямів здійснення політики національної безпеки держави у інформаційній сфері Концепція визначила:

- вживання комплексу заходів стосовно захисту свого інформаційного середовища та входження України в інформаційний простір світу;

- усунення негативних факторів, які порушують інформаційний простір, унеможливлення інформаційної експансії зі сторони іноземних держав (протидія АІА, СІО й іншим ІПВ деструктивного характеру);

- розробленна й запровадження необхідних режимів і засобів одержання, поширення, зберігання та використання суспільно значущої інформації, формування розвинутої інформаційної національної інфраструктури.

В Доктрині інформаційної безпеки в Україні, що затверджена Президентом України (указ № 514/2009 від 8.07.2009 р.), інформаційна безпека визначається як самостійна сфера для забезпечення національної безпеки країни й одночасно як невід’ємна складова кожної з її складових.

Ключовою метою реалізації Доктрини та її положень задекларовано формування в Україні розвинутого інформаційного національного простору й захист інформаційного національного суверенітету.

Доктрина визначає також і принципи забезпечення інформаційної національної безпеки, життєво важливі інформаційні національні інтереси у контексті інтересів суспільства, держави, особи, а також потенційні та реальні загрози інформаційній безпеці країни: в сфері державної безпеки, у воєнній, внутрішньополітичній, зовнішньополітичній, економічній, соціальній, науково-технологічній, гуманітарній, екологічній та ін. сферах.

У відповідності до положень Доктрини, функціонування органів виконавчої влади в процесі забезпечення інформаційної національної безпеки повинно бути зосереджено на конструктивному й ефективному поєднанні діяльності громадянського суспільства, людини і держави за трьома головними напрямками: інформаційно-психологічному, захисту інформації, технологічного розвитку.

Держава з метою забезпечення інформаційної національної безпеки повинна вживати відповідні заходи у всіх сферах, в яких існують потенційні й реальні загрози: у сфері державної безпеки, у воєнній, внутрішньополітичній, зовнішньополітичній, економічній, соціальній, науково-технологічній, гуманітарній, екологічній та ін. сферах.

Національна безпека країн у інформаційній сфері має забезпечуватися через проведення виваженої політики держави у відповідності до прийнятих встановленому порядку стратегій, доктрин, концепцій й програм в різних сферах: політичній, економічній, воєнній, екологічній, соціальній, соціальній, інформаційній, науково-технологічній та ін.

Вибір конкретних шляхів та засобів для забезпечення інформаційної національної безпеки повинно обумовлюватися необхідністю своєчасно вжитти заходи, що будуть адекватні характеру ій масштабам загроз інформаційним національним інтересам.

Основними напрямками політики держави у інформаційній сфері потрібно визначити такі:

- забезпечення в Україні інформаційного суверенітету;

- удосконалення державного регулювання розвитком інформаційної сфери через створення економічних та юридичних (нормативно-правових) передумов для формування інформаційної національної інфраструктури й інформаційних ресурсів, наповнення світового та українського інформаційного просторів достовірною інформацією стосовно України, впровадження у цій сфері новітніх технологій,

- активне залучення та застосування засобів масової інформації до протидії зловживанням службовим становищем, корупції та іншим явищам, що загрожують національній безпеці;

- забезпечення неухильного додержання конституційних прав громадян на доступу до інформації й свободу слова, недопущення неправомірного втручання державних органів влади (включаючи органи місцевого самоврядування) та їхніх посадових осіб в роботу ЗМІ, переслідування журналістів за їхні політичні позиції, дискримінації у інформаційній сфері;

- вжиття комплексних заходів стосовно захисту інформаційного національного простору та протистояння монополізації вітчизняні інформаційної сфери.

За Законом України “Про національну безпеку” керівні принципи та цільові настанови державного керівництва у інформаційній сфері й напрямки діяльності державних органів влади в конкретній обстановці повинні визначатися Стратегією національної безпеки із метою своєчасного виявлення, нейтралізації чи запобігання потенційним й реальним загрозам інформаційним національним інтересам України (і не тільки інформаційним) в усіх серах життєдіяльності. Положення Стратегії національної безпеки, що стосуються забезпечення інформаційної безпеки держав, буде нами розкрито далі при аналізі нормативно-правових актів (указів) Президента України.

2.2. Нормативні акти конституційного напрямку, які закріплюють визначальні положення щодо забезпечення інформаційної безпеки України

Для забезпечення інформаційної національної безпеки важливим нормативно-правовим актом в Україні є Закон України "Про Основи формування інформаційного суспільства в Україні".

Так, в цьому Законі (п. 13 - "Інформаційна безпека у інформаційному суспільстві") визначається, що вирішення проблем інформаційної безпеки повинно здійснюватися за допомогою:

- підвищення рівня координування діяльності державних органів стосовно виявлення, прогнозування й оцінки загроз інформаційній безпеці, нейтралізації й запобігання таким загрозам, забезпечення ліквідації наслідків таких загроз, здійснення міжнародного співробітництва стосовно цих питань;

- створення інформаційної повнофункціональної інфраструктури в державі й забезпечення захисту її елементів критичного характеру;

- удосконалення нормативно-правової (юридичної) бази стосовно забезпечення інформаційної безпеки, а саме протидії комп'ютерній злочинності, захисту інформаційних ресурсів, захисту персональних даних, стосовно правоохоронної діяльності у інформаційній сфері.

Закон України "Про інформацію" (№ 2657-XII від 2.10.1999 р. є ще одним із суттєвих для забезпечення інформаційної національної безпеки нормативним актом. Цей Закон заклав правову основу інформаційної діяльності, утвердив інформаційний суверенітет країни, закріпив права на інформацію та на її доступ, визначив систему зобов’язань й відносин у цій сфері, що є загальноприйнятою для демократичних держав, визначив правові форми міжнародного співробітництва у сфері захисту інформації.

Цей Закон під інформацією розуміє задокументовані чи публічно оголошені відомості стосовно подій й явищ, що відбуваються

навколишньому природному середовищі, суспільств та державі (ст. 1 Закону).

Законом було встановлено загальні правові засади отримання, поширення, використання й зберігання інформації, закріплено права людей на інформацію у всіх сферах державного і суспільного життя в Україні, охарактеризовано систему інформації й її джерела, визначено статус суб'єктів інформаційних відносин, відрегульовано доступ до інформації й забезпечено її охорону, захищено людей й суспільство від неповної і неправдивої інформації. Дію цього Закону поширено на інформаційні відносини, що виникають в усіх сферах життєдіяльності людей, суспільства і держави у процесі отримання, поширення, використання й зберігання інформації (і стосовно використання мережі Інтернет).

У відповідності до Закону (ст. 7), суб'єктами інформаційних відносин виступають: юридичні особи, держава та громадяни України. Такими суб'єктами можуть бути також і інші держави, їхні юридичні особи, міжнародні організації, громадяни й особи без громадянства.

Об'єктами інформаційних відносин, у відповідності до Закону (ст. 8), є задокументована чи публічно оголошена інформація стосовно явищ й подій у галузі політики, охорони здоров'я, економіки, культури, а також в екологічній, міжнародній, соціальній та ін. сферах.

Окрім цього, Закон закріплює права на інформацію, що гарантує ст. 34 Конституції України, а також гарантії реалізації цих прав. У відповідності до Закону (ст. 9), всі юридичні особи, державні органи влади та громадяни України мають права на інформацію, що передбачають можливість вільного одержання, поширення, використання й зберігання відомостей, що необхідні їм для здійснення ними завдань й функцій та реалізації своїх прав, законних інтересів й свобод. Кожному громадянинові забезпечується при цьому вільний доступ до інформації, що стосується особисто його, крім випадків, що передбачені законами України. У процесі реалізації прав на інформацію вищезазначеними суб'єктами не повинні порушуватися громадські,

політичні, соціальні, духовні, економічні, екологічні й інші законні інтереси, права й свободи інших громадян та інтереси й права юридичних осіб.

У відповідності до Закону (ст. 12), основними напрямками інформаційної діяльності держави є: економічний, політичний, соціальний, екологічний, науково-технічний, духовний, міжнародний тощо.

Держава повинна гарантувати свободу інформаційної діяльності відповідно до цих напрямків всім юридичним особам й громадянам у межах їхніх повноважень й функцій, свобод й прав. Держава зобов'язана постійно дбати і про своєчасне формування, належний розвиток й функціонування інформаційних мереж, систем, баз й банків даних в усіх напрямках інформаційної діяльності.

У відповідності до Закону (ст. 13), основними видами інформаційної діяльності в державі є одержання, поширення, використання й зберігання інформації. Одержання, поширення, використання й зберігання задокументованої чи публічно оголошеної інформації відбувається в порядку, що передбачений цим Законом й іншими законодавчими (нормативно-правовими) актами у галузі захисту інформації.

Окрім зазначених вище положень, у Законі "Про інформацію" розкриваються також: 1) галузі, джерела й види інформації та режими доступу до неї (Розділ 3); 2) суб'єкти інформаційних відносин, їх обов'язки й права (Розділ 4).

У відповідності до українського Закону «Про державну таємницю» (ст. 4) Верховна Рада України визначає державну політику стосовно державної таємниці як складової засад зовнішньої та внутрішньої політики. Окрім того, Закон визначає компетенцію державних органів влади (включаючи органи місцевого самоврядування) та їхніх посадових осіб в галузі охорони й захисту державної таємниці (ст. 5), здійснення прав власності на види секретної інформації й їх матеріальні носії (ст. 6), а також порядок фінансування витрат для здійснення діяльності, що пов'язана із державною таємницею (ст. 7).

В окремих розділах Закону "Про державну таємницю" розкривається низка положень стосовно віднесення інформації до категорії державної таємниці. Зокрема, у відповідності до Закону (ст. 8), до державної таємниці в порядку, що встановлюється в цьому Законі, відноситься інформація: 1) у сфері науки, техніки й економіки; 2) у сфері оборони; 3) у сфері охорони правопорядку й державної безпеки; 4) у сфері зовнішніх взаємовідносин.

Інформація, що не належить до державної таємниці:

- стосовно стану довкілля, якості предметів побуту й харчових продуктів;

- стосовн аварій, катастроф, небезпечних природних явищ й інших надзвичайних подій, що можуть статися чи сталися та загрожують безпеці людей;

- стосовно стану здоров'я населення, його життєвого рівня, включаючи одяг, житло, харчування, соціальне забезпечення й медичне обслуговування, а також стосовно соціально-демографічних показників, освіти й культури населення й стану правопорядку;

- стосовно незаконних дій державних органів влади (включаючи органи місцевого самоврядування) та їхніх посадових осіб;

- стосовно фактів порушень свобод й прав громадянина й людини;

- інша інформація, що у відповідності до міжнародних договорів, згоду на обов'язковість яких надала Верховна Рада України, й українських законів, не можна засекречувати.

У Законі розкриті компетенція, обов'язки, права й відповідальність державних експертів стосовно питань таємниць (ст. 9) та порядок належання інформації до категорії державної таємниці (ст. 10).

В Законі окремою нормою визначені положення стосовно Зводу відомостей, які складають державну таємницю (ст. 12). Ці положення конкретизуються у наказі СБУ (№ 440 від 12.08.2005 р.), яким і затверджений Звід відомостей, які складають державну таємницю.

В Законі відповідним розділом виділені положення стосовно охорони державної таємниці (Розділ 4). При цьому в Законі розкриті основні організаційно-правові заходи стосовно охорони державної таємниці (ст. 18).

Зокрема, із метою охорони державної таємниці запроваджені:

- дозвільний порядок здійснення державними органами влади (включаючи органи місцевого самоврядування), установами, організаціями й підприємствами діяльності, що пов'язана з державною таємницею;

- єдині вимоги до виробництва, збереження, користування, обліку, передачі й транспортування матеріальних носіїв секретних видів інформації;

- обмеження передачі іншій державі, оприлюднення чи поширення іншими шляхами секретних видів інформації;

- особливості проведення органами державної влади своїх функцій стосовно органів державної влади (включаючи органи місцевого самоврядування), установ, організацій й підприємств, діяльність яких пов'язана з роботою із державною таємницею;

- обмеження стосовно перебування в Україні й діяльності іноземців, іноземних юридичних осіб, осіб без громадянства та їхнього доступу до інформації з категорії державної таємниці, а також переміщення й розміщення технічних засобів й об'єктів, що належать їм;

- спеціальний порядок доступу й допуску лююдей до державної таємниці;

- режим секретності державних органів влади (включаючи органи місцевого самоврядування), установ, організацій й підприємств, які здійснюють діяльність, що пов'язана з державною таємницею;

- криптографічний й технічний захист секретних видів інформації.

В Законі окремими нормами урегульовуються обов'язки українських громадян стосовно обмеження їхніх прав через доступ й допуск до державної таємниці, збереження державної таємниці, а також положення стосовно належної їм компенсації через виконанням робіт, що передбачають доступ їх до державної таємниці (ст. 29, 28 та 30 відповідно).

Закон також містить ряд важливих положень стосовно встановлення обмежень щодо оприлюднення секретних видів інформації (ст. 31), стосовно передачі державної таємниці міжнародній організації чи іноземній державі (ст. 32), а також стосовно обмежень, що пов'язані з державною таємницею, перебування в Україні й діяльності іноземців, іноземних юридичних осіб й осіб без громадянства, а також переміщення й розташування технічних засобів й об'єктів, що належать їм (ст. 33).

Криптографічний й технічний захист секретних видів інформації здійснюються у порядку, який встановлюють нормативно-правові акти (укази) Президента України.

Розшуково-оперативні заходи стосовно охорони державної таємниці проводяться органами Служби безпеки України у відповідності до Закону України "Про розшуково-оперативну діяльність".

Положення Закону стосовно нагляду за дотриманням законодавства щодо державної таємниці й контролю над забезпеченням охорони державної таємниці виокремлені у окремому розділі (Розділі 5) Закону.

Призначенням законодавства стосовно Програми національної інформатизації є впровадження організаційних, правових, науково-технічних, фінансових, економічних, гуманітарних й методичних засад регулювання процесів формування й реалізації цієї Програми й окремих її проектів (завдань). Закон встановлює також основні функції державних органів влади в процесі проведення інформатизації, зокрема:

- встановлення норм, правил і стандартів застосуванням засобів інформатизації;

- забезпечення інформаційної безпеки держави;

- забезпечення доступу людей та їхніх об'єднань до інформації державних органів влади (включаючи органів місцевого самоврядування) та до інших джерел й видів інформації;

- визначення пріоритетних напрямів інформатизації з метою подальшої її підтримки шляхом державного фінансування та пільгового оподаткування;

- інформатизацію науки, освіти, культури, охорони довкілля та здоров'я людини, державного управління, національної безпеки та оборони держави, пріоритетних галузей економіки;

- підтримку вітчизняного виробництва програмних і технічних засобів інформатизації;

- підтримку фундаментальних наукових досліджень для розроблення швидкісних математичних і технічних засобів обробки інформації;

- забезпечення підготовки спеціалістів з питань інформатизації та інформаційних технологій;

- організацію сертифікації програмних і технічних засобів інформатизації;

- державне регулювання цін і тарифів на використання телекомунікаційних та комп'ютерних мереж для потреб інформатизації у бюджетній сфері;

- захист авторського права на бази даних і програми, створені для потреб інформатизації та особистої інформації.

У законі визначено етапи формування і виконання, порядок здійснення експертизи, механізм контролю за виконанням Національної програми інформатизації, замовників, науково-технічну раду та виконавців програми, їх права та обов'язки.

Окрім того, в цьому Законі закріплені принципи державної політики у сфері інформатизації, визначені основні завдання, напрями, порядок формування та виконання основних етапів програми, очікувані результати.

Зокрема, Законом визначені такі основні напрями інформатизації:

- вироблення державної політики у сфері інформатизації та організаційно-правове забезпечення інформатизації;

- формування національної інфраструктури інформатизації, яка включає: міжнародні та міжміські телекомунікаційні та комп'ютерні мережі; систему інформаційно-аналітичних центрів різного рівня;

- інформаційні ресурси; інформаційні технології; систему науково-дослідних установ з проблем інформатизації; виробництво та обслуговування технічних засобів інформатизації;

- створення системи підготовки висококваліфікованих фахівців у сфері інформатизації;

- інформатизація стратегічних напрямів розвитку державності, безпеки та оборони (із забезпеченням інформаційної безпеки);

- інформатизація процесів соціально-економічного розвитку; - інформатизація пріоритетних галузей економіки;

- інформатизація фінансової та грошової системи, державного фінансово-економічного контролю;

- інформатизація соціальної сфери;

- інформатизація в галузі екології та використання природних ресурсів;

- інформатизація науки, освіти і культури.

Окрім того, в Законі визначено також низку інших важливих положень щодо програми інформатизації в Україні.

2.3. Нормативні акти вищих та центральних органів виконавчої влади, які регулюють діяльність у сфері забезпечення інформаційної безпеки України

В Стратегії національної безпеки відбулося визначення принципів, пріоритетних цілей, механізмів та завдань стосовно забезпечення важливих життєвий інтересів суспільства, держави і особи від внутрішніх й зовнішніх загроз у інформаційній й інших галузях життєдіяльності.

Головна мета Стратегії – потреба забезпечення такого рівня національної безпеки, який гарантував би поступальний розвиток держави, забезпечення свобод й прав людини й громадянина, конкурентоспроможність держави, подальше зміцнення авторитету та міжнародних позицій держави в сучасному світі.

Для досягнення цієї мети необхідною є реалізація політики держави стосовно національної безпеки, що передбачає забезпечення безпеки стосовно інформаційної складової, утвердження засад єдності нації задля розбудови правової, конкурентоспроможної, демократичної держави, зміцнення науково-технологічного потенціалу, формування соціально зорієнтованої ринкової економіки, забезпечення інноваційного розвитку, підвищення рівня життя й добробуту людей, техногенно й екологічно безпечних умов для життєдіяльності суспільства в країні.

В Україні в Стратегії національної безпеки розглядається інформаційна сфера як важлива складова життєдіяльності суспільства, держави й особи та одночасно і як одна з ключових сфер (складових) національної безпеки країни. С коло стратегічних пріоритетів стосовно політики національної безпеки у інформаційній галузі п. 3.10 Стратегіі серед іншого також відносить створення сприятливих зовнішніх й внутрішніх умов для безпеки й розвитку держави за допомогою забезпечення її інформаційної безпеки у процесі інтеграції держави в структури інформаційного глобального суспільства, одним із ключових елементів яких є інформаційна глобальна мережа Інтернет.

До того ж, п. 2.7 Стратегії до загроз й викликів життєво важливим інтересам (національним) України у інформаційній галузі додатково виокремлює: посилення зовнішнього негативного впливу на інформаційний національний простір України, що призводить до розмивання національної ідентичності й суспільних цінностей; недостатні обсяги виробництва національних конкурентоспроможних інформаційних послуг й продуктів, а також стан безпеки інформаційних й комп’ютерних систем (наближений до

критичного) у сфері державного управління, банківської й фінансової системи, енергетики, транспорту, міжнародних й внутрішніх комунікацій тощо.

У відповідності з п. 4.1 у Стратегії, подальший розвиток складових систем управління національною безпекою у інформаційній й інших сферах життєдіяльності суспільства в України повинно здійснюватися у таких напрямках, зокрема як:

1) удосконалення законодавства стосовно питань національної безпеки, передусім за допомогою наступного:

- розвиток правових засад стосовно управління національною безпекою шляхом розробки відповідних концепцій, доктрин, стратегій законів й програм;

- усунення наявних неузгодженостей, прогалин й протиріч у існуючих законах й нормативно-правових актах стосовно питань оборони й національної безпеки;

- впровадження та розробка технічних регламентів й національних стандартів використання інформаційно-комунікаційних технологій, що були б гармонізовані із відповідними стандартами Європи;

- приведення законодавства стосовно питань охорони й захисту державної таємниці до стандартів Європи;

2) підвищення ефективності координації, планування й контролю над діяльністю суб’єктів (учасників) забезпечення національної безпеки у інформаційній галузі та їхньої відповідальності, передусім за допомогою наступного:

- зростання ефективності діяльності суб’єктів (учасників) забезпечення національної безпеки із упереджувального одержання інформації для вчасного виявлення нових типів й існуючих зовнішніх й внутрішніх загроз у інформаційній галузі, розробка дієвих заходів стосовно їхньої нейтралізації й запобігання;

- інформаційно-аналітична підтримка діяльності державних органів влади, передусім в умовах надзвичайних й кризових ситуацій, у тому числі й особливого періоду;

- впровадження й розробка загальнодержавної системи моніторингу й визначення порогових значень індикаторів (показників), що характеризують виникнення реальних загроз безпеці національній, ступінь захищеності інтересів національних у інформаційній галузі та інших галузях життєдіяльності;

- впровадження інформаційно-телекомунікаційних мереж певного ступеня захищеності у державних органах влади.

Стратегія національної безпеки в Україні є документом, що обов'язковий для виконання, й платформою для розробки певних програм за конкретними складовими політики інформаційної безпеки в державі.

Водночас, враховуючи гострі проблеми, чинники й явища, що здійснюють негативний вплив на реалізацію політики держави стосовно забезпечення безпеки національної у інформаційній галузі, чим спричиняють породження нових загроз національним інтересам й національній безпеці в Україні у цій сфері та мають негативний вплив на розвиток усієї української держави й громадянського вітчизняного суспільства та реалізацію українських євроінтеграційних прагнень, Радою НБОУ було прийнято рішення сосовно доцільності вжити невідкладні заходи стосовно забезпечення інформаційної складової безпеки України (21.03.2008 р.).

Одним із ключових нормативно-правових (юридичних) актів, який заклав підвалини для здійснення захисту й забезпечення контролю над інформацією у мережах передачі даних сьогодні є Концепція ТЗІ (технічного захисту інформації), що затверджена Кабінетом Міністрів України (постанова № 1126 від 8.10.1997 р.).

Ще одним важливим документом стосовно контролю над інформацією у інформаційних мережах України стала "Інструкція стосовно порядку зберігання, використання й обліку справ документів, видань й інших

подібних матеріальних носіїв інформації, які мають конфіденційну інформацію, яка належить державі", що затверджена Кабінетом Міністрів України (постанова від 27.11.1998 р.)

Ключовими серед загальних положень даної постанови, ми вважаємо, є такі вимоги:

- стосовно заборони підключатися до глобальної мережі Інтернет локальним обчислювальним мережам, а також окремим електронно-обчислювальним машинам, на яких зберігається або обробляється інформація із обмеженим доступом, яка належить державі й охороняється законодавством України (п. 7 постанови);

- стосовно зобов'язання абонентів заключати договори про надання послуг стосовно доступу до глобальної мережі Інтернет й напротязі 15 робочих днів повідомити про це Державний комітет інформатизації й зв'язку України (п. 8 постанови).

На нашу думку, окрему увагу необхідно звернути на нормативні (юридичні) акти Кабінету Міністрів України, якими регулюється порядок висвітлення діяльності виконавчих органів влади у мережі Інтернет. Зокрема, це постанова Уряду (Кабінету Міністрів України) "Про заходи стосовно створення інформаційної електронної системи "Електронний Уряд" (№ 208 від 24.02.2003 р.).

Висновки до другого розділу

Протягом років незалежності в Україні було закладено законодавчі основи для створення системи забезпечення національної інформаційної безпеки, було напрацьовано, зокрема, суттєву кількість нормативно-правових актів, що визначають основні повноваження державних органів влади у інформаційній сфері.

На найвищому рівні слід розглядати норми Конституції України, в яких закріплюються концептуальні положення національної безпеки у всіх сферах існування України.

На другому рівні слід розглядати закони конститутивного напряму, що визначають важливі положення стосовно забезпечення безпеки в національній інформаційній сфері.

На третьому рівні слід розглядати закони інституційного рівня, в яких закріплено основні форми діяльності органів влади у державі в процесі забезпечення безпеки в національній інформаційній й інших сферах життя й діяяльності суспільства, держави та особи.

РОЗДІЛ 3. ПРОПОЗИЦІЇ ЩОДО ПОКРАЩЕННЯ СИСТЕМИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

3.1. Пропозиції щодо покращення державної політики у сфері забезпечення інформаційної безпеки України

Інформаційна безпека виступає необхідною умовою існування як суспільства і держави загалом, так і особи. Виходячи з цього, маємо виокремити такі рівні стосовно забезпечення інформаційної національної безпеки:

– суспільний рівень (формування якісного необхідного інформаційно-аналітичного простору, багатоканальність й плюралізм у одержанні інформації, потужні незалежні ЗМІ, що належать українським власникам);

– державний рівень (інформаційно-аналітичне забезпечення роботи державних органів влади, інформаційне забезпечення зовнішньої й внутрішньої політики на міждержавній арені, ефективна система захищенності інформації із обмеженим доступом, протидія комп'ютерним злочинам та правопорушенням у інформаційній галузі);

– рівень особи (формування критичного, раціонального мислення на базі принципів вільного вибору).

У процесі виробленні й реалізації політики у галузі забезпечення інформаційної національної безпеки держав необхідно взяти до уваги ряд принципових позицій й моментів.

Перше – правове регулювання в галузі інформаційної безпеки держав стосується тією або іншою мірою прав людей на інформацію, що закріплює Конституція України, положень стосовно демократичного устрою, плюралізму думок тощо, діючих законодавств стосовно інформації, стосовно забезпечення державної (національної) безпеки, охорони комерційної й

державної таємниць, діяльності Інтернету, засобів масової інформації, а також питань стосовно захищенності інформації із обмеженим доступом.

Друге – питання, що пов'язані зі зміною діючого українського законодавства в цій галузі, є, були і будуть заручниками політичної внутрішньої боротьби у країні. Будь-який розгляд у Верховній Раді України питань, що пов'язані з формуванням демократичних інститутів, плюралізмом, статусом ЗМІ, їхньої незалежності, неминуче виступає предметом великої дискусії.

Третє – важливою складовою частиною державної політики у будь-якій галузі слід назвати інформаційне забезпечення. Ця діяльність є і буде ключовим компонентом інформаційної національної безпеки нашої країни напротязі усього періоду її інтеграції. І якщо політики в Україні не сформують чіткі цілі, що будуть відповідати національним інтересам, й правильно не донесуть їх до громадськості, тоді це за них обов'язково зроблять суб'єкти ззовні. А потім вже під зовнішньо організованим тиском громадськості необхідні відповідні рішення будуть таки ухвалені (наприклад, через процедуру референдуму в 1997 р., як це відбулося в Словаччині), але чи будуть вони адекватні інтересам України.

Діяльність в такому напрямку повинна охоплювати постійний моніторинг думки громадськості, який доцільно проводити шляхом технологій контент-аналізу та соціологічних досліджень.

Четверте – хоча громадська думка і є достатньо піддатливою для маніпулювання (впливу), події в листопаді 2004-січні 2005 років в Україні свідчать на користь методів переконання та роз'яснювальної роботи, а не агресивної пропагандиської роботи.

П'яте – пріоритетною аудиторією мтомовно інформаційного впливу треба визначити педагогічний склад закладів вищої освіти й інших освітніх установ та представників. Досвід східноєвропейських країн переконливо показує, що саме ці дві суспільні групи є виразниками позицій у процесі формування думки громадськості та неформальними лідерами.

Основними напрямами політики держави у інформаційній галузі національної безпеки визнано:

– забезпечення інформаційного національного суверенітету країн;

– активне застосування засобів масової інформації у боротьби із зловживаннями службовим становищем, корупцією, іншими явищами, що загрожують й завдають шкоди національній безпеці країн;

– вдосконалення державного регулювання стосовно розвитку інформаційної національної сфери через створення нормативно-правових (юридичних) актів та економічних умов для розвитку інформаційної національної інфраструктури (та ресурсів), наповнення світового та внутрішнього інформаційного простору правдивою інформацією про Україну, впровадження передових технологій в цій галузі;

– забезпечення неухильного дотримання конституційних прав громадян на доступ до інформації, свободу слова, недопущення неправомірного втручання державних органів влади (включаючи органи місцевого самоврядування), їхніх посадових осіб в функціонування засобів масової інформації, переслідування журналістів за їхні політичні позиції та дискримінації у інформаційній галузі;

– вжиття комплексних заходів стосовно захищенності інформаційного національного простору й протистояння монополізації інформаційної національної сфери.

Адекватне реагування на виклики інформаційній національній безпеці виходить за рамки діючої нормативної бази й можливим є лише за умов прийняття певних політичних рішень компетентними владними органами. Треба визнати, що в умовах демократії в Україні формування політики держави у будь-якому напрямку залежить не лише від об’єктивного урахування національних інтересів й експертних оцінок, але й від політичної ситуації у певний період. Так основну рекомендацію стосовно процесу ухвалення певних політичних рішень можна сформулювати таким чином: врахування стратегічних довгострокових національних інтересів.

Дану ознаку довгостроковості може і повинно забезпечити законодавче регулювання найважливіших суспільних відносин. При цьому необхідно виходити із спрямованості нормативно-правових актів на досягнення практичного результату - формування ефективного механізму забезпечення інформаційної безпеки. Останній є системою взаємопов'язаних елементів, які забезпечують захист та розвиток інформаційного простору відповідно до національних інтересів.

У цьому механізмі повинні бути враховані національні інтереси в інформаційному середовищі, внутрішні та зовнішні загрози цим інтересам і передбачена система засобів із виявлення та нейтралізації загроз.

З огляду на структуру інформаційного середовища (простору) забезпечення інформаційної безпеки передбачає захист таких елементів:

– інформації з обмеженим доступом;

– систем і засобів передавання та зберігання інформації;

– інформаційного простору від поширення інформації, зміст якої через неповноту, недостовірність тощо суперечить національним інтересам держави.

До елементів системи забезпечення інформаційної безпеки (у вузькому розумінні) відносяться:

– нормативно-правові акти, які регламентують суспільні відносини в інформаційній сфері та встановлюють юридичну відповідальність у випадку їх порушення;

– державні та недержавні організації, які забезпечують продукцією ринок інформаційних послуг (ЗМІ, інформаційні агенції, служби, аналітичні та дослідні організації, власники каналів електронного зв'язку, Інтернет-провайдери, кіноіндустрія та індустрія розваг тощо);

– сукупність спеціально уповноважених органів держави, які контролюють дотримання інформаційного законодавства;

– практична діяльність зазначених суб'єктів, спрямована на розвиток вітчизняного інформаційного простору.

У широкому розумінні до системи забезпечення Інформаційної безпеки необхідно віднести Верховну Раду України та її законодавчу діяльність, Президента України, регуляторні та контролюючі державні органи, споживачів інформації та інших суб'єктів.

Правове регулювання у сфері інформаційної безпеки буде тією чи іншою мірою стосуватися закріплених у Конституції прав особи на інформацію, положень про демократичний устрій, плюралізм думок тощо, законодавства про інформацію, про забезпечення національної (державної) безпеки, охорону державної та комерційної таємниці, діяльність засобів масової інформації, інтернету, а також питань захисту інформації з обмеженим доступом.

3.2. Пропозицій щодо покращення нормативно-правового забезпечення інформаційної безпеки держави

Сьогодні:

1. Доцільним вбачається об’єднання (кодифікація чи інкорпорація) нормативних актів, що урегламентовують в Україні інформаційну діяльність.

2. Пропонується трирівнева система стосовно кримінально-правової захищенності інформаційної безпеки: безпека стосовно інформаційних впливів, безпека інформації, забезпечення реалізації прав усіх суб’єктів інформаційних національних відносин:

- Злочини, які посягають на безпеку інформації.
  - Злочини, які посягають на безпеку відкритої інформації;
  - Злочини, які посягають на безпеку інформації із обмеженим доступом;
  - Злочини, які посягають на безпеку інформації, що належить до категорії об’єктів інтелектуальної власності, та безпеку ноу-хау;
  - Злочини, які посягають на безпеку відносин в суспільстві та їхніх суб’єктів стосовно інформаційних впливів;

- Злочини, які посягають на безпеку інформації стосовно особи;
- Злочини, які посягають на безпеку відносин в суспільстві та їхніх суб'єктів стосовно впливів шляхом недостовірної інформації;
- Злочини, які посягають на безпеку відносин в суспільстві та їхніх суб'єктів шляхом приховування потрібної інформації;
- Злочини, які посягають на безпеку в суспільстві відносин в суспільстві та їхніх суб'єктів стосовно впливів шляхом забороненої ддя поширення інформації.

- Злочини, які вчиняються в телекомунікаційному середовищі (комп'ютерні злочини).

Встановлення родовим об'єктом саме інформаційних злочинів стосовно інформаційної безпеки у всіх трьох її складових компонентах дає можливість врахувати перспективи видозмінення інформаційних злочинів й появи їхніх нових видів, що будуть посягати на безпеку відносин в суспільстві та їхніх суб'єктів стосовно інформаційних впливів.

3. Реалізувати ідею формування громадського мовлення як комплексного заходу протидії комерціалізації засобів масової інформації.

4. Оптимізувати систему державного управління радіоі- та телеінформаційною сферами.

5. Важливо також широко застосовувати вже достатьо потужні можливості українських неурядових організацій (соціологічних, аналітичних центрів тощо). При цьому логіка дуже проста: якщо їхній потенціал не використовуватиме українська влада, то це будуть робити іноземці. Маємо достатньо прикладів роботи за іноземними грантами виключно (аналіз й отримання інформації із всіх галузей).

6. Пріоритетною аудиторією для державного внутрішнього інформаційного впливу визначити педагогічний склад закладів вищої освіти й інших закладів освіти та представників. Саме ці дві суспільні групи є сьогодні виразниками позицій при формуванні громадської думки та неформальними лідерами.

7. З метою реалізації фінансової незалежності ЗМІ треба передбачити фінансування державою тих з них, що пропонують аналітичні, інформаційні, просвітницькі та навчальні програми (останні переважно є нерентабельні).

8. Під неурядовою організацією треба визнати незалежну, неприбуткову (некомерційну), громадську, дослідну організацію, що має статус юридичної особи і вивчає різноманітні проблеми державного й суспільного життя, здійснює інформаційну діяльність, що спрямована на здійснення впливу на владу та лобіювання шляхом подання обґрунтованої критики, пропозицій або проектів рішень.

9. Для забезпечення інформаційної національної безпеки людини та суспільства стосовно зовнішніх деструктивних впливів (суб'єктом таких впливів може виступати і держава) треба передбачити на законодавчому рівні функціонування незалежних дослідницьких, аналітичних й інформаційних організацій, надавши їх відповідні права та визнавши їхню діяльність неприбутковою (це дозволить забезпечити фінансову незалежність та уникнути податкового тиску). Зазначену проблему треба вирішити шляхом затвердження окремого закону.

10. Розглянути можливості поширення вищезазначених правил функціонування неурядових організацій й на існуючі в Україні представництва іноземних неурядових організацій з наданням їм статусу юридичної особи та розширенням режиму національного фінансування (а відтак і обмеження стосовно частки фінансування).

11. З метою обмежити ймовірний деструктивний вплив іноземних елементів на роботу вітчизняних неурядових організацій передбачити в законі стосовно неурядових організацій диверсифікацію джерел їхнього фінансування й визначити відсоткову межу(обмеження) фінансування функціонування на гранти іноземних держав і міжнародних організацій та із іноземних джерел взвгалі.

12. Передбачити окремо обов'язкову участь українських громадян у керівних структурах неурядових організацій за такою схемою як: керівник –

громадянин України, його заступники - іноземці чи керівник - іноземець, його заступники - громадянини України.

13. Із метою забезпечення принципу демократичності у функціонуванні ЗМІ та колегіальності у процесі прийняття рішень передбачити обов'язкове утворення спостережної ради в ЗМІ, що створені в формі акціонерного товариства (сьогодні це більшість друкованих ЗМІ та телекомпаній).

У напрямі захисту інформації із обмеженим доступом пропонується:

1. Підготувати комплексний законодавчий акт стосовно захисту приватної інформації, де дати визначення поняття такої інформації, повноваження державних органів влади стосовно захищенності приватної інформації; окреслити обов'язки й права осіб стосовно захисту власних інтересів щодо приватної інформації, розробивши його наступним чином: загальні положення, список персональних даних як об'єкту захищенності (розділ 2), перелік суб'єктів, які матимуть доступ до списку персональних даних й їхні повноваження (розділ 3), режим охорони списку персональних даних (розділ 4), відповідальність за порушення законодавства стосовно персональних даних (розділ 5).

У законопроекті потрібно визначити, що формами регулювання роботи із персональними даними держави є: ліцензування роботи із персональними даними, сертифікація інформаційних систем персональних даних, реєстрація баз персональних даних, укладання міждержавних угод стосовно передачі (транскордонної) персональних даних.

2. Закріпити аконодавчо поняття службової таємниці.

3. Розробити Закон України "Стосовно участі України у міжнародному інформаційному обміні", метою якого є створення умов для результативної участі України у інформаційному міжнародному обміні в рамках єдиного інформаційного світового простору, захищенності інтересів держави й громадян, а також інтересів й законних прав юридичних та фізичних осіб у процесі здійсненні такого обміну. Об'єктами інформаційного

міжнародного обміну у відповідності до закону повинні бути: задокументована інформація, інформаційні продукти, інформаційні послуги, інформаційні ресурси, засоби міжнародного інформаційного обміну.

Також в цьому законі треба передбачити порядок передачі за кордон секретної інформації, запровадження обліку такої інформації, що передається міжнародним організаціям та іноземним державам або отримана від них, який детально регламентував би процедуру взаємного обміну секретною інформації між Україною та міжнародними організаціями й іноземними державами.

4. В Законі України "Про інформацію" визначити виключний перелік видів секретної інформації, куди віднести: державну, банківську й комерційну таємниці. Всю іншу інформацію із обмеженим доступом треба відносити до категорії конфіденційної інформації. Враховуючи складність та важливість проблеми, а також потребу залучення до вирішення її усіх зацікавлених державних органів влади, доцільно також обговорити питання стосовно можливої координації такої діяльності зі сторони РНБО України.

5. Уніфікувати із європейськими країнами категорії розмежування стосовно доступу до інформації.

З метою забезпечення захищенності інформаційного національного простору від зовнішнього негативного впливу, потрібно ухвалити Закон України "Стосовно захисту інформації у телекомунікаційно- інформаційних системах", що містив би:

– обов’язкові умови захищенності інформації у процесі надання послуг стосовно передачі даних, передусім із використанням Інтернет;

– правила й вимоги захищенності інформації у електронних мережах, що є власністю держави, чи інформації із обмеженим доступом, захищенність якої гарантується державою;

– механізми здійснення моніторингу мереж стосвно передачі даних виключно на базі національного й міжнародного законодавства, передусім положень резолюцій Ради Європи;

– збереження (обов’язкове) Інтернет-провайдерами відомостей стосовно Інтернет-трафіку напротязі півроку й надання інформації стосовно нього відповідно до рішень суду.

На сьогоднішній день однією із загроз в галузі інформаційної національної безпеки в країні є незаконне створення, продаж й поширення спеціальних технічних засобів (СТЗ) негласного одержавння інформації. Бурхливий розвиток інформаційних технологій дає можливість спрогнозувати якісне й кількісн зростання злочинності в галузях високих технологій, передусім злочинів із застосуванням спеціальних технічних засобів.

З метою протистояння незаконному використанню й обігу СТЗ, враховуючи викладене, пропонується:

1. Ввести кримінальну відповідальність за несанкціоновану розробку, виробництво й торгівлю СТЗ (законодавством України передбачена відповідальність за незаконне придбання, зберігання або використання СТЗ негласного одержавння інформації.

2. Обмежити число державних структур, у склад яких входять підрозділи з технічного документування (залишити право мати ці підрозділи лише СБУ.

3. Ввести обов’язкове ліцензування електронно-обчислювальної техніки ДССЗІ для установ, організацій й підприємств, в яких відбувається обробка інформації із обмеженим доступом і яка належить державі. Посилити контроль над додержанням вимог стосовно категорування приміщень й технічного обладнання, де здійснюється обробка ІзОД.

4. Надати можливість ДССЗІ регулярно проводити перевірки об’єктів, на яких здійснюється оброблення ІзОД, що належить державі.

5. Організувати СБУ тісну взаємодію із органами Державної митної служби, МВС, ГУР МО та СЗР з метою виявити канали незаконного ввезення в нашу державу СТЗ іноземного виробництва.

Так, ефективна реалізація нових норм законодавства в Україні потребує запровадження необхідних організаційних заходів, передусім:

– враховуючи транснаціональний характер правопорушень та комп'ютерних злочинів, розвиток міжнародної взаємодії спеціальних (у тому числі й правоохоронних) органів у цій галузі;

– створення спеціалізованих лабораторій для оброблення електронних доказів та проведення спеціалізованих експертиз із метою вдосконалення розслідування правопорушень та комп'ютерних злочинів;

– створення для правоохоронних органів спільного обліку осіб (юридичних й фізичних), що без встановленого дозволу проникали чи робили спроби проникнення в комп'ютерні системи, або причетні до інших правопорушень в сфері телекомунікаційно-інформаційних технологій;

– вирішення питання стосовно підготовки фахівців в галузі інформаційних технологій лище у профільних закладах освіти в кількості, яка відповідає потребам країни, а також подальшого працевлаштування їхніх випускників у державні структури на пільгових умовах, щоб недопустити відплив з країни кваліфікованих кадрів за кордон;

– сприяння створенню національних програмних послуг й продуктів, розробці інформаційних перспективних технологій з метою зниження рівня залежності від апаратного й програмного забезпечення іноземного виробництва, які можуть містити загрозу використання незадокументованих можливостей.

Водночас, забезпеченню поширення об'єктивних уявлень стосовно нашої країни у світі сприяла б допомога держави українським провідним агентствам, національним радіо- й телекомпаніям, окремим друкованим й електронним засобам масової інформації стосовно відкриття кореспондентських пунктів за кордоном й зростання кількості зарубіжних споживачів їхньої продукції.

Із метою посилити захищенність інформації, яка складає державну таємницю, на об'єктах інформаційної діяльності пропонується:

– посилити контроль зі сторони міністерств й відомств над підпорядкованими установами стосовно питань охорони державної таємниці;

– розробити систему інвестування й державної підтримки вітчизняних виробництв й проектів, що спрямовані на створення нових якісних технологій захисту та інформаційно-технічних засобів;

– передбачити статті видатків у державному бюджеті стосовно криптографічного й технічного захисту інформації;

– підвищити якість підготовки фахівців в галузі захисту інформації, яка складає державну таємницю.

Існує також нагальна потреба відкриття науково-дослідної роботи (НДР) "Шляхи й механізми стосовно забезпечення інформаційної національної безпеки", замовником якої повинно бути, як ми вважаємо, РНБО. Серед важливих наукових завдань, ящо мають бути виконані у межах НДР, передусім, варто забезпечити:

– вдосконалення методик інформаційного забезпечення формування, прийняття та застосування державно-управлінських рішень саме на стратегічному рівні управління;

– наукове обґрунтування методологічних основ створення Концепції інформаційної безпеки, Стратегії інформаційної безпеки та інших документів (керівних) в галузі забезпечення інформаційної безпеки;

– розробка методик та моделей оцінки ефективності політики держави в галузі інформаційної безпеки, складовою яких має стати методика прогнозування негативних наслідків стосовно державно-управлінських рішень у випадку їхнього впровадження;

– визначення технології, методології й розробки програмно-методичних комплексів виявлення СЮ та АЗА, що спрямовані на дискредитацію вищого керівництва країни;

– вироблення єдиного категорійно-понятійного апарату в галузі забезпечення інформаційної національної безпеки.

Особливої актуальності у процесі забезпеченні інформаційної безпеки у сучасних умовах набувають і технології управління інформацією, тобто інформаційного менеджменту. Переваги даного підходу заключаються в тому, що його можна використовувати як для атаки, так й для захисту інформаційного національного простору держави.

Висновки до третього розділу

Систему існуючих нормативно-правових актів стосовно регулювання галузі забезпечення української інформаційної безпеки потрібно удосконалювати, так як в Україні ще поки немає нормативних (юридичних) актів концептуального характеру, що предметно стосувалися б регулювання інформаційної галузі й забезпечення національної інформаційної безпеки. Значне число нормативних актів (і законів, і підзаконних актів, що неузгоджені не тільки між собою, але й із нормами міжнародних законів) значно зменшує ефективність всієї діяльності.

Одним із найвагоміших чинників національної безпеки країн є їхні економічні потенціали, під яким слід розуміти сукупність духовних й матеріальних сил суспільств, а також здатність держав мобілізувати ці сили заддля забезпечення своєї безпеки. Інформація, в свою чергу, охоплюючи всі сфери діяльності людей, підвищує ці економічні потенціали країн, забезпечє зростання духовних й матеріальних сил суспільств і створює умови задля можливостей, що пов’язані із мобілізацією та координацією. Крім того, вона утворює інтелектуальні й матеріальні ресурси країн задля ефективного захисту від в інформаційному відношенні агресивних держав. Очевидно з вищесказаного, що політику держав в галузі інформатизації й створення інформаційних ресурсів має бути спрямовано на створення умов задля якісного й ефективного інформаційного забезпечення вирішення задач стосовно соціально-економічного розвитку країн.

Розгляд проблем інформаційної національної безпеки держав надає можливість стверджувати думку про те, що забезпечення інформаційної національної безпеки слід покладати на інформаційну організацію держав. Остання повинна гарантувати інформаційну національну безпеку держав й її суб'єктів в сучасний час глобалізації й зростання загроз зі сторони міжнародного тероризму. В Україні, на жаль, існує надто багато негативних чинників, що утруднюють чи перешкоджають побудову такої інформаційної організації, та й не на останньому місці з них є і неузгодженість державних органів влади стосовно забезпечення національної інформаційної безпеки. Так, наукове дослідження сукупності проблем, що пов'язані із втіленням у життя та розробкою політики держави у інформаційній галузі, сьогодні набуло особливого значення через те, що їх розв'язання буде сприяти розвиткові інформаційного суспільства в Україні й таким чином забезпеченню інформаційної національної безпеки української держави.

ВИСНОВКИ

За результатами роботи:

1. Термін інформаційної безпеки містить у собі забезпечення вільного доступу людей до різного роду джерел інформації та якісне інформування громадян, а з другого – контроль за нерозповсюдженням таємної інформації, захисту від інформаційних негативних впливів, сприяння цілісності суспільства тощо.

Інформаційна безпека кожної держави характеризується станом захисту й, отже, стійкістю усіх основних сфер життєдіяльності (техносфери, економіки, науки, сфери управління, суспільної свідомості, військової справи і т. ін.) по відношенню до загрозливих небезпечних (деструктивних, дестабілізуючих, суперечуючим інтересам держави тощо) інформаційних впливів, причому і як до вилучення, і до впровадження інформації.

2. Протягом років незалежності в Україні було закладено законодавчі основи для створення системи забезпечення національної інформаційної безпеки, було напрацьовано, зокрема, суттєву кількість нормативно-правових актів, що визначають основні повноваження державних органів влади у інформаційній сфері.

На найвищому рівні слід розглядати норми Конституції України, в яких закріплюються концептуальні положення національної безпеки у всіх сферах існування України.

На другому рівні слід розглядати закони конститутивного напряму, що визначають важливі положення стосовно забезпечення безпеки в національній інформаційній сфері.

На третьому рівні слід розглядати закони інституційного рівня, в яких закріплено основні форми діяльності органів влади у державі в процесі забезпечення безпеки в національній інформаційній й інших сферах життя й діяяльності суспільства, держави та особи.

3. Систему існуючих нормативно-правових актів стосовно регулювання галузі забезпечення української інформаційної безпеки потрібно удосконалювати, так як в Україні ще поки немає нормативних (юридичних) актів концептуального характеру, що предметно стосувалися б регулювання інформаційної галузі й забезпечення національної інформаційної безпеки. Значне число нормативних актів (і законів, і підзаконних актів, що неузгоджені не тільки між собою, але й із нормами міжнародних законів) значно зменшує ефективність всієї діяльності.

Одним із найвагоміших чинників національної безпеки країн є їхні економічні потенціали, під яким слід розуміти сукупність духовних й матеріальних сил суспільств, а також здатність держав мобілізувати ці сили заддля забезпечення своєї безпеки. Інформація, в свою чергу, охоплюючи всі сфери діяльності людей, підвищує ці економічні потенціали країн, забезпечє зростання духовних й матеріальних сил суспільств і створює умови задля можливостей, що пов’язані із мобілізацією та координацією. Крім того, вона утворює інтелектуальні й матеріальні ресурси країн задля ефективного захисту від в інформаційному відношенні агресивних держав. Очевидно з вищесказаного, що політику держав в галузі інформатизації й створення інформаційних ресурсів має бути спрямовано на створення умов задля якісного й ефективного інформаційного забезпечення вирішення задач стосовно соціально-економічного розвитку країн.

Розгляд проблем інформаційної національної безпеки держав надає можливість стверджувати думку про те, що забезпечення інформаційної національної безпеки слід покладати на інформаційну організацію держав. Остання повинна гарантувати інформаційну національну безпеку держав й її суб’єктів в сучасний час глобалізації й зростання загроз зі сторони міжнародного тероризму. В Україні, на жаль, існує надто багато негативних чинників, що утруднюють чи перешкоджають побудову такої інформаційної організації, та й не на останньому місці з них є і неузгодженість державних органів влади стосовно забезпечення національної інформаційної безпеки.

Так, наукове дослідження сукупності проблем, що пов’язані із втіленням у життя та розробкою політики держави у інформаційній галузі, сьогодні набуло особливого значення через те, що їх розв’язання буде сприяти розвиткові інформаційного суспільства в Україні й таким чином забезпеченню інформаційної національної безпеки української держави.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. Богунов В. С. Щодо проблеми законодавчого врегулювання моніторингу телекомунікацій / В. С. Богунов // Матер, наук.-практ. конф. 29 червня 2014 р. "Концептуальні засади забезпечення державної безпеки України". - К.: НА СБУ, 2014. - С. 53-56.

2. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: Навч. посібник / В. А. Ліпкан, Ю. Є. Максименко, Л. В. Желіховськии. - К.: КНТ, 2010. - 280 с. (Серія: Національна і міжнародна безпека).

3. Марущак А. І. Інформаційне право: регулювання інформаційної діяльності: Навч. посібник / А. І. Марущак. - К.: Скіф, КНТ, 2018. - 344 с.

4. Марущак А. І. Правомірні засоби доступу громадян до інформації: Науково-практичний посібник / А. І. Марущак. - Біла церква: Буква, 2016. - 432 с.

5. Петрик В. М. Соціально-правові основи інформаційної безпеки: Навч. посібник / В. М. Петрик, А. М. Кузьменко, В. В. Остроухов / За ред. В. В. Остроухова. - К.: Росава, 2010. - 496 с.

6. Приватне життя і поліція. Концептуальні підходи. Теорія та практика / Відп. ред. Ю. І. Римаренко. - К.: КНТ, 2006. - 740 с. - (Людина. Суспільство. Поліція)

7. Савельев Д. Некоторые проблемы международного права телекоммуникаций [Електронний ресурс] // Інтернет-сторінка "Право та інтернет".

8. Системна інформатизація законотворчої та правоохоронної діяльності: Монографія / Кер. авт. кол. М. Я. Швець; за ред. В. В. Дурдинця, О. В. Зайчука, В. Я. Тація. - К.: Навчальна книга. - 2015. - 639 с.

9. Фронтов В. Регулирование телекоммуникаций в России и странах СНГ: Монография / В. Фронтов, В. Тихвинский. – К.: Горячая линия Телеком, 2013. - 368 с.

10. Юдін О. К. Інформаційна безпека держави: Навчальний посібник / О. К. Юдін, В. М. Богуш. - Х.: Консул, 2015. - 576 с.

11. Конституція України: ухвалена на п'ятій сесії Верховної Ради України 28 червня 1996 р. // Відомості Верховної Ради (ВВР) України - 1996. - № 30. - Ст. 141.

12. Закон України "Про національну безпеку України" від 21 червня 2018 р. № 2469-VIII // ВВР України. - 2008. - № 31. - Ст. 241.

13. Закон України "Про інформацію" від 2 жовтня 1992 р. // ВВР України. - 1992. - № 48. - Ст. 650.

14. Закон України "Про державну таємницю" від 21 січня 1994 р. // ВВР України. - 1994. - № 16. - Ст. 93.

15. Закон України "Про телекомунікації" від 18 листопада 2003 р. // ВВР України. - 2004. - № 12. - Ст. 155.

16. Закон України "Про зв'язок" від 16травня 1995 р. (в редакції від 5 червня 2003 р.) // ВВР України. - 2006. - № 30. - Ст. 258.

17. Закон України "Про радіочастотний ресурс" від 1 червня 2000 р. // ВВР України - 2000. - № 36. - Ст. 298.

18. Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" // ВВР України. - 2007. - № 12. - Ст. 102.

19. Закон України "Про Національну програму інформатизації" від 4 лютого 1998 р. // ВВР України. -1998. - № 27-28. - Ст. 181.

20. Закон України "Про концепцію Національної програми інформатизації" // ВВР України. -1998. -№ 75 -110 с.

21. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31 травня 2005 р. // ВВР України. -2006.-№26. - Ст. 347.

22. Закон України "Про захист суспільної моралі" // ВВР України. - 2004. - № 14. - Ст. 192.

23. Закон України "Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації" від 23 вересня 1997 р. // ВВР України. - 1997. - № 49. - Ст. 299.

24. Закон України "Про підприємництво" від 7 лютого 1991 р. № 698-ХП // ВВР України. - 1991. - № 14. - Ст. 168.

25. Закон України "Про ліцензування певних видів господарської діяльності" від 1 червня 2000 р. // ВВР України. - 2000. - № 36. - Ст. 299.

26. Закон України "Про банки і банківську діяльність" від 7 грудня 2000 р. № 2121-ПІ // ВВР України. - 2001. - № 5-6. - Ст. 30.

27. Указ Президента України № 663/97 "Про рішення Ради національної безпеки і оборони України від 17 червня 1997 року "Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин" [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

28. Указ Президента України від 27 вересня 1999 р. № 1229 "Про затвердження Положення про технічний захист інформації в Україні" [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

29. Указ Президента України "Про впровадження системи стратегічного планування" від 30 квітня 1999 р. № 460 [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

30. Указ Президента України "Про заходи щодо захисту інформаційних ресурсів держави" від 10 квітня 2000 р. // Офіційний вісник України. - 2000. - № 15.

31. Указ Президента України "Про удосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади" від 14 липня 2000 р. // Урядовий кур'єр. - 2000. - 18 лип.

32. Указ Президента України "Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних" від 24 вересня 2001 р. № 891 [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

33. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 19 липня 2001 р. "Про заходи щодо захисту національних інтересів у галузі зв'язку та телекомунікацій " від 23 серпня 2001 р. № 731/2001 // Офіційний Вісник України. - 2001. - № 35. -Ст. 1622.

34. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року з питання "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки" від 6 грудня 2001 р. № 1193/2001 // Офіційний Вісник України 2001. - № 50. - Ст. 2228.

35. Указ Президента України "Про заходи щодо забезпечення інформаційної безпеки держави" від 18 вересня 2002 р. // Офіційний Вісник України. - 2002. - № 38. - Ст. 1771.

36. Указ Президента України від 23 квітня 2008 р. № 377/2008 "Про рішення Ради національної безпеки і оборони України від 21 березня 2008 року "Про невідкладні заходи щодо забезпечення інформаційної безпеки України" [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

37. Указ Президента України "Про удосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади" від 14 липня 2000 р. // Урядовий кур'єр. - 2000. -18 лип.

38. Постанова Кабінету міністрів України від 27 листопада 1998 р. № 1893 "Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави" [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

39. Постанова Кабінету Міністрів України "Про затвердження Порядку підключення до глобальних мереж передачі даних" від 12 квітня 2002 р. № 522 [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

40. Постанова Кабінету Міністрів України "Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади" від 4 січня 2002 р. № 3 [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

41. Постанова Кабінету Міністрів України "Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах" від 16 листопада 2002 р. № 1772 [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

42. Постанова Кабінету Міністрів України від 19 липня 2006 р. № 1000 "Деякі питання обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави" [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

43. Наказ Служби безпеки України та Державної податкової адміністрації України "Про взаємодію Служби безпеки України та органів державної податкової служби України з профілактики, виявлення, припинення, розкриття та розслідування злочинів, інших правопорушень у сфері розроблення, виготовлення спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації та торгівлі ними" від 9 липня 2001 р. № 176/278 // Офіційний Вісник України. - 2001. - № 31. - Ст. 1432.

44. Звід відомостей, що становлять державну таємницю, затверджений наказом Служби безпеки України № 440 від 12 серпня 2005 р. [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

45. Бєляков К. І. Проблеми законодавчого регулювання у сфері користування інформацією з обмеженим доступом в Україні / К. І. Бєляков, Ю. П. Мірошник // Стратегічна панорама. - 2014. - № 3. - С. 171-177.

46. Кормич Б. А. Правова регламентація інформаційної безпеки держави / Б. А. Кормич // Держава і право: зб.наук. пр. Юридичні і політичні

науки. - Вип. 17. - К.: Ін-т держави і права ім. В.М. Корецького НАН України, 2002. - С. 193-198.

47. Конах В. К. Нормативно-правові засади державної політики України у сфері інформаційно-психологічної безпеки / В. К. Конах // Стратегічні приоритети. - 2012. - № 3(24). - С. 152-157.

48. Демський Е. Співвідношення адміністративної ігосподарської відповідальності / Е. Демський // Юридична Україна. - 2015. - № 9. - С. 24-30.

49. Масляниця Й. У. Інформаційні ресурси України :проблеми державного управління: монографія / Й. У. Масляниця, О. В. Соснін, Л. Є. Шиманський. - К.: НІСД, 2002. - 141 с.

50. Про Воєнну доктрину України: указ Президента України від 15.06.2004 р. № 648/2004 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/648/2004.

51. Про основні засади розвитку інформаційного суспільства в Україні: закон України від 09.01.2007 р. № 537-V // ВВР України. - 2007. - № 12. - Ст. 102.

52. Про основи національної безпеки України: закон України (із змінами, внесеними згідно із законами від 15.12.2005 р. № 3200-IV // ВВР. - 2006. - № 14. - Ст. 116; від 01.07.2010 р. № 2411-VI // ВВР. - 2010. - № 40. - Ст. 527) // Відомості Верховної Ради України. - 2003. - № 39. - Ст. 351.

53. Про Стратегію національної безпеки України: указ Президента України від 26.05.2015 р. № 287/2015 [Електронний ресурс]. – Режим доступу:http://www.president.gov.ua/documents/5728.html.

54. Про Доктрину інформаційної безпеки України: указ Президента України від 8.07.2009 р. № 514/2009 [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/9570.html.

55. Про Концепцію державної інформаційної політики : проект Закону України від 13.10.2010 р. № 7251 [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb_n/webproc4_1

56. Виноградова Г. В. Інформаційне право: Навч. посібник / Г. В. Виноградова. - К.: МАУП, 2011. - 144 с.

57. Галамба М. Інформаційна безпека України: поняття, сутність та загрози / М. Галамба [Електронний ресурс]. - Режим доступу: http://www.justinian.com.ua/article.php?id=2463

58. Гуцалюк М. В. Організація захисту інформації: Навч. посібник / М. В. Гуцалюк. - К. : Альтерпрес, 2012. - 224 с.

59. Дмитренко М. Проблеми інформаційної безпеки України / М. Дмитренко [Електронний ресурс]. - Режим доступу: http://social-science.com.ua/article/807

60. Василенко Д. П. Законодавство провідних країн світу в сфері захисту інформації / Д. П. Василенко [Електронний ресурс] – Режим доступу: http://www.kdu.edu.ua/statti/2010-2-1(61)/128.PDF

61. Про захист інформації в автоматизованих інформаційних системах: Закон України [Електронний ресурс]: офіц. вид. станом на 5.07.94 р.; № 80. – Режим доступу: URL: http://rada.gov.ua.

62. Про інформацію: Закон України [Текст]: офіц. вид. станом на 2 жовтня 1992 р. // ВВР України. - 1992. - № 48. [Зміни внесено Законами України № 1642-III від 06.04.2000 р. // ВВР України. - 2000. - № 27; № 304–III від 07.02.2002 р.]

63. Про національну безпеку України: Закон України [Електронний ресурс]: офіц. вид. станом на 21.06.2018 р.; № 2469-VIII. - Режим доступу: URL: http://rada.gov.ua.

64. Черненко Т. В. Пріоритети державної інформаційної політики в умовах гібридної війни / Т. В. Черненко // Стратегічні пріоритети. - № 4 (37), 2015. - С. 83-92.