

ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет права, публічного управління та національної безпеки
Кафедра економічної теорії, інтелектуальної власності та публічного управління

Кваліфікаційна робота
на правах рукопису

КОЗАЧИНСЬКА АНАСТАСІЯ СЕРГІЇВНА
(прізвище, ім'я, по батькові здобувача вищої освіти)

УДК: 659.4:327.88
(індекс)

КВАЛІФІКАЦІЙНА РОБОТА
ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ
(тема роботи)

281 «Публічне управління та адміністрування»
(шифр і назва спеціальності)

Подається на здобуття освітнього ступеня магістр
кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

А. С. Козачинська
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи
Іванюк Ольга Володимирівна
(прізвище, ім'я, по батькові)

кандидат економічних наук, доцент
(науковий ступінь, вчене звання)

Житомир – 2021

Висновок кафедри економічної теорії, інтелектуальної власності та публічного управління

за результатами попереднього захисту: **Козачинської Анастасії Сергіївни**

Протокол засідання кафедри економічної теорії, інтелектуальної власності та публічного управління № _____ від «_____» грудня 2021 р.

Завідувач кафедри економічної теорії, інтелектуальної власності та публічного управління

к.е.н., професор
(науковий ступінь, вчене звання)

(підпис)

Якобчук В.П.
(прізвище, ім'я, по батькові)

«_____» грудня 2021 р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти **Козачинська Анастасія Сергіївна** захистив
(прізвище, ім'я, по батькові)

кваліфікаційну роботу з оцінкою:
сума балів за 100-бальною шкалою _____
за шкалою ECTS _____
за національною шкалою _____

Секретар ЕК

(науковий ступінь, вчене звання)

(підпис)

Пугачова Н.С.
(прізвище, ім'я, по батькові)

АНОТАЦІЯ

Козачинська А.С. – Державна політика у сфері інформаційної безпеки України. Рукопис.

Кваліфікаційна робота на здобуття кваліфікації «Магістр» за спеціальністю 281 «Публічне управління та адміністрування». – Поліський національний університет Міністерства освіти і науки України, 2021.

У рамках дослідження визначено історичні особливості формування та становлення терміну «інформаційна безпека», проаналізовано світовий досвід функціонування державної політики у сфері інформаційної безпеки та перспективи його застосування у вітчизняних умовах, а також можливості покращення систем державної політики інформаційної безпеки.

Ключові слова: державна політика, інформаційна безпека, інформаційні загрози, інформаційний простір, безпека.

SUMMARY

Kozachynska A.S. - State policy in the field of information security of Ukraine. Manuscript.

Qualification work for obtaining the qualification "Master" in the specialty 281 "Public Administration". - Polissya National University of the Ministry of Education and Science of Ukraine, 2021.

The study identifies the historical features of the formation and formation of the term "information security", analyzes the world experience of state policy in the field of information security and prospects for its application in domestic conditions, as well as opportunities to improve public information policy.

Key words: state policy, information security, information threats, information space, security.

ЗМІСТ

ВСТУП.....	5
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ	
БЕЗПЕКИ.....	
1.1. Теоретичні засади створення та функціонування інформаційних ресурсів в Україні.....	8
1.2. Електронні інформаційні ресурси: суть та класифікація.....	11
1.3. Державна інформаційна політика України.....	14
Висновки до розділу 1.....	17
РОЗДІЛ 2. НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ	
БЕЗПЕКИ.....	
2.1. Нормативно-правове регулювання інформаційної безпеки.....	19
2.2. Загрози інформаційній безпеці України.....	20
2.3. Методи протидії інформаційним загрозам.....	23
Висновки до розділу 2.....	27
РОЗДІЛ 3. МІЖНАРОДНЕ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ	
ТА ЇХ ЗНАЧЕННЯ.....	
3.1. Використання України світового інформаційного простору.....	28
3.2. Зарубіжний досвід інформаційної безпеки в публічному управлінні.....	30
3.3. Роль та місце інформаційних ресурсів в системі публічного управління...	32
Висновки до розділу 3.....	35
ВИСНОВКИ.....	36
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	38
ДОДАТКИ.....	41

ВСТУП

Актуальність теми дослідження. Починаючи з кінця ХХ ст. для будь-якої держави інформація є стратегічно важливим ресурсом, де втілюються конституційні права та свобода громадян, а саме право вільного пошуку, отримання, передачі та поширення інформації всіма можливими законними засобами.

Інформаційні ресурси є найціннішими здобутками кожної нації, саме тому збереження інформації є головним завданням кожної держави.

Проблемою вітчизняного та світового документознавства є зберігання інформаційних надбань держави, яка потребує нововведень.

Розвиток інформаційної сфери все більше впливає на політичну, економічну, соціокультурну, оборонну складові розвитку суспільства та держави, забезпечення національної безпеки в сучасних умовах.

Згідно статті 17 Конституції України: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» [12; Ст.17]. Таким чином наша держава показує, що інформації українського народу має бути захищеною і це є найголовнішим її завданням, оскільки інформація – це зброя будь-якої спільноти. Адже, як сказав Натан Ротшильд «хто володіє інформацією, той володіє світом».

Із все більшим розвитком інформаційного суспільства в Україні більшість фахівців почали звертати увагу на поліпшення формування та використання інформаційних ресурсів. Почали з'являтися публікації у цій сфері, на державному рівні розробляються нові проекти законів щодо вдосконалення державної системи інформаційних ресурсів.

Мета дослідження: розглянути нинішній стан та розвиток державних інформаційних ресурсів України, проаналізувати систему державного управління інформаційних ресурсів.

Об'єкт дослідження: інформаційні ресурси та їх складові.

Предмет дослідження: використання інформаційних ресурсів в Україні.

Завдання дослідження:

- встановити особливості інформаційних ресурсів, класифікувати їх та визначити етапи створення;

- встановити етапи розвитку інформаційного суспільства в Україні;

3.проаналізувати нормативно-правову базу формування та використання інформаційних ресурсів;

- з'ясувати сучасний стан, проблеми та шляхи вдосконалення інформаційних ресурсів України.

Методи дослідження: для розкриття теми дипломної роботи застосовувалися історичні та системні підходи, порівняльний та структурно-функціональний аналіз, із допомогою яких вдалося розглянути загальні та особливі тенденції розвитку опрацьованих явищ та процесів.

До нормативно-правової бази можемо віднести: Конституцію України, закони України, нормативно-правові акти Президента України та інших органів державної влади.

Апробація результатів дослідження:

1. Козачинська А.С. Роль та місце інформаційних ресурсів в системі публічного управління. *Студентські наукові читання – 2021: Матеріали Міжфакультетської студентської науково-практичної конференції «Студентські наукові читання – 2021» за результатами I туру Всеукраїнського конкурсу студентських наукових робіт. у 2 томах. Т. 2. Житомир: Поліський національний університет, 2021. С.87*

2. Козачинська А.С. Загрози інформаційної безпеки, що пов'язані із інформаційно – комунікаційною сферою. Механізми управління розвитком територій: зб. наукових праць у 2 ч. Ч. 2. Житомир: Поліський національний університет, 2021. С.71

3. Козачинська А.С. Інформаційні ресурси України. Інструменти і практики публічного управління в контексті децентралізації : Матеріали III

Міжнародної науково-практичної конференції, 23 червня 2021 року. – Житомир : Поліський національний університет, 2021. С.232

Практичне значення отриманих результатів: Запропоновані нами в роботі заходи щодо удосконалення захисту інформаційних ресурсів України можуть сприяти підвищенню рівня захищеності інформаційних ресурсів України.

Структура дипломної роботи: дипломна робота складається із вступу, трьох розділів, висновків та списку використаної літератури. Загальний обсяг роботи складає 45 сторінок друкованого тексту, 35 з них основного тексту.

РОЗДІЛ 1.

ТЕОРЕТИЧНІ ПОГЛЯДИ СТВОРЕННЯ ТА ФУНКЦІОНУВАННЯ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

1.1. Теоретичні засади створення інформаційних ресурсів в Україні.

У зв'язку із швидким темпом зростання розвитку інформаційно-комунікаційних технологій набуло особливого значення введення електронних інформаційних ресурсів, які на сьогоднішній час стали зручним та ефективним видом передачі інформації.

Згідно статті першій Закону України «Про Національну програму інформатизації» інформаційні ресурси – сукупність документів в інформаційних системах (бібліотеках, архівах, банках даних тощо), які створені внаслідок використання певних засобів і методів опрацювання даних (технологій) [9]. Також у цій статті сформульовано ще одне визначення цього терміну: «інформаційна технологія – це планомірна організована сукупність інформаційних процесів з використанням засобів обчислюваної техніки, що забезпечують високу швидкість обробки даних, скорий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування» [9].

Отже, можна зробити висновок, що інформаційні технології це сукупність методів, засобів пошуку, розповсюдження, захисту та відображення інформації за допомогою нинішніх автоматизованих систем і мереж обміну даними.

Інформаційні ресурси можна поділити на національні, міждержавні, а також приватні, корпоративні, відомчі, регіональні. Структура, порядок формування, поширення та користування інформаційними ресурсами незалежно від їх виду регламентується відповідними нормами законодавства [5; с. 69]

Зважаючи на те, що національна безпека України з кожним днем все більше залежить від інформації, національні інформаційні ресурси держави можна розподілити на декілька рівнів важливості:

1. Стратегічні інформаційні ресурси – життєво важливі інформаційні ресурси, що становлять загрозу інтересам держави;
2. Критичні інформаційні ресурси – це інформаційні ресурси, втрата яких може завдати значних економічних, політичних та соціальних збитків державі;
3. Цінні інформаційні ресурси – це інформаційні ресурси втрата яких приведе за собою значні втрати життєздатності систем економіки, науки, виробництва та інших форм власності держави;
4. Загальносуспільні інформаційні ресурси – це ресурси, які задовольняють суспільні взаємини та які не мають особливих ознак, які б могли призвести до великих загроз державному суспільному ладу, державним інституціям тощо. [3; с.5] Найголовнішим видом інформаційних ресурсів є національні інформаційні ресурси ті, які задовольняють основні потреби народу, органів державної влади та органів місцевого самоврядування, фізичних та юридичних осіб. Саме ці ресурси є основою зміцнення та забезпечення суверенітету й інформаційної безпеки держави, а також слугують для вирішення завдань економіки, науки та інших сфер діяльності.

Також потрібно звернути увагу на те, що база національних інформаційних ресурсів включає в себе такі елементи:

- ✓ Інформаційні ресурси Кабінету Міністрів України, Верховної Ради України, Конституційного Суду України, Секретаріату Президента України, Верховного Суду України, Національного банку України, влади;
- ✓ Інформаційні ресурси органів державної влади та органів місцевого самоврядування, державних організацій та підприємств;
- ✓ Інформаційні ресурси національної системи науково-технічної інформації;
- ✓ Інформаційні ресурси музейного фонду України;

- ✓ Інформаційні ресурси національного архівного фонду;
- ✓ Національний електронний реєстр інформаційних ресурсів України;
- ✓ Інші організації, що мають національний статус згідно чинного законодавства України [6;с. 55]

Під інформаційними ресурсами також розуміють електронні інформаційні ресурси, які розміщені в електронних базах, у комп'ютерних системах, у системах обробки та передачі даних. Їх також називають веб-ресурсами.

Під час розміщення інформації, яка відповідає вимогам чинного законодавства, на веб-ресурсі діють такі заборони:

1. Не можна вказувати інформацію насильницького, анти людського характеру на своєму веб-ресурсі;
2. Зневажливо відноситись до релігійних, націоналістичних, культурних, політичних прав людини і поширювати інформацію, яка здатна спричинити ворожнечу;
3. Вказувати дані громадян, які можуть нашкодити репутації відповідним особам;
4. Розповсюджувати персональні дані без згоди суб'єкта даних та іншу конфіденційну інформацію;
5. Використовувати сварливі слова при викладі інформації;
6. Поширювати інформацію, що є власністю людини, без її письмової згоди [4;с.112]

Особа, яка веде свій веб-ресурс має право створити свій електронний інформаційний ресурс, як засіб масової інформації. Створити свій власний електронний інформаційний ресурс має право:

- Громадянин України;
- Трудові колективи організацій та підприємств, за рішенням загальних зборів (конференції);
- Юридичні особи України та інших держав;
- Громадяни інших держав і особи без громадянства [11; с. 187].

Наразі інформаційні ресурси стали основою більшості економічних,

управлінських та інших процесів. Інформація стала ключовим ресурсом країни, а новітні системи, які є основою її створення, обробки та поширення, позитивно впливають на швидкий розвиток та є складовою базової соціальної інфраструктури населення.

Отже, на сьогоднішній день виникла гостра потреба у необхідності забезпечити участь України у міжнародних органах з питань формування та застосування загальновідомого інформаційного простору та посилити участь України в міжнародних організаціях, які відповідають за розробку та формують відкриті стандарти у сфері інформатизації та телекомунікаційних технологій сьогодення. З тих же причин потрібно враховувати націоналістичні інтереси України та вдосконалювати її інформаційну безпеку.

1.2. Електронні інформаційні ресурси: суть та класифікація.

Основною розвитку інформаційних ресурсів є перетворення їх у електронний варіант із подальшим їх перенесенням на цифрові носії. Це дало можливість досить легко поширювати, пересилати інформацію за допомогою мережі Інтернет, а також дізнаватися потрібну інформацію у відкритому доступі.

Таким чином, розглянемо декілька основних термінів інформаційної галузі.

За Законом України «Про інформацію» інформацією називають будь-які відомості або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [8];

Інформаційний суверенітет держави – здатність держави контролювати та направляти потоки інформації з-поза меж держави з метою дотримання законів України, прав та свобод громадян, гарантування національної безпеки країни [8];

Інформаційний ресурс – це комплекс документів у інформаційних системах (бібліотеках, архівах, банках даних тощо)[8];

Електронний інформаційний ресурс – це інформаційний ресурс, який зберігається в електронному чи комп'ютеризованому варіанті та може бути досягнутий, знайдений та перероблений засобами електронної мережі або іншої електронної технології обробки даних [8].

Впровадження новітніх інформаційних технологій сприяло появі нових електронних ресурсів, таких як: бази даних, електронні видання, мультимедіа тощо.

Електронні інформаційні ресурси це можливість ефективно та швидко знайти різноманітну інформацію в різних областях діяльності людини.

На рис. 1.1 наведено види електронних інформаційних ресурсів.



Рис. 1.1 Види електронних інформаційних ресурсів. [11;с.5]

Внаслідок швидкого економічного розвитку швидкість розвитку електронних інформаційних ресурсів стрімко зростає. Завдяки використанню інформаційних технологій можна прискорити процес виконання операцій, що стосуються пошуку, аналізу, зберігання електронних інформаційних ресурсів у будь-якій системі управління.

На рис. 1.2 наведено ключові фактори негативного впливу на електронні інформаційні ресурси.



Рис. 1.2. Фактори, що негативно впливають на розвиток EIP [10;с.11]

На сьогоднішній день існує дуже багато різноманітних видів електронних інформаційних ресурсів. За словами Савенко З.В. їх можна класифікувати за такими категоріями, приклад яких наведено у таб. 1.1.

Класифікація електронних інформаційних ресурсів [19;с.9]

№ п/п	Ознаки	Приклад електронних інформаційних ресурсів
1.	За ступенем організації	Від постійного тексту, який не має поділу на абзаци, параграфи тощо, до формального представлення інформаційних даних у базах даних.
2.	За типом ресурсу	<ul style="list-style-type: none"> ➤ Електронні дані(зображення, звукові дані тощо); ➤ Електронні програми (програмне забезпечення): системні, прикладні та сервісні; ➤ Комбіновані: інтерактивні мультимедійні онлайніві служби.
3.	За типами носіїв електронних ресурсів	<ul style="list-style-type: none"> ✓ Локального доступу (інформаційні дані зафіксовано на окремому фізичному носіїві, інформація зчитується завдяки комп'ютерному пристрою); ✓ Ресурси віддаленого доступу (інформаційні дані, які подаються в інформаційних мережах).
4.	За технологією розповсюдження	<ul style="list-style-type: none"> ➤ Локальні електронні видання; ➤ Мережеві; ➤ Комбінованого розповсюдження.
5.	За характером взаємодії з користувачем	<ul style="list-style-type: none"> ✓ Обумовлені електронні інформаційні ресурси; ✓ Інтерактивні ресурси.
6.	За специфікою електронних ресурсів	<ul style="list-style-type: none"> ➤ За цільовим призначенням; ➤ За періодичністю; ➤ За структурою; ➤ За правовим статутом; ➤ За наявністю друкованого еквіваленту.

1.3 Державна інформаційна політика України

У Законі України «Про інформацію» державна інформаційна політика зазначається як сукупність основних напрямів та способів діяльності держави по отриманню, використанню, розповсюдженню та зберіганню інформації [8].

Головними напрямками та способами державної інформаційної політики є [8]:

1. Раціональне забезпечення доступу до інформації;
2. Створення спільної системи охорони інформації та ін.
3. Створення національних систем та мереж інформації;
4. Забезпечення вільного доступу громадян до інформації;

Державна політика у цій галузі є основою функціонування інформації – втілення права на пошук, отримання, передачу та використання інформації, що зафіксовані у Загальній декларації прав людини та у Конституції України [12]. У той же час інформаційна галузь відноситься до стратегічних інтересів будь-якої держави і саме тому вимагає особливої уваги. Від ступеня керованості державним інформаційним простором залежить стан економічної, політичної, оборонної та інших складових безпеки України.

Під керованість підрозумівають теперішній рівень управління галуззю, який спричинений, передусім, гармонізацією вітчизняного законодавства щодо інформаційної сфери з міжнародно-правовими нормами, європейськими стандартами та національними традиційними.

Суб'єктами інформаційних взаємозв'язків є: громадяни України, юридичні, фізичні особи та сама держава. Згідно Закону України «Про інформацію» держави інших країн, їхні громадяни та юридичні особи без громадянства також можуть бути суб'єктами інформаційних відносин. Від імені держави виступають: Президент України, Кабінет Міністрів, Верховна Рада України, Державний комітет телебачення та радіомовлення України та Національна рада з питань телебачення та радіомовлення.

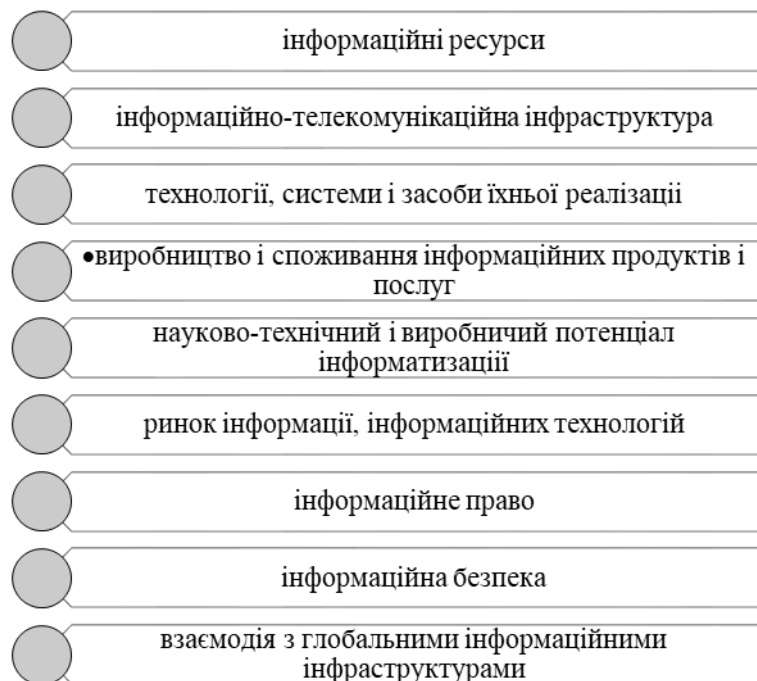


Рис. 1. 3. Об'єкти державної інформаційної політики

Державну інформаційну політику створюють та здійснюють органи державної влади спільної компетенції, а також відповідні органи спеціальної компетенції. Усі громадяни України, юридичні особи та державні органи мають право на інформацію та на вільне використання, зберігання та розповсюдження інформації (Рис. 1.3).

Метою державної інформаційної політики є побудова в Україні вільного та демократичного інформаційного суспільства, що інтегроване в світовий інформаційний простір. Для реалізації цього завдання необхідно зосередити зусилля на створенні потрібних умов та механізмів, що спрямовані на створення, розвиток та забезпечення ефективного використання інформаційних ресурсів.

Державна інформаційна політика є основною складовою зовнішньої та внутрішньої політики держави та охоплює усі галузі життя людей. Ця сфера має бути єдиною, концептуально надійною та результативною. Вона має бути незалежною від тимчасових факторів, особистих уподобань та уявлень.

Відповідно, надзвичайно важливим є ідентифікація та попередження виникнення внутрішніх та зовнішніх загроз інформаційній безпеці.

Інформаційна безпека визначається станом захищеності інформаційного суспільства, що забезпечує його утворення, розвиток та використання метою якої є інтереси громадян, організацій та держави [8].

Інформаційне середовище - це діяльність суб'єктів, що пов'язана із утворенням, перетворенням та споживанням інформації. Інформаційне середовище умовно можна поділити на три частини:

- Створення та поширення вихідної та похідної інформації;
- Утворення інформаційних ресурсів, планування інформаційних продуктів, надання інформаційних послуг;

- Використання інформації;

Та дві забезпечувальні предметні частини:

- Утворення та застосування інформаційних систем, інформаційних технологій та засобів їхнього забезпечення;

- Утворення та вживання способів та механізмів інформаційної безпеки.

Також існує більш ширше поняття **інформаційної безпеки** – це стан захищеності потреб в інформації особистості, суспільства та держави, при якому забезпечується їхнє існування та поступовий розвиток незалежно від існування внутрішніх та зовнішніх інформаційних загроз [8].

Залежно від виду загроз інформаційної безпеки інформаційну безпеку розглядають як:

- Інформації та інформаційні ресурси від безпідставного діяння сторонніх осіб;
- Забезпечення стану захищеності особистості, суспільства та держави від впливу неякісної інформації;
- Інформаційних прав та свобод людини та громадянина.

Інформаційна безпека є однією із сторін розгляду інформаційних взаємозв'язків в межах інформаційного законодавства з позицій захисту життєвих інтересів суспільства, держави та акцент уваги на загрози людським інтересам та на систему усунення та запобігання таким правовим викликам та методам.

Висновки до першого розділу

У першому розділі нами було визначено теоретичні засади створення інформаційних ресурсів в Україні. А також розкрили поняття інформаційних ресурсів. За статтею 1 Закону України «Про Національну програму інформатизації» інформаційні ресурси це комплекс документів в інформаційному колі (бібліотеках, архівах, банках даних тощо), що створені внаслідок задіяння відповідних засобів та методів опрацювання даних (технологій).

Усі інформаційні ресурси поділяються на:

1. Стратегічні інформаційні ресурси є життєво важливими інформаційними складовими, що становлять загрозу інтересам держави;

2. Критичні інформаційні ресурси – це інформаційні ресурси, втрата яких може завдати значних економічних, політичних та соціальних збитків державі;

3. Цінні інформаційні ресурси – це інформаційні ресурси втрата яких приведе за собою значні втрати життєздатності систем економіки, науки, виробництва та інших форм власності держави;

4. Загальносуспільні інформаційні ресурси – це ресурси, які задовольняють суспільні взаємини та які не мають особливих ознак, які б могли призвести до великих загроз державному суспільному ладу, державним інституціям тощо. [3; с.5] Найголовнішим видом інформаційних ресурсів є національні інформаційні ресурси ті, які задовольняють основні потреби суспільства, органів державної влади та органів місцевого самоврядування, фізичних та юридичних осіб. Саме ці ресурси є основою зміцнення та забезпечення суверенітету й інформаційної безпеки держави, а також слугують для вирішення завдань економіки, науки та інших сфер діяльності.

У результаті дослідження ми вияснили головні напрямки та способи державної інформаційної політики, серед яких:

1. Забезпечення доступу громадян до інформації;
2. Створення національних систем та мереж інформації;
3. Забезпечення продуктивного використання інформації;
4. Створення спільної системи охорони інформації та ін.

Та визначили, що метою державної інформаційної політики є побудова в Україні вільного та демократичного інформаційного суспільства, що інтегроване в світовий інформаційний простір, а також, що державна інформаційна політика є основною складовою зовнішньої та внутрішньої політики держави та охоплює усі галузі життєдіяльності суспільства.

РОЗДІЛ 2. НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Нормативно-правове регулювання інформаційної безпеки

Забезпечення інформаційної безпеки України, безпеки її національних інтересів в інформаційній сфері завбачає пріоритетний розвиток системи нормативно-правового регулювання відносин у цій сфері протидії загрозам цих інтересів та упорядкування відповідного правотворчого процесу.

Останнім часом державні органи все більше приділяють увагу обговоренню проблем вдосконалення правового забезпечення інформаційної безпеки України.

Система правового регулювання інформаційної безпеки, у свою чергу, включає масу правових норм, які регулюють відносини в даній сфері.

Правові норми складають базу забезпечення інформаційної безпеки і визначають ефективність діяльності держави, суспільства та окремих громадян із захисту національних інтересів України в інформаційній сфері. До складу цієї бази входять норми міжнародних договорів України, акти Президента України, постанови уряду та нормативні акти органів державної влади, які регулюють відносини у цій сфері. [20; с.1-2].

Наразі перед державою постала необхідність прийняти велику кількість нормативно-правових актів, які відповідають європейським стандартам.

За словами Юрія Максименка аналіз стану нормативно-правового регулювання інформаційної безпеки реалізується за трьома чинниками. Інформаційну безпеку України становлять три структурні елементи:

1. Інформаційна безпека у сфері прав і свобод людини та громадянина.
2. Інформаційно-психологічна безпека.
3. Інформаційно-технічна безпека.

Нормативно-правове регулювання інформаційної безпеки України це форма владного правового впливу на суспільні інформаційні відносини, яка здійснюється державою з метою їх упорядкування, фіксування та забезпечення. [14; с. 118]

Нормативно-правове регулювання інформаційної безпеки у сфері прав та свобод реалізується Конституцією України та опорними законами України, такими як: «Про Концепцію Національної програми інформатизації», «Про інформацію», «Про Національну програму інформатизації», «Про поштовий зв'язок», «Про науково-технічну інформацію» та ін.

Вказані вище нормативно-правові акти регулюють питання забезпечення інформаційної безпеки, питання захисту інформації, охорони державної таємниці, забезпечення захисту конфіденційної інформації та інформаційних ресурсів.

2.2. Загрози інформаційній безпеці України

Загрози інформаційної безпеки – це існуючі або можливі явища та фактори, що утворюють загрозу буденним інтересам людини та громадянина, суспільства та держави в інформаційній сфері.

Інформаційна безпека України забезпечується шляхом захисту державного інформаційного простору від інформаційних загроз та через підтримання його стійкому розвитку з метою втілення життєво важливих інтересів та потреб громадянина, суспільства та держави в інформаційній сфері.

Основними положеннями забезпечення інформаційної безпеки України є:

- верховенство права;
- перевага захисту прав і свобод людини та громадянина в інформаційній сфері;
- своєчасні та адекватні заходи захисту життєво важливих державних інтересів України від дійсних та можливих загроз інформаційній безпеці;

- захист інформаційного суверенітету України;
- незалежність думки та слова, а також вільне виявлення своїх поглядів та принципів;
- свобода збирати, зберігати, використовувати та поширювати інформацію;
- захист інформаційного суверенітету, національного суверенітету, конституційного ладу та територіальної цілісності України;
- утворення в інформаційному просторі української ідентичності як невід'ємного компонента постійного суспільно-політичного дискурсу;
- сприяння розвитку в національному інформаційному просторі контенту, який підтримує збереження та захист загальнолюдських цінностей, інтелектуальний, духовний та культурний розвиток Українського народу [8].

Державна політика у сфері інформаційної безпеки реалізується з метою недопущення перешкоджання виконання важливих інтересів та потреб громадянина, суспільства та держави зовнішніми та внутрішніми загрозами державній безпеці в інформаційній сфері, що є гарантією стійкого розвитку державного інформаційного простору.

Загрозами національній безпеці України в інформаційній сфері є [8]:

- загрози комунікативного характеру, що проявляються в сфері виконання потреб людини та громадянина, суспільства та держави щодо формування, використання, розповсюдження та розвитку державного ресурсу інформації;
- загрози технологічного характеру в сфері функціонування і захищеності телекомунікаційних, кібернетичних та інших систем, що утворюють матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору.

Загрози комунікативного характеру в сфері реалізування потреб людини та громадянина, суспільства та держави щодо утворення, використання, поширення та розвитку державного контенту та інформації включають:

а) навколишні негативні інформаційні впливи на свідомість людини та товариства через інформаційні ресурси, а саме: засоби масової інформації, мережу Інтернет, які завдають шкоду державі та основною ціллю яких є спроби змінити психічні та емоційні стани людини, її фізіологічні та психологічні характеристики; керування свободою вибору, шляхом поширення у національному інформаційному просторі культу насильства та жорстокості, зверхнього ставлення до людської та національної гідності, розпалювання міжетнічної та міжнаціональної, міжрелігійної ворожнечі, ненависті за етнічною, мовною, релігійною та іншими ознаками; розповсюдження закликів до сепаратизму, повалення конституційного ладу чи порушення територіальної єдності країни;

б) поширення суб'єктами інформаційної діяльності недостовірної та упередженої інформації для приниження органів державної влади, підриву суспільно-політичної ситуації, що перешкоджає правильному прийняттю політичних рішень, а також завдає шкоди державним інтересам країни та створює негативний імідж України;

Загрози технологічного характеру у сфері діяльності та захищеності телекомунікаційних, кібернетичних та інших автоматизованих систем, які утворюють матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору включають [8]:

а) застосування іноземними країнами кібервійськ, кіберпідрозділів, нових видів інформаційної зброї та зброї кібернетичного характеру на шкоду нашій державі;

б) вияви кіберзлочинності, кібертероризму чи кібернетичної військової агресії, що загрожують стійкому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем, методом вторгнення, несанкціонованого доступу або недотримання діяльності телекомунікаційних, кібернетичних, автоматизованих комп'ютерних систем, які незалежать від форми власності, з метою: вчинення терористичних актів; перехоплення

інформації в телекомунікаційних мережах; створення радіоелектронних бар'єрів, засобів зв'язку та управління.

в) використання неліцензійного та несертифікованого програмного забезпечення, засобів та комплексів обробки інформації.

2.3. Методи протидії інформаційним загрозам

На сьогодні інформація є визначальним ресурсом розвитку сучасного суспільства. Вона активно впливає на всі сфери життєдіяльності як окремих країн, так і всього світового співтовариства завдяки бурхливому розвитку інформаційно-комунікаційним технологіям.

Зазвичай вчені виділяють такі основні зовнішні джерела інформаційної безпеки [2; с. 105]:

— негативні наслідки діяльності іноземних політико-економічних, військових, розвідувальних, інформаційних та ін. структур, які спрямовані проти національних інтересів України, а також вірогідного послаблення можливостей їх реалізації;

— діяльність або прагнення державних та приватних структур іноземних держав до ущемлення національних інтересів на міжнародній арені, нанесення потенційної та реальної шкоди такими діями;

— підсилення конкурентної боротьби на міждержавному та транснаціональному рівні за володіння та користування теперішніми технологіями, засобами, системами;

— терористична, екстремістська та інша протиправна діяльність світових злочинних об'єднань;

— робота наземних, , космічних, морських та повітряних технічних засобів та приладів (супутників, радіоелектронного обладнання, інтернет-ресурсів та ін.) іноземних розвідувальних служб, яка псує інтереси держави;

— загострення енергетичних проблем;

— підготовка іншими країнами стратегій війн малої інтенсивності у інформаційній, технологічній, економічній та ін. сферах життєдіяльності, які передбачають суттєву дестабілізацію державної і недержавної складових у загальній системі забезпечення національної безпеки України.

Розглядаючи найбільш назрілі та значимі для сьогодення інформаційні загрози життєдіяльності держави та суспільства, зазначимо, що внутрішні та зовнішні загрози пов'язані між собою.

На сьогоднішній день в державі розроблена та затверджена Стратегія національної безпеки України (прийнята та затверджена Указом Президента України від 26 травня 2015 року № 287 "Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України"), яка основним видом інформаційних загроз національній безпеці нашої держави визначає агресивні дії Російської Федерації в інформаційному просторі [17].

Безпосередньо для нормативно-правового регулювання інформаційної безпеки держави було прийнято Указ Президента України №47/2017 Про рішення Ради національної безпеки та оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України", який затвердив основні положення забезпечення інформаційної безпеки держави в умовах ведення гібридної війни з Росією. Ця Доктрина визначила основні інтереси та прагнення України в інформаційному середовищі, основні загрози їх практичній реалізації пріоритетів та векторів державної політики в інформаційній галузі. Вона також розмежувала основні види зовнішніх інформаційних загроз, передусім з боку Росії, а саме [17]:

— проведення інформаційної експансії державою агресором та структурами, які їй підконтрольні [17];

— проведення інформаційних операцій, які спрямовані на зменшення обороноздатності держави, Збройних Сил України та інших військових утворень, посилення панічних, екстремістських настроїв серед населення, часткову чи повну дестабілізацію політичного чи соціально-економічного

життя, провокування та розгортання міжетнічних, міжконфесійних і соціальних конфліктів [17];

— домінування держав-агресора в інформаційному середовищі на тимчасово окупованих територіях [17];

— створення засобами інформаційного впливу негативного іміджу України на міжнародній арені [17];

інформаційним загрозам [17];

— пропаганда в світі та Україні автономістських, федералістських та ізоляціоністських настроїв і концепцій існування [17]

— обмеження можливостей України, окремих структур та органів ефективно протидіяти зовнішнім.

Для результативної боротьби зовнішнім інформаційним загрозам розроблено комплексна система механізм протидії, що включає такі елементи: сфери безпеки; параметри інформаційної безпеки; перелік інформаційних загроз та наслідки їх реалізації для України; мету забезпечення безпеки; система моніторингу та оцінки зовнішніх джерел інформаційної небезпеки; методи протидії зовнішнім інформаційним загрозам збоку державних структур [21; с. 182].

Для того щоб ефективно протистояти інформаційним впливам, попереджувати негативні наслідки від впливу пропаганди, необхідним є боротьба із інформаційними загрозами на стратегічному і тактичному рівнях, що може включати наступні напрями [17]:

1. Зміцнення співпраці щодо протидії пропагандистським впливам з іноземними державами.

2. Активізація виробництва власного інформаційного продукту та його поширення у Європі і світі.

3. Поліпшення нормативно-правового регулювання інформаційної безпеки, зокрема прийняття стратегії інформаційної безпеки на основі діючої доктрини.

4. Ефективна реалізація положень інформаційної доктрини в Україні.

5. Формування та зміцнення інформаційного простору держави, в якому циркулюватиме достовірна, неупереджена інформація.

6. Активізація громадських об'єднань та інших зацікавлених сторін до виявлення неправдивої інформації, що пришвидшить її нейтралізацію.

Таким чином, під поняттям методів реалізації державної політики протидії зовнішнім інформаційним загрозам варто розуміти комплекс різнопланових видів та способів діяльності державних структур та інституцій та засобів їх взаємодії, які дають змогу найбільш ефективно реагувати відповідним чином на зовнішні інформаційні загрози або управляти тими ризиками, що їх зумовили для подальшої їх нейтралізації. На відміну від традиційних методів нейтралізації інформаційних загроз, інноваційні методи ґрунтуються на принципах керування ризиками та можуть швидко блокувати деструктивні чинники та властивості загроз та надати стимул розгортанню і реалізації конструктивних елементів, властивостей та процесів в інформаційному просторі України. Для подолання інформаційних загроз нагально необхідним є ефективно реалізовувати державну доктрину інформаційної безпеки, підсилювати координацію та співпрацю з іншими країнами та із громадянським суспільством для виявлення інформаційних загроз; формування власного інформаційного простору з поширенням достовірної інформації. Перспективними з точки зору нових досліджень може бути науковий пошук найбільш результативних інструментів використання способів протидії інформаційних загроз.

Висновки до другого розділу

У другому розділі нами було визначено, що правові норми складають базу забезпечення інформаційної безпеки і визначають ефективність діяльності держави, суспільства та окремих громадян із захисту національних інтересів України в інформаційній сфері. До складу цієї бази входять норми міжнародних договорів України, акти Президента України, постанови уряду та нормативні акти органів державної влади, які регулюють відносини у цій сфері. [20; с.1-2].

Також розкрили питання загроз інформаційній безпеці України та шляхи їх подолання.

РОЗДІЛ 3.

МІЖНАРОДНЕ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТА ЇХ ЗНАЧЕННЯ

3.1. Використання України світового інформаційного простору.

Із появою інформаційних та телекомунікаційних технологій використання інформації набуло великого розвитку. Поряд із позитивними чинниками є ряд і негативних серед яких загроза цифрового розвитку або інформаційної залежності.

Ще у 90-х роках ХХ ст. американські фахівці прийшли до висновку, що країни, які перші пізнають інформаційний простір, матимуть велику перевагу над тими, що будуть після них. Ці висновки на сьогоднішній день повністю підтвердились. Прикладом можуть слугувати дані Світового банку, за якими капіталовкладення у нематеріальні активи, що формують національні бази знань, таких країн, як США, Скандинавські країни, Японія, Південна Корея, Сінгапур, в яких високий рівень знань та засобів комунікації, переважають капіталовкладення в головні фонди. У США фірми кожного року все більше витрачають на купівлю патентів, ліцензій та інформаційних систем 32 млрд. доларів, а міжнародні витрати на закупівлю нематеріальних виробничих ресурсів, що перевищують 100 млрд. доларів на рік. Світові інвестиції в науку (85%) втілюють країни-члени Організації Економічного Співробітництва та Розвитку, 11% - Індія, Китай та Бразилія та країни Східної Азії, 4% - інші країни світу, серед яких Україна [9;с.22].

Важливим досягненням нашої держави став вступ до Європейського Союзу, адже ЄС є сформованим інформаційним суспільством з високим рівнем згуртованості у світі та європейським інформаційним простіром.

Наразі на ринку існує потужна конкуренція інформаційних послуг та технологій у якій Україна має низький рівень. За соціологічним дослідженням

40% громадян України оцінюють рівень об'єднаності України у світовому інформаційному просторі низьким, лише 8,5% людей вважають високим.

Віддаючи перевагу інформаційній сфері економіки, стратегія Європейського Союзу відрізняється своїм відкритим соціальним спрямуванням. А ось у США перевага надається технологічним аспектам інформаційної супер мережі, Європа ж свій акцент робить на соціальний вимір.

Таким чином Європейська комісія розробила дослідження яке називається «Робота, та життя в інформаційному суспільстві». У цьому дослідженні підкреслюється, що сучасні технологічні трансформації створюють складні соціальні проблеми, які пов'язані із сферою зайнятості: чи зможуть люди пристосуватися до змін в умовах, коли інформаційні технології руйнують робочі місця? Також існує проблема інформаційного розриву між індустріальними та менш розвинутими країнами, молодим та старим поколінням. У дослідженні також зазначається, що можлива маніпуляція масою з боку тих, хто більше володіє знаннями та має доступ до інформації.

Простежується також аналіз проблем об'єднання України в європейський інформаційний простір, які спричинені внутрішніми та зовнішніми чинниками.

Насамперед, це відсутність національної системи класифікації інформації, слабкість системи стандартизації та сертифікації. В країні ще досі діють колишні стандарти системи ГОСТ, які не погоджені з міжнародним законодавством. Кількість періодичних видань та обсяги книгодрукувань значно скоротилися.

Національна система зберігання інформації перебуває у застарілому стані. Бібліотеки та архіви іноді перебувають у непридатних для них приміщеннях, що призводить до втрати маси інформації та обмежує громадян у вільному доступі до інформації.

Україна стоїть перед завданням розробки інноваційної політики та стратегії, що має багатий людський потенціал та слугує дієвому зростанню власного історичного потенціалу. Держава узгоджує всі процеси, які трансформують основи суспільства. Здебільшого, це стосується зовнішнього

напряму її діяльності. Тут український уряд працює вкрай завзято. Сьогодні Україна представлена в одних із потужніших міжнародних організаціях, як Європейська конференція Адміністрацій зв'язку, Міжнародний Союз електрозв'язку, Регіональне співтовариство в галузі зв'язку Європейський інститут телекомунікаційних стандартів. Також успіхом є підписання Паризького меморандуму згоди щодо розвитку Інформаційного суспільства, за яким високий пріоритет у взаємовідносинах між Європейською Комісією та Україною належить побудові в Україні інформаційного суспільства.

У висновку хотілося б сказати, що розвиток інформаційних технологій призвів до вільного потоку інформації. Розподіл інформаційних ресурсів між державами є також міжнародною проблемою, як і світовий розподіл енергетичних чи продовольчих ресурсів.

3.2. Зарубіжний досвід інформаційної безпеки в публічному управлінні

Наявність багатьох загроз інформації визначають актуальність проблеми інформаційної безпеки як компонент загальної проблеми інформаційного забезпечення розвитку людини, суспільства та держави загалом.

На інтернаціональному рівні інформація вважається важливим ресурсом життєзабезпеченням суспільства та має широке соціальне значення. Головними напрямками захисту інформації є: захист прав особистої інформації, захист державних інтересів, захист підприємницької та фінансової діяльності, захист інформації від комп'ютерних злочинів [18; с.44]

Важливим кроком у регулювання питання захисту інформації стало прийняття резолюції Генеральної Асамблеї ООН 54/90 «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» у 1999 році. У цьому документі постало питання захисту глобальних та телекомунікаційних систем та питання боротьби з тероризмом та криміналом.

Світове співтовариство признало міжнародну безпеку як глобальну проблему, яка вимагає негайного вирішення [1; с. 122].

Головним документом правового значення в США який безпосередньо стосується інформаційної безпеки є «Закон про інформаційну безпеку» виданий у 1906 році. В ньому окреслено можливі шляхи забезпечення безпеки в комп'ютерних системах.

В європейських країнах у сфері системи інформаційної безпеки в 2006 році була прийнята «Стратегія безпеки інформаційного суспільства: діалог, партнерство та розширення можливостей». У цій стратегії розглянуто сучасний стан загроз безпеці інформаційного суспільства та встановлено можливі заходи щодо забезпечення системи інформації безпеки.

За останні роки в ЄС діють декілька інноваційних проектів у сфері протидії кіберзлочинності. У червні 2010 р. було прийнято рішення про заснування Спеціальної групи з кіберзлочинності в ЄС (European Union Cybercrime Task Force), покликаної сприяти транскордонній боротьбі з кіберзлочинністю. [13; с. 207]. В Україні головними нормативно-правовими актами, що регулюють інформаційний простір є: Конституція України, Про Концепцію Національної програми інформатизації» (1998р.), «Про інформацію» (1992р.), Закони України: «Про основи національної безпеки України» (2003р.), «Про захист інформації в інформаційно-телекомунікаційних системах» (1994р.), Указ Президента України Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» та інші.

Отже, наразі нашій державі необхідно переймати досвід у європейських держав, у яких вже наявна система інформаційної безпеки, яка попереджає про можливі загрози та адекватно реагує на них. Щоб створити таку ж систему і у нас, потрібно поєднати найбільш прийнятні положення різних європейських країн та систематизувати їх до українських реалій.

3.3. Роль та місце інформаційних ресурсів в системі публічного управління

Термін «інформаційне забезпечення» доволі часто вживається у різних сферах діяльності держави. Разом з тим, незважаючи на суттєву кількість публікацій, що торкаються цього поняття, питання інформаційного забезпечення, особливо у сфері державного управління, у теоретичному плані в Україні до сьогодні належним чином не опрацьовано. Аналіз підтверджує, що інформаційне забезпечення державного управління є складним та різностороннім, проте нині немає єдиного розуміння щодо цього поняття. Така неозначеність є проблемою, яка перешкоджає розробці методологічних засад інформаційного забезпечення системи державного управління, так і його практичній реалізації.

Інформаційне забезпечення є одним із найголовніших питань для України в умовах формування сучасного інформаційного суспільства.

«Інформаційне забезпечення державного управління – це комплекс заходів органів державного управління усіх рівнів та всебічних дій суб'єктів інформаційної діяльності з метою формування, вживання та захисту в інформаційному просторі держави потрібних інформаційних ресурсів та їх своєчасне надання для реалізації функцій управління органів державної влади» [8].

Роль інформаційного забезпечення полягає в утворенні належних умов для здійснення персоналізованих функцій управління на підставі належної інформації.

Варто зазначити, що теза ряду авторів стосовно системності інформаційного забезпечення є позитивною, адже ґрунтовний аналіз схеми, поданої на малюнку 3.1, говорить про те, що виконання загального процесу кібернетичного управління вимагає комплексного підходу до інформаційного забезпечення виконання різнорідних функцій на всіх рівнях та етапах державного управління, а це дає можливість зробити акцент на необхідності

певної інформаційної підсистеми в рамках всієї системи державного управління.



Рис. 3.1. Кібернетична модель функціонування системи державного управління

Із усього вище сказаного випливає потреба у класифікації видів інформаційного забезпечення. Слід зазначити, що систематизації видів інформаційного забезпечення системи державного управління серед науковців та практиків на сьогодні відсутня. Головною причиною цього є те, що традиційно інформаційне забезпечення порівнюють із інформаційно-аналітичним в інтересах діяльності органів державного управління [7; 16], під яким розуміють «сукупність технологій, методів збирання та обробки інформації, що характеризує об'єкт управлінського впливу (соціальні, політичні, економічні та інші процеси), специфічних прийомів їх діагностики, аналізу та синтезу, а також оцінки наслідків прийняття різних варіантів політичних рішень». При чому у кінцевому результаті продуктом інформаційно-аналітичної роботи в державному управлінні є аналітичний документ.

Розглядаючи інформаційне забезпечення в системі державного управління Варто звернути свою увагу на її класифікацію. В основу класифікації входять функції, які здійснюють реалізацію компонентів інформаційного забезпечення системи державного управління. До видів інформаційного забезпечення державного управління входять [8]: *моніторинг стану* – комплекс заходів, що спрямовані на отримання інформації на базі всіх

доступних даних, з метою оцінки та передбачення розвитку процесів управління; **інформаційно-аналітичне забезпечення** – комплекс заходів, що формують процеси утворення інформаційних продуктів на основі використання статистичних інформаційних ресурсів, проведення розрахунків, моделювання ситуацій, аналізу та синтезу документованих даних та інформації з метою підтримки прийняття рішень органами державного управління всіх рівнів; **організаційно-управлінське забезпечення** – сукупність заходів, що використовують органи державного управління, аби правильно зробити рішення та донести його до своїх підлеглих; **іміджеве забезпечення** – застосування засобів масової інформації задля висвітлення діяльності системи державного управління та підняття позитивного рейтингу серед громадськості; **морально-психологічне забезпечення** – заходи, що використовуються з метою підтримання та відновлення у персонала системи державного управління моральних та психологічних якостей, його морально-психологічного стану на рівні, необхідному для успішного виконання завдань за призначенням; **захист інформаційних ресурсів** - правові, адміністративні, організаційні, технічні та інші заходи, що забезпечують збереження, цілісність інформації (інформаційних ресурсів) та належний порядок доступу до неї (них).

Усі ці види становлять базовий перелік інформаційного забезпечення системи державного управління.

Отже, у висновку хочеться сказати, що роль інформаційного забезпечення в системі державного управління полягає у створенні гідних умов для реалізації персоналізованих функцій управління на підставі відповідної інформації. А також спрямувати нові дослідження на обґрунтування та розкриття особливостей основних видів інформаційного забезпечення в системі державного управління та механізмів їх реалізації.

Висновки до третього розділу

У третьому розділі ми дослідили зарубіжний досвід інформаційної безпеки в публічному управлінні та з'ясували роль та місце інформаційних ресурсів в системі публічного управління. Головною роллю інформаційного забезпечення є утворення належних умов для здійснення персоналізованих функцій управління на підставі належної інформації. А також проаналізували усі наявні види інформаційного забезпечення державного управління.

ВИСНОВКИ

У висновку можна сказати, що в умовах сучасності термін «інформація» все частіше використовується дослідниками, як один із найважливіших стратегічних ресурсів. Однією із проблем сьогодення є трактування та сприйняття феномену, який називається «інформаційний ресурс».

Отже, на основі всього вище сказаного, можна відмітити, що інформаційні ресурси – це комплекс документів в інформаційних системах (бібліотеках, архівах, банках даних тощо), що створені внаслідок використання певних засобів та методів опрацювання даних (технологій).

Також потрібно зробити висновок, що під електронним інформаційним ресурсом розуміють інформаційні ресурси, які розміщені в комп'ютерних системах, в електронних базах тощо. При їх отриманні чи передачі за допомогою мережі Інтернет, їх називають веб-ресурсами.

Інформаційні ресурси виступають важливими елементами політичних, економічних, правових та інших суспільних процесів. Інформація у різних формах та виглядах введена до ринкових відносин.

За роки незалежності України у сфері інформатизації сталися певні позитивні зрушення, але й залишилася ціла низка невирішених важливих заходів, цілеспрямованих на розвиток інформаційного суспільства та вдосконалення керування інформаційними ресурсами на урядовому рівні.

Національний лад організації інформаційних ресурсів є одним із найважливіших умов розбудови самостійної демократичної держави. Побудова такої системи вимагає розсудливої урядової політики у сфері інформації, яка має бути спрямована на: захист вже наявних та сформованих нових функцій інформаційного ладу для досконалого комплектування загальнонаціональних інформаційних ресурсів; створення умов для пристосування інформаційних органів до нових потреб шляхом заохочування узгодженого попиту на інформацію та її використання у сферах культури, освіти, науки, управління та підприємницької діяльності.

Потребує подальшого покращення нормативно-правове забезпечення інформаційних ресурсів. Необхідно покращити процеси передачі державних інформаційних ресурсів для торгівельного використання, погодити правові норми, які впорядковують доступ до державних інформаційних ресурсів, формують порядок передачі та покращення інформації про діяльність органів державної влади, підприємств та організацій у відкритих мережах. Терміновим є питання прийняття Кодексу про інформацію.

У правовому, організаційному та організаційно-технічному планах Україні ще багато потрібно зробити для створення системи управління національними інформаційними ресурсами, лояльного захисту каналів державного управління, сучасних технологій та новітніх виробництв, що задовольняють вказівні аспекти країн у світі, – все те, що потребує державного захисту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Аверченков В. И. Системы защиты информации в ведущих зарубежных странах: 55 учеб.пособие для вузов / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский. – Брянск: БГТУ, 2007. – 225 с.
2. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти: монографія/ За загальною редакцією д-ра юрид. наук, проф. Бандурки О.М. — Харків: Видво Ун-ту внутр. Справ, 2000. — 368 с.
3. Баркова О. В. Електронні ресурси: аспекти типології / О. В. Баркова — Національна академія наук України, Національна бібліотека України імені В. І. Вернадського. - К., 2014
4. Безручко Д.С. Ключові напрями впливу інформаційно-комунікаційних технологій на економіку / Д.С. Безручко: VII Міжнародна науковопрактична конференція «Соціально-економічні реформи у контексті інтеграційного вибору України» 20.10.11р. [Електронний ресурс]. – Режим доступу: http://www.confcontact.com/2011/6_bezruchko.php.
5. Войчишин К.С. Створення системи інформаційних ресурсів: стандартизація і сертифікація – основа інформаційної інфраструктури [Текст] / К.С.Войчишин // Інформаційні технології і системи. – 2011. – Т.5, №1-2. – С.69-83.
6. Давидова І.О. Управління електронними інформаційними ресурсами: питання методології та організації [Текст] / І.О.Давидова // Вісн. Харк. держ. акад. культури. – 2011. – Вип. 10. – С.55-61
7. Енциклопедія державного управління : у 8 т. / Нац. акад. держ. упр. При Президентіві України ; наук.-ред. колегія : Ю. В. Ковбасюк (голова) та ін. – Київ : НАДУ, 2011. – Т. 2: Методологія державного управління / наук.-ред. колегія : Ю. П. Сурмін (співголова), П. І. Надолішній (співголова) та ін. – 2011. – 692 с.
8. Закон України «Про Інформацію» від 2 жовтня 1992 року № 2657-ХІІ

9. Закон України «Про Національну програму інформатизації» від 04.02.1998 № 74/98-ВР
10. Зернецька О.В. Глобальний розвиток систем масової комунікації і міжнародні відносини [Текст] / О.В.Зернецька.– К.: Освіта, 2002.– 351с.
11. Ковтанюк Ю. С. Електронне документознавство в Україні: сутність наукового напрямку, історія формування, перспективи розвитку: дис. канд. іст. наук / Ковтанюк Юрій Славович; Держ. архів. служба України, УНДІАСД. – К., 2012. – 252 с.
12. Конституція України від 28.06.1996р.
13. Логінова Н. І., Дробожур Р. Р. Правовий захист інформації: навчальний посібник / Логінова Н.І., Дробожур Р. Р. – Одеса: Фенікс, 2015. – 264 с.
14. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України: Дис.... канд. юрид. наук. – К., 2007.
15. Маращук А.І. Інформаційні ресурси держави: зміст та проблеми захисту [Електронний ресурс]. – Режим доступу: <http://www.ndcpi.org.ua>.
16. Президентіві України ; наук.-ред. колегія : Ю. В. Ковбасюк (голова) та ін. – Київ : НАДУ, 2011. – Т. 2: Методологія державного управління / наук.-ред. колегія : Ю. П. Сурмін (співголова), П. І. Надолішній (співголова) та ін. – 2011. – 692 с.
17. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про національну безпеку України": Указ Президента України від 26.05.2015 № 287/2015 [Електронний ресурс]. — Режим доступу: [www.president.gov.ua/ documents/ 2872015190](http://www.president.gov.ua/documents/2872015190)
18. Петрик В.М. Забезпечення інформаційної безпеки держави / В. М. Петрик, М.М. Присяжнюк // Підручник – К. : ДНУ «Книжкова палата України», 2015. – 675 с.
19. Савченко З. В. Формування і використання інформаційних електронних науково-освітніх ресурсів / З. В.

20. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В.А. Садовниченко и В.П. Шерстюка. – М., 2002.

21. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз // Підприємництво, господарство і право. — № 10. — 2017. — С. 182—189.

22. Шпакова О. Политика информационной безопасности в Украине: правовой базис [Текст] / О.Шпакова // Актуальні проблеми міжнародних відносин.– Вип.65(Ч.1), 2008.– С.242-249.