МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

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

Кваліфікаційна робота
на правах рукопису

ЛОНСЬКА ВАЛЕРІЯ ГЕННАДІЇВНА
(прізвище, ім'я, по батькові здобувача вищої освіти)

УДК: 351.347:004
(індекс)

КВАЛІФІКАЦІЙНА РОБОТА

ПУБЛІЧНЕ УПРАВЛІННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

(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

В. Г. ЛОНСЬКА
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи
ДОВЖЕНКО Валентина Анатоліївна
(прізвище, ім'я, по батькові)

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

Житомир – 2023

Висновок кафедри економічної теорії, інтелектуальної власності та публічного управління
за результатами попереднього захисту: **ЛОНСЬКУ Валерію Геннадіївну** допущено до захисту.

Протокол засідання кафедри економічної теорії, інтелектуальної власності та публічного управління № ____ від «____» грудня 2023 р.

Завідувач кафедри економічної теорії, інтелектуальної власності та публічного управління

к.е.н., професор	_____	Валентина ЯКОБЧУК
(науковий ступінь, вчене звання)	(підпис)	(власне ім'я, прізвище)

«___» грудня 2023 р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти **ЛОНСЬКА Валерія Геннадіївна** захистила
(прізвище ,ім'я, по батькові)

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

Секретар ЕК

_____-____	_____	Настасія ПУГАЧОВА
(науковий ступінь, вчене звання)	(підпис)	(власне ім'я, прізвище)

АНОТАЦІЯ

ЛОНСЬКА В. Г. Публічне управління у сфері інформаційної безпеки – Рукопис.

Кваліфікаційна робота на здобуття освітнього ступеня «Магістр» за спеціальністю 281 – «Публічне управління та адміністрування». – Поліський національний університет, Житомир, 2023.

Досліджено основні принципи та напрями діяльності публічного управління у сфері забезпечення інформаційної безпеки, завдання розвитку ефективної стратегії в умовах зростаючих кіберзагроз та технологічних викликів. Проаналізовано ключеві аспекти управління інформаційних ресурсів Житомирської ОВА, дії та процеси, які спрямовані на ефективне збереження, обробку та використання інформації. Запропоновано шляхи удосконалення управління інформаційними ресурсами так як умови гібридної війни визначають необхідність сучасної модернізації інформаційної політики держави.

Ключові слова: інформація, ресурси, безпека, держава, процеси управління, публічне управління, стратегія, захист.

ABSTRACT

LONSKA V. Public administration in the field of information security – Manuscript.

Qualification work for obtaining the Master's degree in specialty 281 – "Public management and administration". – Polissia National University, Zhytomyr, 2023.

The main principles and directions of public administration in the field of ensuring information security, the task of developing an effective strategy in the conditions of growing cyber threats and technological challenges have been studied. The key aspects of management of information resources of Zhytomyr OVA, actions and processes aimed at effective storage, processing and use of information are analyzed. Ways to improve the management of information resources are proposed, as the conditions of hybrid war determine the need for modern modernization of the information policy of the state.

Key words: information, resources, security, state, management processes, public administration, strategy, protection.

ЗМІСТ

ВСТУП

Актуальність теми. Умови воєнного стану, безсумнівно, ставлять перед нашою країною найвищі виклики та вимагають надзвичайної уваги до всіх сфер життя. Серед них особливе місце посідає сфера інформаційної безпеки, яка в умовах конфлікту стає не лише ключовою, але й стратегічною для збереження незалежності та безпеки нації. Публічне управління у цьому контексті набуває особливого значення, оскільки воно є механізмом, що формує не лише ефективні стратегії та політики, але й є основою для координації зусиль усіх сфер суспільства. У цій надзвичайній обстановці важливо розуміти, що публічне управління у сфері інформаційної безпеки стає важливим керівним інструментом, спроможним забезпечити не лише захист від кіберзагроз, але й зберегти стійкість та єдність країни в умовах воєнного стану.

Інформаційні ресурси на національному рівні вивчали Бучик С.С., Довгань О.Д., Марутян Р., Приймак Ю.Ю., Сосін О.В., Юдін О.К. та ін. Питанням інформаційної безпеки присвячені роботи таких дослідників: Аніщук В., Виздрик В., Кормич Б.А., Костікова М.В., Мельник О., Нестеренко Г., Плєхова Г. А. та ін. Проте сучасні умови створюють нові загрози, що потребують додаткових досліджень.

Предметом дослідження є сукупність теоретичних, методологічних та прикладних аспектів управління у сфері інформаційної безпеки держави.

Об'єктом дослідження є процес захисту національного інформаційного простору в умовах воєнного стану.

Метою дослідження є ідентифікувати особливості публічного управління у сфері інформаційної безпеки держави та запропонувати сучасні механізми захисту національного інформаційного простору.

Відповідно до мети, у роботі потрібно вирішити низку *завдань:*

1. Розкрити сутність поняття та завдання управління інформаційними ресурсами держави у сфері інформаційної безпеки держави.

2. Оцінити інформаційні ресурси та ідентифікувати особливості управління інформаційною безпекою Житомирської ОВА.

3. Обґрунтувати напрями модернізації інформаційної політики держави в умовах гібридної війни.

Для ухвалення у кваліфікаційній роботі поставлених завдань сприяло використання *спеціальних та загальнонаукових методів здійснення досліджень***.** Відповідно, були вжиті таки методи як: монографічний метод, аналіз та синтез, метод порівняння, метод узагальнення – їх використано для теоретичних основ; абстрактно-логічний метод – для розгляду та обґрунтування пропозицій щодо модернізації інформаційної політики держави в умовах гібридної війни.

Елемент наукової новизни кваліфікаційної роботи полягає у обґрунтуванні сучасних механізмів захисту національного інформаційного простору та напрямів модернізації інформаційної політики держави.

Практичне значення отриманих результатів. Запропоновані у роботі підходи та пропозиції, спрямовані на модернізацію інформаційної політики держави, можуть бути використані суб'єктами публічного управління різних рівнів.

Апробація результатів дослідження. Результати проведеного дослідження за темою кваліфікаційної роботи доповідались та опубліковані у трьох збірниках тез конференцій.

Інформаційною базою дослідження були наукові праці вітчизняних і іноземних дослідників у сфері управління інформаційною безпекою, нормативно-правові документи, звіти органів виконавчої влади, ресурси Internet-мережі.

Структура роботи. Кваліфікаційна робота складається зі вступу, трьох розділів та висновків, що викладені на 42 сторінках друкованого тексту. Матеріали роботи містять 4 рисунки та 5 таблиць, список використаних джерел із 44 найменувань.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

1.1. Понятійно-категоріальний апарат інформаційної безпеки держави

Понятійно-категоріальний апарат інформаційної безпеки держави є ключовим елементом для розуміння та аналізу важливого аспекту сучасного суспільства. Цей набір термінів та понять визначає основні принципи та напрями діяльності у сфері забезпечення безпеки інформації, ставлячи перед сучасними державами завдання розвивати ефективні стратегії в умовах зростаючих кіберзагроз та технологічних викликів.

Перше визначення поняття інформаційної безпеки було сформульоване Л. Дж. Хоффманом, він підкреслив , що «інформаційна безпека – це певне становище інформації, відповідно якому забезпечується зберігання визначених політикою властивостей інформації» [34, с. 34].

Те як ми можемо сприймати інформаційну безпеку, саме як стан захищеності чи в цілому просто інформацію є найбільш поширеним підходом до сутності досліджуваного феномену. Беручи до уваги висловлення Б. Кормича, «інформаційна безпека – це певний стан повної захищеності встановлених законодавством норм та параметрів інформаційних процесів та відносин, який може забезпечувати важливі умови для існування держави, громадянина та суспільства в цілому , як суб’єктів цих процесів та відносин» [9, с. 109].

Інформаційна безпека як стану, почала розглядатись у чинній Стратегії інформаційної безпеки яка була затверджена Указом Президента України від 28 грудня 2021 року. Стратегія говорить про те що «інформаційна безпека України – є складовою частиною національної безпеки України. Це відповідний стан захищеності державного суверенітету, територіальної цілісності,

демократичного конституційного ладу та інших не менш важливих інтересів громадянина, суспільства та держави» [32].

Беручи до уваги проаналізовану нами наукову літературу , в якій розглядалися питання інформаційної безпеки, можна зробити висновок що більша кількість науковців висловлюють однакову думку , що інформаційна безпека – це невід'ємна складова національної безпеки та представляє собою:

– певне становище при якому особа відчуває повну захищеність свої інтересів, та суспільства в цілому . Відповідно до цього стану нанесення будь якої шкоди через негативні наслідки функціонування інформаційних технологій чи недостовірну інформацію має бути мінімальним. (Л. Харченко, В. Ліпкан, О. Логіно, А. Баранов, В. Богуш, О.Юдін, І. Чиж та ін.);

– стан при якому головним чинником є захищеність інформаційного простору, який має забезпечувати його утворення , застосування і розквіт в інтересах громадянина , організації та держави в цілому (В. Богуш, Юдін, Ю. Бондар та ін.).

Беручи до уваги зазначене вище , можна підкреслити, що більша частина науковців вважають інформаційну безпеку певною здатністю системи протистояти несподіваним чи необдуманим внутрішнім та зовнішнім загрозам. Можливість забезпечити безпосередній захист суб'єктів від негативного інформаційного впливу.

На нашу думку, інформаційна безпека України – це не лише технічно складний процес захисту від кіберзагроз, але й стратегічна мета, спрямована на збереження суверенітету, ефективне управління державою та забезпечення безпеки громадян. Це взаємодія технологій, освіти, свободи слова та публічного управління для побудови стійкого інформаційного простору, що сприяє розвитку країни та її громадян в умовах глобальних викликів та невизначеності.

Важливою ознакою інформаційної безпеки можна назвати імовірність появи загрози підвищеного ризику реалізації загрози або небезпеки для громадянина , суспільства та держави. Важливим критерієм ефективного

забезпечення інформаційної безпеки можна назвати високий рівень безпеки яка досягається мінімальними витратами.

На нашу думку, інформаційну безпеку держави можна розглядати як вагому функцію держави, невід'ємну складову національної безпеки країни, яка відповідає за стан захищеного інформаційного простору. Стан при якому головним чинником виступає захищеність національних інтересів держави в інформаційному середовищі, загалом можна відокремити все як процес при якому здійснюється управління наявними загрозами та майбутніми небезпеками. Також це можливість надати захист установлених законом правил, за якими здійснюються інформаційні процеси в державі, взаємодія між суспільством ,яка пов'язується із захистом досить важливих інтересів громадянина, держави від реальних та потенційних загроз в інформаційному просторі.

1.2. Інформаційний ресурс, як найважливіший ресурс держави

Інформаційні ресурси визнаються ключовою та невід'ємною складовою системи інформаційної безпеки, становлячи основний ресурс для взаємодії та обміну даними. Їх важливість полягає в тому, що вони не лише надають можливість зберігання та передачі інформації, але і створюють базу для розробки стратегій захисту від потенційних загроз.

Інформаційні ресурси мають важливе значення як стратегічний, так і тактичний об'єкт, особливо для державних структур. Врахування цих ресурсів є невід'ємною частиною прийняття рішень у всіх сферах державного управління. Розвиток інформаційного середовища має велике вплив на національну безпеку.

Інформаційні ресурси представлені документами і масивами документів, які знаходяться в різних інформаційних системах, таких як бібліотеки, архіви, фонди, банки даних, депозитарії, музейні сховища та інші.

Також існують інформаційні ресурси спільного користування, які включають інформаційні ресурси державних органів з науково-технічною інформацією, наукові та науково-технічні бібліотеки, а також комерційні центри, фірми, організації, які займаються науково-технічною діяльністю та мають угоди про спільне використання цих ресурсів.

Іншою важливою сферою є інформаційні ресурси науково-технічної інформації, які включають систематизовану колекцію науково-технічної літератури і документації. Це охоплює книги, брошури, періодичні видання, патентну документацію, нормативно-технічну документацію, промислові каталоги, конструкторську документацію, звітну науково-технічну документацію з наукових та дослідних робіт, а також депоновані рукописи та переклади науково-технічної літератури й документації, збережені на паперових або інших носіях.

Більш всеосяжним визначення інформаційного ресурсу ми можемо побачити в Законі України «Про національну програму інформатизації» [25]. У ст. 1 даного Закону інформаційний ресурс розкривається безпосередньо як «комплекс документів в інформаційних системах, таких як бібліотеки, архіви, банки даних та інші»[25].

Українське законодавство не надає повного юридичного визначення складових елементів інформаційних ресурсів. Відсутні вичерпні критерії, якими можна класифікувати інформаційні ресурси як державні або недержавні. Це створює труднощі у формуванні системи національних інформаційних ресурсів, управлінні цією системою, а також у правовому регулюванні функцій, пов’язаних з володінням, використанням і розпорядженням інформаційними ресурсами.

Основними ознаками інформаційного ресурсу є його системотворча та керівна роль у діяльності людини, суспільства та держави. Він позитивно впливає на соціально-економічний розвиток суспільства і держави, а також забезпечує національну безпеку. У разі дефіциту, низької якості або негативної інформаційної експансії з боку інших країн, інформаційний ресурс може

завдати шкоди суспільному життю. Він також може стати об’єктом кримінальних зазіхань і вимагати спеціальних заходів і засобів захисту. Окрім того, він має якості і ознаки, що характерні іншим ресурсам.

Варто відмітити, що інформаційні ресурси поділяються на дві категорії – національні та державні, залежно від їх значимості. Національні інформаційні ресурси охоплюють результати інтелектуальної діяльності у всіх сферах життєдіяльності людини, суспільства і держави. Вони представлені окремими документами і масивами документів, базами даних і знань, архівами, бібліотеками, музейними фондами та іншими матеріальними носіями інформації. Ці ресурси є об’єктом права власності будь-якого суб’єкта України і мають значущу споживчу цінність в політичній, економічній, науковій, освітній, соціокультурній, оборонній, ринковій, історичній, інформаційній та інших сферах [31]. Національні інформаційні ресурси підпадають під юрисдикцію України і є національним надбанням.

Національні інформаційні ресурси охоплюють всю інформацію, яка належить Україні, незалежно від її змісту, форми, часу та місця створення, а також форми власності [11, с. 496]. Це включає окремі документи і масиви документів, які є результатом інтелектуальної та творчої діяльності, і вони можуть бути зафіксовані на будь-яких носіях інформації. Національні інформаційні ресурси доступні для використання особами, суспільством та державою через засоби масової інформації, телекомунікації, архіви, бібліотеки, музеї, фонди, банки даних, публічні виступи, художньо-виконавську діяльність та інші засоби [11, с. 496].

Національні інформаційні ресурси є важливою ланкою для гарантування суверенітету та інформаційної захищеності держави, а також слугують для рішення певних завдань суб’єктів української економіки, науки та культури та ще багатьох сфер діяльності [3, с. 87]. У складі національних інформаційних ресурсів можуть бути інформаційні ресурси різної приналежності і форм власності.

Державні інформаційні ресурси є систематизованою інформацією, яка є доступною за допомогою інформаційних технологій, а право на володіння, використання або розпорядження такою інформацією присвоєні державним органам, військовим формуванням, державним підприємствам, установам та організаціям, а також фізичним і юридичним особам, які здійснюють обробку цієї інформації відповідно до наданих їм повноважень.

Інформаційні ресурси держави є вагомою частиною національних інформаційних ресурсів і мають споживчу цінність, яка охоплює політичну, економічну, наукову, освітню, соціокультурну, оборонну, ринкову, історичну, інформаційну та інші сфери. Будь-який суб'єкт інформаційних відносин в Україні має право на доступ до державних інформаційних ресурсів згідно з політикою безпеки та чинним законодавством.

Відповідно до Закону України «Про інформацію», право власності на інформацію може виникати наступними підставами: створення інформації своїми силами та за свій кошт, договір на створення інформації або договір, що передбачає перехід права власності на інформацію до іншої особи. Варто зазначити, що інформація, створена на кошти державного бюджету, є державною власністю.

Державні інформаційні ресурси, відповідно до визначення О. Юдіна, є результатами інтелектуальної та практичної діяльності, які формуються у всіх сферах життєдіяльності людини, суспільства та держави. Вони фіксуються та систематизуються на певних матеріальних носіях інформації, таких як окремі документи, бази даних, архіви, бібліотеки, музейні фонди та інші. Державні інформаційні ресурси можуть містити дані, відомості та знання, які є об'єктом права власності держави, незалежно від форми власності на час їх створення. Вони також мають споживчу цінність і призначені для розвитку і задоволення потреб громадян, суспільства та держави, а також підлягають захисту відповідно до визначеної політики безпеки та чинного законодавства [37, с. 300].

Відмітимо, що державні інформаційні ресурси можуть бути розділені на дві групи відповідно до їх призначення [3, с. 88]:

1. Інформаційні ресурси, направлені на вирішення завдань конкретного органу управління певної ланки. Ці ресурси призначені для внутрішнього використання і забезпечують збір, обробку, зберігання та поширення інформації, необхідної для функціонування цього органу. Вони можуть включати бази даних, електронні системи документообігу, спеціалізовані інформаційні системи та інші компоненти.

2. Інформаційні ресурси, направлені на зовнішніх користувачів, формуються інформаційно-аналітичними структурами. Ці ресурси мають на меті надання інформаційної підтримки, аналізу та послуг різним зацікавленим сторонам, таким як громадяни, бізнес-суб'єкти, наукові установи та інші. Вони можуть бути орієнтовані на надання публічної інформації, статистичних даних, консультацій, експертних оцінок тощо.

Якщо інформаційні ресурси орієнтовані на зовнішнього користувача і мають загальне методичне керівництво, виконують схожі завдання на основі єдиних нормативних документів, то вони можуть бути класифіковані як державні інформаційні системи.

Варто також зауважити, що до державних інформаційних ресурсів висуваються вимоги щодо:

– нагальності та вірогідності приведених у них даних. Дані, що наведені на державних інформаційних ресурсах, повинні бути актуальними та надійними, відповідати дійсному стану речей і бути підтвердженими надійними джерелами;

– вичерпної повноти інформаційних джерел. Ресурси повинні містити достатню кількість інформації для задоволення потреб користувачів. Вони мають бути оснащені необхідними документами, даними, посиланнями та іншою інформацією, що допомагає розуміти та контекстуалізувати надані дані;

– компактності викладу. Інформація повинна бути подана зрозуміло і лаконічно. Ресурси повинні забезпечувати зручний та зрозумілий доступ до

інформації, використовуючи логічну структуру, систематизацію та належну організацію даних;

– оперативності пошуку. Ресурси повинні мати зручні засоби пошуку та навігації, що дозволяють користувачам ефективно знаходити необхідну інформацію. Швидкий та точний пошук за ключовими словами, категоріями, тегами або іншими параметрами є важливим аспектом державних інформаційних ресурсів [3, с. 89].

Згідно з Приймаком, державні інформаційні ресурси мають типову структуру, яка складається з двох частин:

а) обов'язкової. Обов'язкова частина включає основну інформацію і вихідні дані. Основна частина ресурсу містить ключову інформацію, що передбачена для користувачів. Ця частина може включати законодавство, нормативні акти, статистичні дані, звіти, рішення, протоколи тощо – в залежності від призначення конкретного ресурсу. Вихідні дані є джерелами інформації, на основі яких створюється основна частина. Це можуть бути документи, звіти, дослідження, статистика, аналітичні матеріали тощо;

б) факультативної. Факультативна частина включає довідково-бібліографічний апарат і додаткову інформацію. Довідково-бібліографічний апарат включає розділи або ресурси, що допомагають користувачам у знаходженні додаткових джерел інформації. Це можуть бути бібліографічні списки, посилання на релевантні джерела, довідкова інформація про авторів або організації, методологічні пояснення тощо. Додаткова інформація може включати розширені пояснення, графіки, діаграми, візуалізації, пояснювальні записки, архівні матеріали або інші дані, які доповнюють основну інформацію [18].

У контексті впровадження електронного урядування, державні електронні інформаційні ресурси набувають особливої ваги. Основними завданнями щодо цих ресурсів є наступні:

– утворення та ведення Національного реєстру електронних інформаційних ресурсів, особливо реєстрацію та облік електронних

інформаційних ресурсів держави , створення та можливості доступної інформації про склад, розповсюдження і умови використання електронних інформаційних ресурсів;

– упорядкування, забезпечення доступу до наявних державних електронних інформаційних ресурсів та їх актуалізація;

– формування та гарантування ефективного використання електронних інформаційних ресурсів органами державної влади;

– покращення нормативно-правової бази, безпосередньо підкреслення порядку і умов користування, сплати виконаних робіт, пов’язаних з створенням, вживанням та захистом державних електронних інформаційних ресурсів;

– погоджування діяльності органів державної влади та підприємництва (бізнесу) у галузі формування, вживанням та захисту державних електронних інформаційних ресурсів [17].

Є певні особливо важливі правові та організаційні засади які передбачають оцінку стану який показує наскільки є захищені державні інформаційні ресурси в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах державних органів, органів місцевого самоврядування, військових формувань, створених відповідно до законів України, підприємств, установ і організацій незважаючи на форми власності [19]. Оцінювання стану захищеності державних інформаційних ресурсів в державних системах перед умовлене проведенням відповідних заходів, які є спрямовані на знаходження та знищення загроз для державних інформаційних ресурсів. Цей процес здійснюється з метою забезпечення безпеки та захисту інформації, що належить вищезазначеним державним та недержавним суб’єктам [19].

Отже, інформаційний ресурс визнається найважливішим для держави, оскільки він є основою для розвитку, прийняття управлінських рішень та забезпечення національної безпеки. Його значення полягає в підтримці національних інтересів, прав людини та основних свобод, а також ефективному

функціонуванні суспільства та державних органів. Як ключовий компонент суверенітету, інформаційний ресурс має визначальний вплив на різні аспекти економіки, науки, культури та інших галузей діяльності. Забезпечення його якості, захисту та ефективного використання стає стратегічним завданням для держави в умовах сучасного інформаційного суспільства.

1.3. Поняття та завдання управління інформаційними ресурсами держави у сфері інформаційної безпеки держави

Управління інформаційними ресурсами держави – це комплекс заходів, стратегій і процесів, спрямованих на ефективне використання, розвиток і захист інформаційних ресурсів у галузі державного управління. Його основне завдання полягає в забезпеченні доступу до інформації, оптимальному використанні інформаційних технологій та забезпеченні кібербезпеки державних інформаційних систем.

Управління інформаційними ресурсами держави є важливим аспектом діяльності сучасного уряду. Залежно від країни, управління інформаційними ресурсами може здійснюватися на різних рівнях, включаючи національний, регіональний та місцевий.

Основні завдання управління інформаційними ресурсами в Україні включають:

1. Гарантування доступу до інформації.

Забезпечення доступу до інформації є одним з основних завдань управління інформаційними ресурсами держави. Це дає змогу громадянам отримувати доступ до публічної інформації про діяльність уряду, його рішення, законодавство та послуги, що надаються.

Створення та підтримка веб-порталів, електронних систем документообігу, баз даних та інших інформаційних ресурсів дає змогу зробити інформацію доступною для широкої аудиторії. Громадяни можуть швидко та

зручно отримувати необхідну інформацію без потреби фізичного відвідування урядових установ або отримувати документи в паперовому форматі.

Окрім того, забезпечення доступу до інформації також може включати розробку та впровадження електронних сервісів для громадян, таких як електронне голосування, електронні форми звернень, онлайн-консультації та інші інтерактивні сервіси, що спрощують взаємодію громадян з урядовими органами та забезпечують доступ до потрібних послуг інтернет-користувачам.

Загалом, забезпечення доступу до інформації є важливим аспектом підвищення прозорості, демократичності та ефективності державного управління.

2. Керування інформаційною безпекою.

Керування інформаційною безпекою є важливою функцією держави для забезпечення захисту державної інформації. Це охоплює широкий спектр заходів, що направлені на запобігання несанкціонованому доступу, втраті, зміні або розголошенню інформації.

Одним з основних елементів керування інформаційною безпекою є розробка та впровадження політики безпеки. Політика безпеки визначає загальні принципи та цілі безпеки інформації, а також встановлює рамки і вимоги для захисту інформації. Вона повинна бути розроблена з урахуванням специфіки державних органів і відображати їх потреби та загрози.

Окрім політики безпеки, держава також повинна застосовувати технологічні заходи захисту. Це можуть бути різноманітні заходи, такі як шифрування інформації, встановлення брандмауерів і систем виявлення вторгнень, резервне копіювання даних, контроль доступу до інформації і т.д. Використання сучасних технологій є важливим для забезпечення ефективного захисту інформації.

3. Розвиток електронного урядування. Це означає використання сучасних технологій для забезпечення ефективного та електронного надання послуг громадянам і бізнесу. Це може включати електронну реєстрацію документів, електронні форми подання заяв, онлайн-платежі, електронне голосування тощо.

4. Координація інформаційних систем. Державні органи мають співпрацювати та координувати свої інформаційні системи для ефективного обміну інформацією та спільного вирішення завдань. Це може включати створення централізованих баз даних, встановлення стандартів обміну інформацією, розробку інтероперабельних систем, спільне використання інформаційних ресурсів тощо.

5. Розробка та впровадження стратегій і політик у галузі інформаційних ресурсів. Держава має розробляти стратегії і політики, направлені на ефективне використання інформаційних ресурсів. Це включає планування розвитку інформаційних технологій, стандартизацію, регулювання використання інформаційних систем, управління даними тощо.

6. Забезпечення охорони особистих даних. Держава має забезпечувати захист особистих даних громадян, що збираються та обробляються урядовими органами. Це включає розробку правил та політик щодо збору, зберігання та обробки особистих даних, контроль за їх використанням та запобігання несанкціонованому доступу до них.

7. Створення інформаційно-аналітичних систем. Держава може розвивати інформаційно-аналітичні системи для збору, обробки та аналізу даних з метою прийняття обґрунтованих рішень. Це може включати системи моніторингу, прогнозування, аналізу показників та статистики, які допомагають уряду здійснювати ефективне управління.

8. Розвиток інформаційної культури. Держава може сприяти розвитку інформаційної культури серед громадян шляхом проведення навчальних заходів, надання доступу до освітніх ресурсів, підтримки цифрової грамотності та свідомого використання інформаційних технологій.

Висновки до розділу 1

Беручи до уваги інформацію яка зазначена вище, можна підкреслити що, управління інформаційними ресурсами держави у сфері інформаційної безпеки є невід'ємною складовою ефективного функціонування сучасного суспільства. Це включає в себе впровадження технологічних заходів, розробку стратегій та політик, які спрямовані на забезпечення конфіденційності, цілісності та доступності інформації державних інформаційних ресурсів. Основні завдання управління включають реалізацію ефективних заходів кіберзахисту, розробку політики безпеки та створення інфраструктури, яка забезпечує відповідність вимогам сучасного цифрового середовища. Ці заходи не лише забезпечують захист інформаційних ресурсів держави, але й сприяють підвищенню рівня прозорості, демократії та ефективності державного управління в цілому.

РОЗДІЛ 2.
АНАЛІЗ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ВОЄННОГО СТАНУ

2.1. Інформаційні ресурси Житомирської ОВА

Умови воєнного стану створюють суттєві виклики для управління інформаційною безпекою держави. Аналіз управління в цих умовах включає кілька ключових аспектів:

1. Кіберзахист та кібервійська безпека. Умови воєнного стану можуть підвищити загрозу кібератак та кібервійництва. Управління інформаційною безпекою повинно включати розширені заходи кіберзахисту, виявлення та протидії кібернападам, а також вдосконалення інфраструктури для захисту критичних інформаційних систем.

2. Забезпечення зв'язку та інформаційної доступності. Забезпечення надійного і безперебійного зв'язку стає пріоритетом для забезпечення ефективної комунікації та обміну інформацією між військовими, правоохоронними та цивільними структурами. Це може включати розробку резервних систем і засобів зв'язку.

3. Стратегічне управління інформацією. З урахуванням воєнних загроз інформаційне управління повинно бути орієнтоване на забезпечення безпеки критичної інформації та вдосконалення стратегій обробки, аналізу та розповсюдження важливої інформації для державних органів та військових підрозділів.

4. Роль громадськості та медіа. Важливо враховувати роль громадськості та медіа в умовах воєнного стану. Забезпечення точної та об'єктивної інформації, а також взаємодія з громадськістю, може бути критичним для підтримки національного єднання та реагування на інформаційні загрози.

5. Етичні та правові аспекти. Умови воєнного стану підсилюють етичні та правові аспекти управління інформаційною безпекою. Додержання

міжнародних норм, захист прав людини та гарантування етичного використання інформаційних засобів стає суттєвим завданням.

Зауважимо, що аналіз управління інформаційною безпекою в умовах воєнного стану вимагає комплексного підходу, обов'язкового залучення технологій та розробки чітких стратегій для захисту критичних інформаційних ресурсів держави.

В рамках даного дослідження оцінимо інформаційні ресурси та інформаційну безпеку Житомирської ОВА.

Житомирська ОВА (ЖОВА), має різні інформаційні ресурси, які включають, але не обмежуються наступними:

1. Веб-сайт: ЖОВА має власний веб-сайт (рис. 2.1).

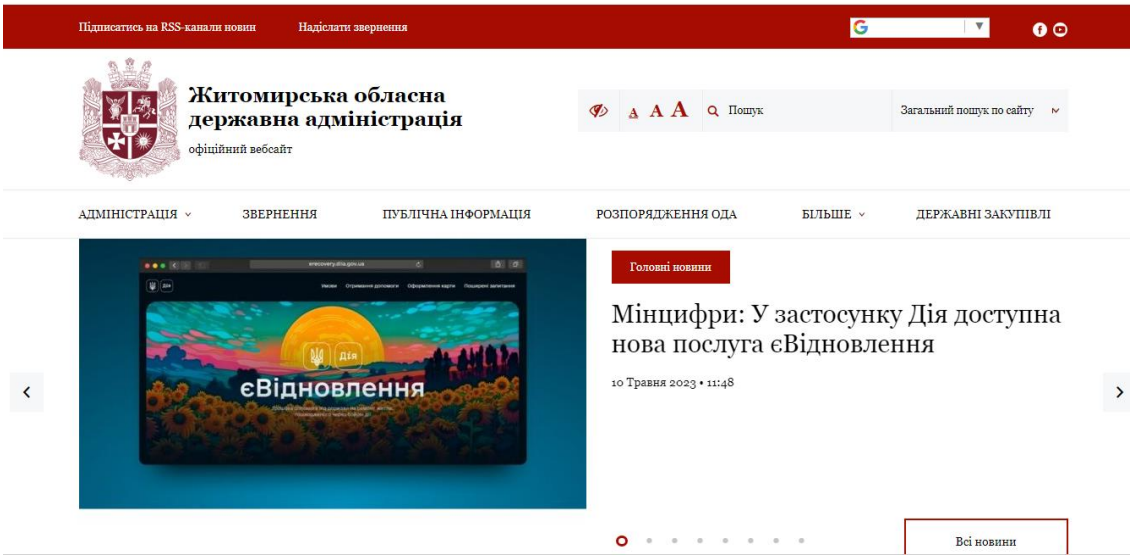

Рис. 2.1. Сторінка Житомирської обласної військової адміністрації

Джерело: побудовано автором за [17].

Сайт містить тематичні новини, нормативно-правові документи, інформацію про структуру облдержадміністрації, графік роботи, посилання на сторінки всіх управлінь, відділень та управлінь, що входять до структури Житомирської облдержадміністрації та на сторінки районних державних адміністрацій.

Відвідувачі сайту можуть безкоштовно отримати правову допомогу. Для цього достатньо зателефонувати по телефону, або перейти за вказаним посиланням.

На сайті Житомирської ОВА користувачі також можуть ознайомитися з повним переліком усіх адміністративних послуг, що можна отримати в різних Департаментах адміністрації (рис. 2.2).

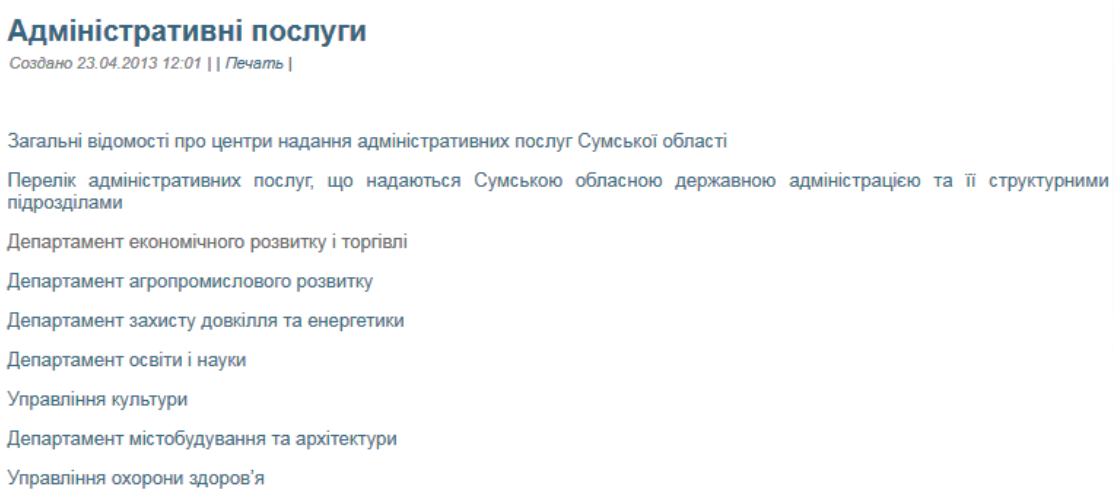

Рис. 2.2. Адміністративні послуги Житомирської ОВА

Джерело: побудовано автором за [17]

Також вже декілька років поспіль через сайт ЖОВА доступні наступні онлайн-послуги:

– запис на прийом до керівництва області;

– отримання посвідчення про реєстрацію місця проживання (для оформлення ID-картки);

– реєстрація місця проживання малолітньої дитини;

– зняття з реєстрації місця проживання малолітньої дитини;

– зняття з реєстрації місця проживання;

– реєстрація місця проживання;

– зняття з реєстрації місця проживання померлої особи [17].

2. Електронна пошта та електронні скриньки. ЖОВА має свою систему електронної пошти для спілкування з громадянами, представниками бізнесу та іншими органами.

3. Електронні системи управління документами. В наявності апарату ЖОВА є системи електронного документообігу (СЕДО). Відсоток працівників, що використовують СЕДО складає 5%.

Електронний цифровий підпис (ЕЦП) є наявним в обласній державній адміністрації присвоєний 1 ключ, Головному фінансовому управлінні облдержадміністрації належить 6 ключів.

Відповідно , інші інформаційні ресурси теж ведуться в електронному форматі, які створили слушним до нормативно-правових актів та розпорядчих документів (ЄІАС «Діти», центральний фондовий каталог архівного фонду України «FCDB», система обліку і обробки особових карток державних службовців, «Картка», «Парус-бухгалтерія») [17].

4. Електронні сервіси та портали. ОВА надає електронні сервіси та функціонал через спеціалізовані портали, такі як електронні сервіси для подання звернень (рис.2.3), отримання інформації, реєстрації та оплати послуг тощо.

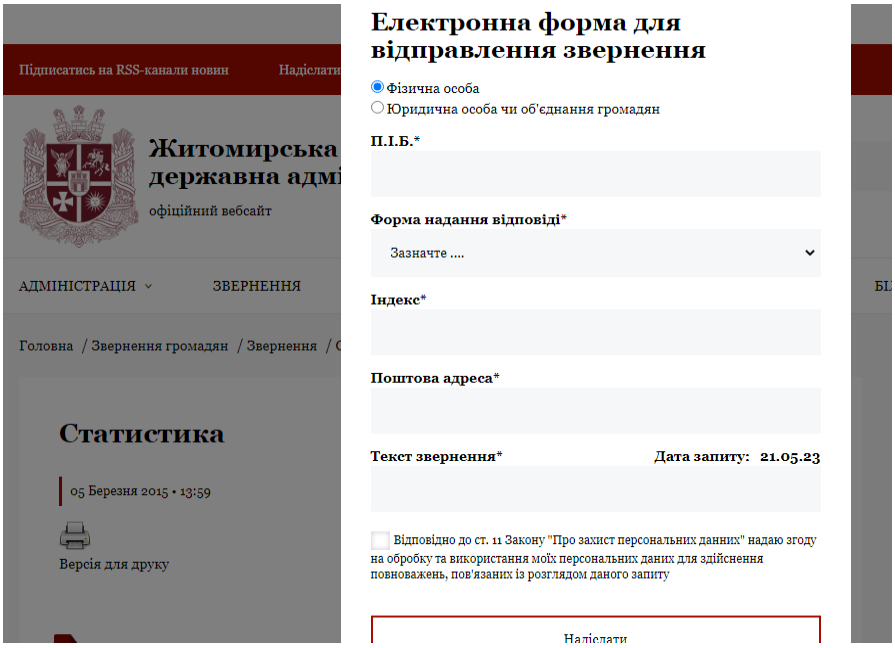

Рис. 2.3. Електронний сервіс для подання звернень Житомирської ОВА

Джерело: побудовано автором за [17]

Відмітимо, що впродовж 2022 року в кількість запитів на інформацію, що надійшли електронною поштою склала 366, що становить 92% від усіх отриманих запитів (табл.2.1).

Таблиця 2.1

Інформація про кількість запитів на інформацію до Житомирської ОВА у 2022 році

Запити за типом входження запиту	Кількість, од.
Поштою	25
Електронною поштою	366
Факсом	-
Телефоном	-
Особистий прийом	6
Загальна кількість отриманих запитів на інформацію	398

Джерело: складено автором за даними [17]

5. Інформаційні бази даних. Житомирська ОВА має інформаційні бази даних, що містять інформацію про різні аспекти діяльності обласної адміністрації, такі як бюджет, проекти, звіти, статистика тощо.

6. Соціальні медіа. Офіційна сторінка Житомирської ОВА є у соціальній мережі Facebook (рис. 2.4), у застосунку Telegram та на платформі YouTube.

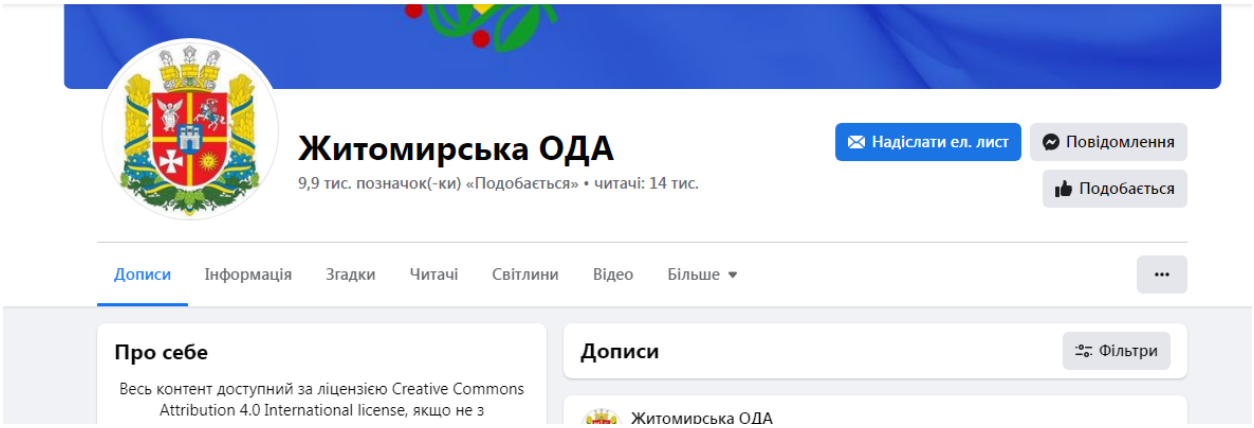

Рис. 2.4. Сторінка Житомирської ОВА у соціальній мережі Facebook

Джерело: побудовано автором за [17]

7. Електронні системи моніторингу та звітності: Житомирська ОВА може мати системи моніторингу та звітності, які допомагають відстежувати та

оцінювати різні аспекти роботи адміністрації, наприклад, фінансову звітність, стан виконання проектів тощо.

Важливо зазначити, що конкретні інформаційні ресурси та системи, що використовуються Житомирською ОВА, визначені внутрішніми процедурами та політикою адміністрації, а також залежать від доступності технічних засобів та ресурсів.

Отже, Житомирська ОВА володіє різноманітними інформаційними ресурсами, які використовуються для забезпечення діяльності організації. Ці ресурси включають електронні бази даних, документи, звіти, внутрішню інформацію та інші матеріали, необхідні для ефективного функціонування Житомирської ОВА. Інформаційні ресурси Житомирської ОВА мають свою характеристику, включаючи рівень конфіденційності, доступність та актуальність. Завдяки цим ресурсам забезпечується обмін інформацією між різними структурними підрозділами, координація дій та прийняття рішень.

Житомирська ОВА активно використовує інформаційні ресурси для виконання своїх завдань, включаючи планування, аналіз, прийняття рішень та забезпечення комунікації внутрішньої та зовнішньої. Ці ресурси важливі для забезпечення ефективного функціонування Житомирської ОВА та досягнення її поставлених цілей.

ЖОВА вкладає значні зусилля в забезпечення інформаційної безпеки. Організація використовує електронний цифровий підпис (ЕЦП) для підписування електронних документів, що сприяє визначенню їх автентичності та запобіганню несанкціонованому доступу.

Важливою складовою інформаційної безпеки є наявність електронних систем управління документами (СЕДО), які допомагають ефективно керувати обігом інформації та забезпечувати її захист від втрати або несанкціонованого доступу. Впровадження інформаційних баз даних сприяє надійному зберіганню різноманітних даних, таких як бюджетні звіти, проекти та статистична інформація.

Система електронної пошти та електронних скриньок забезпечує безпечний зв’язок із громадянами, підприємствами та іншими організаціями, де застосовуються сучасні заходи шифрування для захисту від несанкціонованого доступу до персональних даних. Усі ці заходи підтримують безпеку електронних сервісів та порталів, які використовуються для подання звернень, отримання інформації, реєстрації та оплати послуг. Дані про високий відсоток використання електронною поштою (92%) для звернень свідчать про успішну інтеграцію електронних сервісів та високий рівень довіри до них серед громадян.

Окрім того, ЖОВА має соціальні медіа-присутність у Facebook та Telegram, що може вимагати спеціальних заходів безпеки для захисту інформації та забезпечення взаємодії з громадськістю без ризику конфіденційності. Загалом, Житомирська ОВА демонструє високий стандарт інформаційної безпеки, впроваджуючи сучасні технології та забезпечуючи відповідність нормативам та вимогам у цій сфері.

Отже, Житомирська ОВА ефективно використовує електронний цифровий підпис та системи електронного документообігу для забезпечення автентичності та захисту інформації. Важливою є роль електронної пошти, електронних сервісів та соціальних мереж у взаємодії з громадськістю. Застосування інформаційних баз даних та сучасних технологій в ЖОВА свідчить про високий стандарт інформаційної безпеки, необхідний для ефективного управління та забезпечення надійності інформаційних ресурсів.

2.2. Особливості управління інформаційними ресурсами та інформаційною безпекою Житомирської ОВА

Управління інформаційними ресурсами Житомирської адміністрації включає ряд дій та процесів, спрямованих на ефективне збереження, обробку та використання інформації.

Основні аспекти управління інформаційними ресурсами можуть включати наступне:

1. Створення політики управління інформацією. Житомирська адміністрація розробила політику, яка визначає правила, процедури та відповідальності стосовно управління інформаційними ресурсами. Це включає вимоги до збереження документів, безпеки інформації, розподілу обов'язків та доступу до інформації.

2. Системи електронного документообігу та управління документами. Адміністрація використовує спеціальні системи електронного документообігу для збереження, обробки та керування офіційною документацією. Ці системи включають функції реєстрації, архівації, пошуку та контролю доступу до документів.

3. Забезпечення безпеки інформації. ЖОВА приділяє увагу заходам безпеки інформації для запобігання несанкціонованому доступу, витоку чи пошкодженню важливої інформації. Це може включати використання шифрування, бекапів, встановлення прав доступу та інших технічних заходів безпеки.

4. Розвиток та підтримка інформаційних систем. Адміністрація веде роботу з розробки, впровадження та підтримки інформаційних систем, які використовуються для обробки та аналізу інформації.

5. Технічна інфраструктура. Для ефективного управління інформаційними ресурсами, Житомирська адміністрація забезпечує належну технічну інфраструктуру, включаючи комп'ютери, сервери, мережеве з'єднання та інші необхідні засоби. Вона забезпечує їх належну роботу, безпеку та оновлення.

Зазначимо, що ЖОВА досить непогано на сьогодні забезпечена комп'ютерною, обчислювальною та периферійною технікою. Розподіл комп'ютерної техніки по категоріях, забезпеченість обчислювальною та периферійною технікою облдержадміністрації наведено в табл. 2.2 – 2.4.

Таблиця 2.2

Розподіл комп'ютерної техніки ЖОВА по категоріях 2016–2021 рр.

Роки	2016	2017	2018	2019	2020	2021
Загальна кількість комп'ютерів, одиниць	522	550	639	783	805	819
Кількість автоматизованих робочих місць, одиниць	239	266	311	429	464	482
Загальна кількість серверів, одиниць	15	17	19	22	25	25

Джерело: складено автором за даними [17]

Бачимо, що за останні 6 років загальна кількість комп'ютерів збільшилася на 297 одиниць; кількість автоматизованих робочих місць зросла на 243 одиниці, а загальна кількість серверів збільшилася на 10 одиниць.

Таблиця 2.3

Забезпеченість державних службовців ЖОВА обчислювальною технікою станом на 31.12.2021 р.

Найменування пристрою	Застаріла (та, яку вироблено понад 5 років тому)	Сучасна	Поповнення (та, яку було поставлено на баланс після 01.01.2021р.)	Та, що не використовується (підлягає списанню)
Стаціонарні комп'ютери	372	325	23	91
Ноутбуки	3	18	7	2
Сервери	16	15	0	1
Разом	391	358	30	94

Джерело: складено автором за даними [17]

Тут також відмічаємо, що 91% всієї обчислювальної техніки ЖОВА – це сучасні комп'ютери (325 од.), ноутбуки (18 од.) та 15 серверів.

Впродовж 2021 року на баланс ЖОВА поставлено 30 одиниць обчислювальної тезки для роботи державних службовців установи.

Серед периферійних пристроїв, якими користуються державні службовці ЖОВА – 10 сканерів та 106 принтерів (табл. 2.4).

Таблиця 2.4

Забезпеченість державних службовців ЖОВА периферійними пристроями станом на 31.12.2021 р.

Найменування пристрою	Сумарно, одиниць
Багатофункціональні пристрої	22
Сканери	10
Принтери	106

Джерело: складено автором за даними [17]

Що стосується підключення до мережі Інтернет, то тут зазначимо, органи які є підпорядковані апарату облдержадмінастрації і користуються мережею Інтернет сягає 100%, а ось в структурних підрозділах облдержадміністрації – 80% (табл. 2.5).

Таблиця 2.5

Доступ державних службовців ЖОВА до локальної обчислювальної мережі та мережі Інтернет на 31.12.2021 р.

Доступ	Сумарно, одиниць
Під'єднано до ЛОМ	578
Мають доступ до мережі Інтернет	470

Джерело: складено автором за даними [17]

6. Збереження та архівування інформації. Важлива частина управління інформаційними ресурсами – це забезпечення належного збереження та архівування інформації. Адміністрація розробила політику збереження документів та встановила процедури для їх зберігання.

7. Навчання та підготовка персоналу. Ефективне управління інформаційними ресурсами вимагає наявності кваліфікованого персоналу. Адміністрація забезпечує навчання та підготовку співробітників щодо правильного використання інформаційних систем, безпеки даних та дотримання політики управління інформацією.

Тут варто зазначити, що загалом персонал Житомирської ОВА має невисоку цифрову грамотність. Значний відсоток службовців – це люди старшого покоління, яким досить важко дається нові інформаційні технології.

Разом з тим, працівники ОВА постійно вдосконалюють свою цифрову грамотність на різноманітних курсах та навчаннях.

Статистика свідчить про те, що в 2021 році навчання цифровій грамотності на курсі «Цифрова грамотність для державних службовців» пройшли 22 службовці Житомирської обласної адміністрації різних категорій.

8. Моніторинг та оцінка. Для ефективного управління інформаційними ресурсами, Житомирська адміністрація періодично проводить моніторинг та оцінку використання інформаційних систем, ефективності процесів та рівня безпеки. Це дає змогу виявляти можливі проблеми та вживати заходи для їх вирішення та покращення роботи.

Що стосується управління інформаційною безпекою в Житомирській обласній військовій адміністрації, то його особливості визначаються контекстом роботи цієї адміністрації та особливостями українського публічного сектору:

1. Специфіка державної діяльності. Управління інформаційною безпекою в ЖОВА пов’язане з виконанням державних функцій, включаючи збереження та обробку конфіденційної інформації, тож особливий акцент робиться на запобіганні несанкціонованому доступу та збереженні цілісності даних.

2. Високий рівень конфіденційності. Оскільки ЖОВА взаємодіє з різними видами чутливої інформації, управління інформаційною безпекою націлене на збереження високого рівня конфіденційності та запобігання витокам даних.

3. Використання сучасних технологій. Для забезпечення ефективності та захищеності інформаційних ресурсів ЖОВА використовує сучасні технології, включаючи шифрування, інтегровані системи безпеки та інші заходи.

4. Регулярні аудити та перевірки. Організація проводить регулярні аудити та перевірки інформаційних систем для виявлення можливих слабких місць та вдосконалення заходів безпеки.

5. Взаємодія з іншими організаціями. З огляду на співпрацю та обмін інформацією з іншими державними структурами, ЖОВА активно залучається

до розробки та дотримання загальнодержавних стандартів інформаційної безпеки.

6. Фокус на ризиках та невідповідності. Управління інформаційною безпекою в ЖОВА орієнтоване на виявлення та зменшення ризиків, а також дотримання законодавства та внутрішніх політик щодо інформаційної безпеки.

7. Адаптація до змін в загрозах. З огляду на постійні зміни в сфері кібербезпеки, ЖОВА відзначається готовністю та здатністю адаптувати свої стратегії та заходи безпеки до нових загроз та викликів.

8. Інтеграція інформаційної безпеки в управлінські процеси: Управління інформаційною безпекою в ЖОВА вбудоване в усі рівні управлінської структури, що дозволяє забезпечити цілісний та системний підхід до збереження та захисту інформації.

Висновки до розділу 2

Отже, управління інформаційними ресурсами та інформаційною безпекою в Житомирській ОВА визначається високим рівнем конфіденційності та специфікою державної діяльності. Особливості цього процесу включають ретельно розроблену політику збереження та архівування інформації, акцент на навчанні персоналу з урахуванням різниці в цифровій грамотності, систематичні моніторинги та оцінки ефективності, а також інтеграцію інформаційної безпеки в усі рівні управлінської структури. Заходи, спрямовані на адаптацію до змін в кібербезпеці та впровадження новітніх технологій, свідчать про високий ступінь готовності ЖОВА до ефективного та безпечного управління інформаційними ресурсами.

РОЗДІЛ 3.
НАПРЯМИ МОДЕРНІЗАЦІЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ДЕРЖАВИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

3.1. Зарубіжний досвід публічного управління у сфері інформаційної безпеки держави

Зарубіжний досвід у сфері публічного управління інформаційною безпекою держави свідчить про необхідність поєднання технологічних інновацій, стратегічного планування та ефективних політичних рішень для забезпечення стійкості та захищеності національної кіберінфраструктури. Визначаючи оптимальні моделі управління, країни успішно інтегрують сучасні підходи до кібербезпеки в державні стратегії, реагуючи на постійно зростаючі виклики та загрози в цифровому просторі.

Абсолютно логічним є наведення у першу чергу досвіду забезпечення інформаційної безпеки, який накопичено найбільш впливовою в політико-економічному і військовому відношенні державі – Сполучених Штатах Америки (США). В аспекті забезпечення інформаційної безпеки США можна вважати піонерами, адже це не лише держава, яка уперше у світі запровадила електронне урядування з використанням новітніх інформаційних технологій, а й створила особливу систему захисту національного інформаційного суверенітету і безпеки інформаційних ресурсів.

Переходячи безпосередньо до характеристики системи американської моделі адміністрування інформаційної безпеки, слід зауважити, що у США функціонує кілька інституцій забезпечення інформаційної безпеки: Агентство національної безпеки (АНБ), Національне управління кібербезпеки міністерства внутрішньої безпеки США, Федеральне бюро розслідувань (ФБР), Центральне розвідувальне управління (ЦРУ). Слід зазначити, що серед державних інституцій забезпечення інформаційної безпеки АНБ розвиває також партнерство з приватним сектором і науковими установами у вигляді

планування заходів протидії загрозам у неурядових комп'ютерних мережах (таким чином держава бере участь у захисті найважливіших приватних телекомунікаційних, електричних, банківських мереж (телекомунікації, електромережі, мережі банківських розрахунків, інтернет-провайдери). АНБ залучає до проведення дії з захисту від тероризму приватні установи і громадські організації (CERT, ISACA, CSX, CCSIS). Експерти зауважують, що на сьогодні в США у забезпеченні інформаційної безпеки задіяно більш ніж 150 державних організацій і ще більша кількість приватних, які координуються АНБ [38].

Разом із тим, найважливішою інституцією, яка здійснює державне регулювання інформаційною безпекою є Президент США. Чинні сьогодні організаційно-правові засади захисту національного інформаційного простору беруть початок з інформаційного забезпечення політики безпеки та визискування систем оборони та системою управління в інтересах вищих органів державної влади [38].

Основні законодавчі засади забезпечення інформаційної безпеки США було сформовано після другої світової війни, коли американська інформаційна система зіштовхнулася з деструктивним впливом радянської пропаганди. Структурно законодавство США у сфері забезпечення інформаційної безпеки складається як з федеральних законів, так і законів штатів. Незважаючи на існуючи істотні відмінності законів штатів, акти інформаційного законодавства є одними із найбільш уніфікованих, адже в американському суспільстві існує розуміння того, що інформаційна безпека держави є запорукою безпеки кожного громадянина.

Правову основу адміністрування інформаційної безпеки США становлять закони «Про охорону особистих таємниць» (1974 р.), «Про таємницю» (1974 р.), «Про висвітлення діяльності уряду», «Про право на фінансову таємницю» (1978 р.), «Про доступ до інформації про діяльність ЦРУ» (1984 р.), «Про безпеку комп'ютерних систем» (1987 р.), «Про комп'ютерне шахрайство та зловживання» (1986 р.) [38].

За ініціативи Президента США Р. Рейгана було розроблено та ухвалено Закон «Про свободу інформації», а забезпечення інформаційної безпеки стало пріоритетним завданням політики Державного департаменту. Пізніше, у 1987 р. прийнято Закон Mb HR-145 «Про забезпечення безпеки ЕОМ», норми якого лягли в основу майбутнього законодавства про кібернетичну безпеку. Цим законом уперше у правовій системі США регламентовано статус нового інституту – «інформації обмеженого доступу», під якою американські спеціалісти розуміють несекретну, але важливу з точки зору національної безпеки несекретну інформацію урядових відомств, а також інформаційні дані, що формуються і поширюються або опрацьовуються в інформаційно-телекомунікаційних системах корпорацій та приватних фірмах, що працюють за замовленням уряду США.

Окрім законів важливе значення для інформаційної безпеки США мають Директиви Президента США, який очолює Раду національної безпеки. Найважливішими серед них є: Директива PD/NSC-24 1977 р. «Політика в галузі захисту систем зв'язку», Директива SDD –145 1984 р. «Національна політика США в галузі безпеки систем зв'язку в автоматизованих інформаційних системах».

Як і сусідні США, Канада сьогодні також приділяє значну увагу регулюванню забезпеченню інформаційної безпеки і проводить системну комплексну політику щодо її реалізації. У Канаді держава є головним суб'єктом управління всіма інформаційними потоками в суспільстві та забезпечення інформаційної безпеки. У порівнянні з низкою інших держав участь громадянського суспільства у відповідних процесах є мінімальною, що обумовлено високим ступенем довіри громадян до держави. Уряд сьогодні досяг значних успіхів в оптимальному правовому регулюванні всіх інформаційних відносин і процесів. На сьогодні політика регулювання інформаційної безпеки Канади визнається показовою багатьма державами та міжнародними організаціями у світі. Слід зазначити, що інформаційна безпека Канади є невід'ємною частиною побудови інформаційного суспільства в

державі. Питання про інформаційну безпеку актуалізувалося в Канаді на початку 1990-х років, коли спостерігалося стрімке зростання комп'ютеризації та інформатизації суспільних і управлінських процесів. У 1993 р. Центр безпеки національного відомства безпеки зв'язку Канади розробив «Канадські критерії безпеки комп'ютерних систем», які передбачали розробку цільної системи порівнянь для можливості протиставлення різних систем обробки інформації, яка відображалась за певним ступенем та критеріями безпеки, при якій було створено основи для створення специфікацій безпечних комп'ютерних систем, розробку уніфікованого підходу і стандартних засобів для опису характеристик безпечних комп'ютерних систем [38].

Основним досягненням Канади в адмініструванні інформаційної безпеки держави є створення «Інформаційної магістралі» – стратегічного документа, затвердженого урядом, який передбачає адміністративно-правові і технічні заходи, спрямовані на забезпечення автентичності інформації, що міститься в інформаційних мережах, виробничій сфері, надання публічних і приватних послуг та ін. у 1994 р було засновано Консультативна Рада з інформаційної магістралі, яка на постійній основі розробляє та вносить пропозиції щодо удосконалення нормативної основи забезпечення інформаційної безпеки в державі.

Основним об'єктом охорони системи забезпечення інформаційної безпеки Канади є електронної уряд, який відкриває для громадян широкі можливості щодо взаємодії з державою за допомогою доступного і рівного доступу до публічних послуг.

У сусідній Франції система державного регулювання забезпечення інформаційної безпеки є дещо схожою на німецьку. Взагалі, французька практика показує зведення інформаційної безпеки просто до забезпечення Францією кібернетичної безпеки і безпеки даних Інтернету. Якщо розглядати детально, ми можемо побачила що загалом Франція немає окремих спеціалізованих правових актів, які б могли регулювати роботу спеціалістів в роботі з інформацією. Слід зазначити, що порушення безпеки державної

таємниці несе за собою кримінальну відповідальність, а порушення безпеки персональної інформації та комерційної таємниці буде нести за собою кримінальну, трудову та цивільну.

В основі управлінської французької національної моделі інформаційної безпеки – готовність до ведення інформаційної війни як у цивільній площині, так і по лінії військового відомства. Так як інформаційна війна є важливим питанням для даної країни, військова складова передбачає обмежену роль інформаційних операцій [38].

В свою чергу, цивільний компонент передбачає більш широкий діапазон застосування спеціальних адміністративних інформаційних заходів, спрямованих на недопущення втручання у бази даних державних установ, підприємств, організацій, недопущення розголошення персональних даних та ін. Особливе місце у політиці інформаційної безпеки Франції посідає протидія інформаційним загрозам у сфері економіки. Французькі експерти з питань безпеки висловлюють всі погляди , тому їхні підходи допускають, що союзники держави можуть також бути одночасно і об’єктом інформаційної війни.

З інституційної точки зору, протидія загрозам інформаційному середовищу у Франції традиційно здійснюється на місцях поліцейськими управліннями. При кожному регіональному французькому поліцейському управлінні існує спеціальний відділ по боротьбі зі злочинами у сфері інформаційних технологій [38].

«Яскравою» особливістю такого підходу є те, що інформаційною безпекою займаються не лише вузькопідготовлені спеціалісти, а й фінансисти, юристи, аудитори та ін. Причиною цього є розвиток електронної комерції у Республіці. Незважаючи на значні фінансові витрати на це, такий підхід дає позитивні результати: на сьогодні у Франції практично не вчиняються шахрайські дії з банківськими картками.

Окрім цього, нещодавно у Франції було створено Центр електроніки і озброєнь (CELAR). Це орган, який займається широким спектром питань, в

тому числі: проблемами електронної війни, інформаційних систем, телекомунікацій, інформаційної безпеки та електронних компонентів.

Отже, зарубіжний досвід публічного управління у сфері інформаційної безпеки свідчить про важливість поєднання технологічних інновацій, стратегічного планування та ефективних політичних рішень для забезпечення стійкості національної кіберінфраструктури.

Зокрема, досвід Сполучених Штатів Америки вказує на необхідність існуючого партнерства між державними установами, приватним сектором та науковими установами у сфері кібербезпеки. Використання широкого спектру правових інструментів, таких як закони, директиви Президента та партнерство з громадськістю, дозволяє забезпечити високий рівень захищеності інформації в цифровому просторі.

Також, німецькомовні країни, такі як Німеччина та Австрія, активно застосовують інтегровані підходи до управління інформаційною безпекою, враховуючи як аспекти кібербезпеки, так і захист економічної інформації. Ці практики визнані світовими гравцями і можуть слугувати прикладом для розвитку ефективних стратегій інформаційної безпеки в інших країнах.

3.2. Шляхи удосконалення управління інформаційними ресурсами Житомирська ОВА

Умови гібридної війни визначають необхідність сучасної модернізації інформаційної політики держави. Зі зростанням викликів у цифровому просторі та активізацією гібридних загроз, стратегічний розвиток інформаційної політики стає критичним для забезпечення національної безпеки та відповіді на сучасні виклики. На нашу думку, існує кілька шляхів удосконалення управління інформаційними ресурсами Житомирська ОВА:

1. Розвиток і впровадження сучасних інформаційних технологій. Цей пункт передбачає використання новітніх інформаційних систем, програмного

забезпечення та технологій, які дозволять автоматизувати різні аспекти управління інформаційними ресурсами. Наприклад, це може включати впровадження системи електронного документообігу, централізованого сховища даних, системи моніторингу мережі тощо. Це допоможе забезпечити ефективний обмін інформацією, швидкий доступ до ресурсів та полегшить процеси прийняття управлінських рішень.

2. Навчання та підвищення кваліфікації працівників. Для ефективного управління інформаційними ресурсами необхідно мати кваліфікований персонал, який розуміє сучасні методи та підходи до управління інформацією. Організація навчань, семінарів та тренінгів для працівників Житомирської ОВА є ключовим аспектом. Це дасть змогу їм оволодіти новими навичками, оновити свої знання та працювати більш ефективно з інформаційними ресурсами.

3. Система контролю використання інформаційних ресурсів. Організація ефективної системи контролю є важливим кроком для забезпечення безпеки та використання інформаційних ресурсів відповідно до встановлених стандартів. Житомирська ОВА може розглянути впровадження системи моніторингу та аудиту використання інформаційних ресурсів, яка дасть змогу відстежувати доступ до даних, контролювати виконання політик безпеки, виявляти потенційні загрози та ризики. Це забезпечить високий рівень захищеності інформаційних ресурсів та допоможе вчасно реагувати на можливі вразливості.

4. Розробка стратегії та політик управління інформаційними ресурсами. Важливим кроком удосконалення управління інформаційними ресурсами є розробка стратегії, яка визначатиме основні цілі, завдання та напрямки розвитку інформаційного середовища Житомирської ОВА. Також варто розглянути створення політик, що визначатимуть правила використання, доступу та захисту інформаційних ресурсів. Це сприятиме стандартизації процесів управління та забезпечить їх послідовність.

5. Співпраця зі сторонніми експертами та організаціями. Для досягнення високих результатів у управлінні інформаційними ресурсами, Житомирська ОВА може встановити партнерські відносини зі спеціалізованими експертами

та організаціями, які мають досвід у цій галузі. Це може включати залучення консультантів з інформаційної безпеки, проведення аудитів та оцінку поточного стану інформаційних ресурсів.

Варто зазначити, що серед основних проблем забезпечення інформаційної безпеки системи Житомирська ОВА наступні:

– відсутність усталеного поняття «інформаційна безпека». Це вказує на неоднозначність та недостатню узгодженість у розумінні та визначенні поняття «інформаційна безпека». Відсутність чіткого визначення може ускладнювати розробку та впровадження ефективних стратегій і політик інформаційної безпеки;

– недієвий механізм функціонування системи електронного врядування. На даний момент система електронного врядування не працює в повному обсязі. Це може створювати проблеми з обробкою та зберіганням інформації, доступом до неї та забезпеченням її безпеки;

– формування інноваційних інформаційних загроз. Швидкий технологічний прогрес призводить до появи нових типів загроз та ризиків, пов’язаних з інформаційною безпекою. Ці загрози потребують термінового та ефективного вирішення, але можуть бути складні для боротьби з ними;

– підготовка якісного кадрового складу. Забезпечення інформаційної безпеки вимагає наявності кваліфікованого персоналу. Однак, формування такого кадрового складу може бути викликом, так як вимагає спеціалізованих знань і навичок у сфері інформаційної безпеки;

– відсутність дієвих механізмів забезпечення інформаційної безпеки. Недостатня наявність ефективних механізмів та інструментів для забезпечення інформаційної безпеки може створювати прогалини та вразливості у системі публічного управління. Це може включати недостатню захищеність мереж, слабкі паролі, відсутність систем резервного копіювання та відновлення даних, недостатнє оновлення програмного забезпечення та апаратних засобів тощо;

– відсутність комплексних інституцій забезпечення системи інформаційної безпеки. Для успішного забезпечення інформаційної безпеки в

публічному управлінні необхідно наявність комплексних інституцій, які будуть відповідальні за планування, розробку та впровадження стратегій, політик і механізмів забезпечення інформаційної безпеки. Ці інституції повинні мати достатні ресурси, авторитет та координаційні здібності для ефективного виконання своїх функцій.

Висновки до розділу 3

Таким чином, удосконалення управління інформаційними ресурсами Житомирської ОВА є стратегічним завданням, спрямованим на забезпечення національної безпеки та відповідь на виклики гібридної війни в цифровому просторі. Розвиток та впровадження сучасних інформаційних технологій, навчання та підвищення кваліфікації персоналу, система контролю використання інформаційних ресурсів, розробка стратегії та політик, а також співпраця зі сторонніми експертами становлять ключові елементи цього процесу.

Ці заходи сприятимуть ефективному впровадженню інновацій, підвищать рівень інформаційної безпеки та забезпечать високу готовність до вирішення викликів, що виникають у сучасному цифровому середовищі.

ВИСНОВКИ

Таким чином, дослідивши особливості публічного управління у сфері інформаційної безпеки держави, ми дійшли наступних висновків:

1. Ознайомившись із понятійно-категоріальним апаратом інформаційної безпеки держави, можемо сказати, що інформаційна безпека держави – це важлива функція держави, яка має невід'ємну складову національної безпеки країни, включаючи становище яке відповідає щодо захисту інформаційного простору. В роботі було вказано окремі стани які є центральними в питанні безпеки інформаційного середовища, першочергово можна виокремити процес який відповідає за управління загрозами та можливими небезпеками, він спеціалізується на забезпечені інформаційного суверенітету держави та захищеності встановлених законом правил, відповідно яким здійснюються інформаційні процеси в державі.

2. Розглянувши інформаційний ресурс, як найважливіший ресурс держави, ми з'ясували, що даний ресурс визнається найважливішим для держави, оскільки він є основою для розвитку, прийняття управлінських рішень та забезпечення національної безпеки. Його значення полягає в підтримці національних інтересів, прав людини та основних свобод, а також ефективному функціонуванні суспільства та державних органів. Як ключовий компонент суверенітету, інформаційний ресурс має визначальний вплив на різні аспекти економіки, науки, культури та інших галузей діяльності. Забезпечення його якості, захисту та ефективного використання стає стратегічним завданням для держави в умовах сучасного інформаційного суспільства.

3. Дослідивши поняття та завдання управління інформаційними ресурсами держави у сфері інформаційної безпеки держави, ми вияснили, що управління інформаційними ресурсами держави у сфері інформаційної безпеки є невід'ємною складовою ефективного функціонування сучасного суспільства. Це включає в себе впровадження технологічних заходів, розробку стратегій та політик, які спрямовані на забезпечення конфіденційності, цілісності та

доступності інформації державних інформаційних ресурсів. Основні завдання управління включають реалізацію ефективних заходів кіберзахисту, розробку політики безпеки та створення інфраструктури, яка забезпечує відповідність вимогам сучасного цифрового середовища. Ці заходи не лише забезпечують захист інформаційних ресурсів держави, але й сприяють підвищенню рівня прозорості, демократії та ефективності державного управління в цілому.

4. Оцінивши інформаційні ресурси Житомирської ОВА, ми дійшли висновку, що Житомирська ОВА ефективно використовує електронний цифровий підпис та системи електронного документообігу для забезпечення автентичності та захисту інформації. Важливою є роль електронної пошти, електронних сервісів та соціальних мереж у взаємодії з громадськістю. Застосування інформаційних баз даних та сучасних технологій в ЖОВА свідчить про високий стандарт інформаційної безпеки, необхідний для ефективного управління та забезпечення надійності інформаційних ресурсів.

5. Дослідивши особливості управління інформаційними ресурсами та інформаційною безпекою Житомирської ОВА, ми зрозуміли, що управління визначається високим рівнем конфіденційності та специфікою державної діяльності. Особливості цього процесу включають ретельно розроблену політику збереження та архівування інформації, акцент на навчанні персоналу з урахуванням різниці в цифровій грамотності, систематичні моніторинги та оцінки ефективності, а також інтеграцію інформаційної безпеки в усі рівні управлінської структури. Заходи, спрямовані на адаптацію до змін в кібербезпеці та впровадження новітніх технологій, свідчать про високий ступінь готовності ЖОВА до ефективного та безпечного управління інформаційними ресурсами.

6. Ознайомившись із зарубіжним досвідом публічного управління у сфері інформаційної безпеки держави, ми дійшли висновку, що такий досвід свідчить про важливість поєднання технологічних інновацій, стратегічного планування та ефективних політичних рішень для забезпечення стійкості національної кіберінфраструктури.

Зокрема, досвід Сполучених Штатів Америки вказує на необхідність існуючого партнерства між державними установами, приватним сектором та науковими установами у сфері кібербезпеки. Використання широкого спектру правових інструментів, таких як закони, директиви Президента та партнерство з громадськістю, дозволяє забезпечити високий рівень захищеності інформації в цифровому просторі.

Також, німецькомовні країни, такі як Німеччина та Австрія, активно застосовують інтегровані підходи до управління інформаційною безпекою, враховуючи як аспекти кібербезпеки, так і захист економічної інформації. Ці практики визнані світовими гравцями і можуть слугувати прикладом для розвитку ефективних стратегій інформаційної безпеки в інших країнах.

7. Обґрунтувавши шляхи удосконалення управління інформаційними ресурсами Житомирська ОВА, можемо сказати, що удосконалення управління інформаційними ресурсами Житомирської ОВА є стратегічним завданням, спрямованим на забезпечення національної безпеки та відповідь на виклики гібридної війни в цифровому просторі. Розвиток та впровадження сучасних інформаційних технологій, навчання та підвищення кваліфікації персоналу, система контролю використання інформаційних ресурсів, розробка стратегії та політик, а також співпраця зі сторонніми експертами становлять ключові елементи цього процесу. Ці заходи сприятимуть ефективному впровадженню інновацій, підвищать рівень інформаційної безпеки та забезпечать високу готовність до вирішення викликів, що виникають у сучасному цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бугайчук К., Шорохова Г. Забезпечення кібербезпеки як умова протидії терористичній діяльності: нормативно-правові аспекти. *Протидія терористичній діяльності: міжнародний досвід і його актуальність для України :* матеріали II Міжнародної науково-практичної конференції (15.12.2017). Київ : Національна академія прокуратури Україну. С. 135–138.

2. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. / за ред. О. М. Суходолі. Київ: НІСД, 2020. 28 с.

3. Довгань О.Д. Інформаційні ресурси: національні та державні, зміст, поняття. *Інформація і право*. 2015. №3. С. 85–91.

4. Єрменчук О. П. Складові національної інфраструктури. Науковий вісник ДДУВС. 2017. № 4. С. 109–115.

5. 8. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монограф. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

6. Клочко А. Забезпечення інформаційної безпеки в умовах сучасного суспільства. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2022. №3(63). С. 38–42. URL: https://doi.org/10.32689/2523-4625-2022-3(63)-6 (дата звернення: 29.11.2023).

7. Конституція України, прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 р. / Верховна Рада України. Київ: Преса України, 1997. 80 с.

8. Концепція створення та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів : Розпорядження Кабінету Міністрів України від 05.09.12 р. № 634-р. URL : http://zakon2.rada.gov.ua/laws/show/634-2012-%D1%80 (дата звернення: 24.11.2023).

9. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : дис. … д-ра юрид. наук: спец. 12.00.07. Одеса, 2004. 427 с.

10. Кулицький С.П. Основи організації інформаційної діяльності у сфері управління: навч. посібник. Київ: МАУП, 2002. 224 с.

11. Марутян Р. Національні інформаційні ресурси як першооснова інформаційного суверенітету України. *Актуальні проблеми міжнародної безпеки : український вимір.* Київ : ВД «Стилос», 2020. 496 с.

12. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.

13. Нижник Н., Ситник Г., Нижник В. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : навчальний посібник. Ірпінь, 2000. 234 с.

14. Новородовський В. Інформаційна безпека України в умовах Російської агресії. *Соціум. Документ. Комунікація*. 2020. Вип. 9. С. 150-179

15. Олійник О. Принципи забезпечення інформаційної безпеки України. *Юридичний вісник повітряне і космічне право*. 2016. № 4(41). С. 72–78.

16. Онищенко О., Горовий В., Попик І. Національні інформаційні ресурси як інтегративний чинник вітчизняного соціокультурного середовища : монографія. Національна бібліотека України ім. В. І. Вернадського. Київ, 2014. 324 с.

17. Офіційний сайт ЖОВА. URL : https://oda.zht.gov.ua/ . (дата звернення: 23.11.2023).

18. Приймак Ю.Ю. Національні інформаційні ресурси – джерело державних інформаційних продуктів та послуг. *Державне управління : теорія та практика.* 2019. № 2. URL: www.academy.gov.ua/ej/ej10/doc_pdf/Priymak.pdf (дата звернення: 23.11.2023).

19. Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : наказ Адміністрації Державної служби

спеціального зв'язку та захисту інформації України від 02.12.14 р. № 660. URL : http://zakon.rada.gov.ua/go/z0090-15 (дата звернення: 23.11.2023).

20. Про власність : Закон України від 7 лютого 1991 р. № 697-X11 URL : http://zakon4.rada.gov.ua/laws/show/697-12. (дата звернення: 24.11.2023).

21. Про Державну службу спеціального зв'язку та захист інформації України : Закон України. URL : http://zakon2.rada.gov.ua/laws/show/3475-15. (дата звернення: 24.11.2023).

22. Про інформацію: закон України від 02.10.1992 р. URL : https://zakon.rada.gov.ua/laws/main/2657-12#Text (дата звернення: 22.11.2023).

23. Про Концепцію Національної програми інформатизації : Закон України від 1998 р. *Відомості Верховної Ради України (ВВР).* 1998. № 27–28. Ст. 182.

24. Про науково-технічну інформацію : Закон України №3322-X11 від 25 червня 1993 р. URL : http://zakon4.rada.gov.ua/laws/show/3322-12. (дата звернення: 23.11.2023).

25. Про Національну програму інформатизації : Закон України від 4 лютого 1998 р. № 74/98-ВР. URL : http://zakon4.rada.gov.ua/lawws/74/98-%D0%B2%D1%80. (дата звернення: 10.05.2023).

26. Про рішення Ради національної безпеки і оборони України від 15.10.2021 р. «Про Стратегію інформаційної безпеки» : указ Президента ННІНО НАУ Інформаційна безпека України від 28.12.2021 р. URL : https://zakon.rada.gov.ua/laws/show /685/2021#n14 (дата звернення: 21.11.2023).

27. Романов І.В., Рижов І.М., Тонконог І.О. Методологія комплексного оцінювання розвитку національних інтересів України в секторі економічної та державної безпеки. *Інформаційна безпека людини, суспільства, держави.* 2019. № 3 (27). URL: http://academy.ssu.gov.ua/ua/page/page_1581426025.htm (дата звернення: 12.12.2023).

28. Саган О.В. Протидія медіа-інформаційному тероризму як питання національної безпеки України : автореф. дис. … канд. політ. наук: 21.01.01.

Київ, 2021. 22 с. URL: https://niss.gov.ua/sites/default/files/2021-04/06.04.2021_1-avtorefer_pidpis.-sagan_sig.pdf (дата звернення: 09.12.2023).

29. Семенець-Орлова І., Клочко А., Амро, Т. Публічне управління у сфері інформаційної безпеки для забезпечення розвитку демократії в Україні (контекст воєнного стану). 2022. № 5 (33). С. 73–82. DOI: https://doi.org/10.32689/2617-2224-2022-5(33)-10

30. Соснін О.В. Національні інформаційні ресурси : проблеми визначення і розуміння. *Стратегічна панорама*. 2014. № 4. С. 141–146.

31. Стратегії розвитку України : теорія і практика; за ред. О.С. Власюка. Київ : НІСД, 2002. 864 с.

32. Стратегія інформаційної безпеки: затверджена Указом Президента України від 28 грудня 2021 року № 685/2021.

33. Хорошко В., Хохлачова Ю., Пірцхалава Т., Іванченко І. Інформаційна зброя як інструмент інформаційної війни. *Захист інформації.* 2022. Том 24, № 2. С. 50–58. URL: https://jrnl.nau.edu.ua/index.php/ZI/article/view/16930 (дата звернення: 25.11.2023).

34. Хоффман Л. Дж. Сучасні методи захисту інформації / пер. з англ. Київ : Світанок, 1983. 57 с.

35. Цимбалюк В.С., Гавловський В.Д., Гриценко В.В. та ін. Основи інформаційного права України [навч. посіб.]. Київ: Знання, 2004. 274 с.

36. Шпакова О. Политика информационной безопасности в Украине : правовой базис. *Актуальні проблеми міжнародних відносин*. 2018. Вип. 65 (Ч. 1). С. 242–249.

37. Юдін О.К., Бучик С.С. Концептуальний аналіз уразливості державних інформаційних ресурсів. *Наукоємні технології*. 2019. № 3(19). 299–304.

38. Яковлєв П. О. Досвід державного регулювання забезпечення інформаційної безпеки зарубіжних держав (на прикладі Сполучених Штатів Америки, Канади, Німеччини, Франції). *Вісник Харківського національного*

університету імені В. Н. Каразіна. Серія «Право». 2020. №30. С. 106–113. URL: https://doi.org/10.26565/2075-1834-2020-30-13

39. Chala N.D., Poplavska O.M. Transforming the Relations between State and Society in the Context of the 4th Industrial Revolution: Ukraine's Experience. *Public Policy and Administration*. 2020. Vol 19. № 1. P. 89–98.

40. Chulitskaya T., Matonyte I. Social security discourses in a non-democratic state: Belarus between Soviet paternalistic legacies and neo-liberal pressures. *Public Policy and Administration*. 2020. Vol 17. № 4. P. 539–554.

41. Melnyk I. Principles of Formation of Information Policy of Ukraine In the Conditions of Hybrid War. *Krakowskie Studia MałopolskieIssue*. 2020. № 2 (26). P. 136–149. URL: https://doi.org/10.15804/ksm20200209 (дата звернення: 12.12.2023).

42. Лонська В. Г. Інформаційний ресурс як об’єкт управління. *Механізми управління розвитком територій* : збірник наукових праць учасників конференції (жовтень, 2023). Житомир: ПНУ. 2023. С. 165–170.

43. Лонська В.Г Зміст та характеристика державних інформаційних ресурсів. *Інструменти та практики публічного управління в контексті децентралізації* : збірник наукових праць учасників конференції (22-23 червня 2023 року). Житомир: ПНУ. 2023. С. 317–324.

44. Лонська В.Г., Русак В.В. Інформаційна безпека держави в умовах антитерористичних операцій та гібридної війни. *Студентські наукові читання – 2022* : наукова практична конференція за результатами 1 туру всеукраїнського конкурсу студентських наукових робіт (листопад 2022 року). Житомир : ПНУ. 2022. С. 80–83.