ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ
В.Н.КАРАЗІНА
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
«ІНСТИТУТ ДЕРЖАВНОГО УПРАВЛІННЯ»

До захисту
Завідувач кафедри права, національної безпеки
та європейської інтеграції
д.ю.н., професор Величко Лариса Юріївна
_____

ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ В УМОВАХ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Кваліфікаційна робота на здобуття освітнього ступеня «магістр»
281 Публічне управління та адміністрування
28 Публічне управління та адміністрування

Виконавець
Здобувач 2 курсу, групи ППГЗ-2-23 С. В. Богомолов

Науковий керівник
д.ю.н., доцент С. М. Клімова

Харків – 2024

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

CERT-UA – Урядова команда реагування на комп'ютерні надзвичайні події України

Держспецзв'язку – Державна служба спеціального зв'язку та захисту інформації України

Єдиний веб-портал – Єдиний веб-портал

ЄРД – Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань

Закон № 389 – Закон України «Про правовий режим воєнного стану» від 12.05.2015 р. № 389-VIII

Закон № 5203 – Закон України «Про адміністративні послуги» від 06.09.2012 № 5203-VI

КМУ – Кабінет Міністрів України

МКІП – Міністерство культури та інформаційної політики

ОДА – обласна державна адміністрація

ОДВ – органи державної влади України

ОМС – орган місцевого самоврядування

Портал – Єдиний державний вебпортал відкритих даних

ВСТУП

Актуальність дослідження полягає в тому, що швидкий розвиток інформаційних технологій в Україні значно впливає на всі сфери життя, зокрема на роботу правоохоронних органів. Впровадження сучасних ІТ-рішень дозволяє не лише підвищити ефективність боротьби зі злочинністю, але й покращити якість надання адміністративних послуг. Завдяки інформаційним системам правоохоронці отримують швидкий доступ до необхідних даних, що сприяє прийняттю обґрунтованих рішень і запобігає виникненню помилок.

Цифровізація тотально осягає різні сфери життєдіяльності людини, чим формує нові можливості та умови для нормативно-правового, політичного, економічного, соціального та іншого розвитку людини. Нові напрями діяльності, які переважною більшістю є інформаційними, несуть у собі певні ризики і загрози як нормативного регулювання, й у сформованої системи суспільного укладу. Завдяки інформації та інформаційним технологіям стимулюються корисні та позитивні зміни в суспільстві, що формують потребу у формуванні нових підходів до захисту інформації в Державній податковій службі України.

Відкритість, прозорість та підзвітність діяльності органів влади, залучення громадян до прийняття рішень є важливими цінностями відкритого врядування у демократичному суспільстві. Уряд України продовжує впроваджувати механізми відкритого врядування, незважаючи на військову агресію росії. Зусилля держави та громадянського суспільства об’єднуються для боротьби проти країни-агресорки та забезпечення демократичного майбутнього України.

До актуальних питань правового регулювання суспільних відносин у сфері використання інформаційних технологій також слід віднести: захист персональних даних, а також інформації, яка відноситься до державної чи

комерційної таємниці від так званих хакерських атак; протидію поширенню в Інтернеті культу насильства та жорстокості, дитячої порнографії та іншого забороненого законом контенту; запобігання використанню соціальних мереж, месенджерів для забезпечення діяльності злочинних організацій, включаючи терористичні та радикальні організації; використання інформаційних технологій та відповідних потужностей для так званого майнінгу – забезпечення функціонування криптовалютних платформ, що перевантажує електричні мережі та часто призводить до нецільового використання технологічних потужностей; забезпечення збереження цінної інформації на альтернативних цифрових носіях з метою її захисту від втрати, знищення (стирання); правове регулювання електронної торгівлі, включаючи питання її обліку, визначення вартості цифрових продуктів, оподаткування тощо (адже комп'ютерна програма може коштувати набагато більше, ніж декларується її автором чи покупцем); захист інтелектуальної власності, авторських прав в Інтернет [89, с.247].

Згідно зі звітом ООН, Україна посіла 69 місце серед 193 країн світу у рейтингу готовності до діяльності електронного уряду.

Наукова дослідженість питань інформаційного забезпечення правоохоронних органів встановлено у роботах таких авторів: В. Андрущенко, Г.Блінова, О. Блохіної, Л.Баранник, С.Клімова, В. Мігалатюк, Л. Ніколаєва, О.Сударенко та інші.

Інформаційна безпека стала предметом дослідження О. Данильяна, О. Дзьобаня, Ю. Калиновського, О. Каплі, Катерліна, А. Крупнової, Д. Олєйнікова, А. Ряполова, Т. Салаєва та інших.

Інформаційні права стали предметом досліджень таких учених: Ю.Базанов, А.Баранов, В. Білоус, І.Борко, В.Брижко, М. Бем, І. Городиський, К.Денисенко, Т.Джига, О.Косов, О.Кравчук, О.Наливайко, О.Радзієвська та ін. Розвиток інформаційного суспільства вивчали: А. Башук, Г. Блінова, Н.Гавриленко, О.Григор'єв, С.Грищак, Г.Демошенко, Д. Дюжник, П.Клімушин, О. Косілова, І.Костецька, Д.Ланде, Н. Лащенко, М.Липчук,

Н.Литвин, Мануель Кастельс, Л.Наливайко, О.Орлова, Пекка Хіманен, А.Серенок, Ю.Соломко, І.Сопілко, Ю.Фольварочний, В. Фурашев та інші.

Об'єктом дослідження є процес організації діяльності правоохоронної діяльності в умовах інформаційного суспільства.

Предмет дослідження – сукупність теоретико-методичних і практичних аспектів щодо удосконалення інформаційного забезпечення правоохоронних органів в умовах воєнного стану.

Мета дослідження – теоретичне обґрунтування та розробка заходів щодо удосконалення інформаційного забезпечення правоохоронних органів та посилення інформаційної безпеки в сфері державного управління.

Завданнями роботи є:

1) з'ясувати поняття, зміст та сутність інформатизації в умовах формування інформаційного суспільства;

2) проаналізувати інформаційне забезпечення правоохоронних органів у нашій державі;

3) встановити особливості інформаційної безпеки в Україні під час воєнного стану;

4) проаналізувати напрямки інформатизації діяльності орагнів Міністерства внутрішніх справ України;

5) дослідити ефективності заходів інформаційної безпеки на сучасному етапі розвитку суспільства;

6) сформулювати пропозиції щодо вдосконалення організації роботи правоохоронних органів на основі впровадження новітніх європейських підходів та ІТ-технологій;

7) окреслити напрями вдосконалення інформаційного забезпечення правоохоронних органів.

Методи дослідження. В магістерській роботі використовуються різні методи наукового пізнання. Загальнонаукові методи, методи окремих напрямків науки: науки державного управління, права, соціології та економіки.

У першому розділі магістерської роботи використовується загальнонауковий діалектичний метод, за допомогою якого з’ясовано особливості інформатизації суспільства та проблеми організації діяльності правоохоронних органів щодо їх інформатизації.

У другому розділі роботи застосовувався «порівняльний аналіз» відносно аналізу шляхів інформатизації управлінських процесів у правоохоронних органах, органах юстиції як України, так і інших держав, які є лідерами у цифровізації управління. Також здійснювалося порівняння інформатизації управлінських процесів в нашій державі з тими країнами, які є найбільш цифровізованими за висновками міжнародних організацій.

Системний підхід застосовувався під час оформлення напрямків удосконалення організації діяльності органів МВС.

Науково-теоретичним підґрунтям цієї роботи стали наукові роботи фахівців у галузі державного управління, економіки, політології, інформатики та права. Досліджувалися нормативно-правові акти, матеріали Уповноваженого Верховної Ради України з прав людини, Генеральної прокуратури України, Міністерства внутрішніх справ України, Державної служби спеціального зв’язку та захисту інформації України та інших суб’єктів публічного адміністрування.

Практичне значення магістерської роботи полягає в можливості використання напрацювань під час підготовки і викладання дисципліни «Інформаційні платформи для суспільного управління» зі спеціальності «публічне управління та адміністрування», під час удосконалення інформаційного забезпечення суб’єктів публічного адміністрування.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ ОРГАНІЗАЦІЇ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ В УМОВАХ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

1.1 Сутність і зміст організації діяльності правоохоронних органів в умовах інформаційного суспільства

Категорія «інформація» сприймалася як феномен, що досліджується у різних галузях науки – філософія, соціологія, політологія, право та інші. Інформація у сфері управління не виникає нізвідки і зникає в нікуди. Як інформація впливає прийняття управлінських рішень, і прийняті рішення впливають обсяги інформації, підтверджують певні факти.

Інформація як наукова категорія постала як наслідок необхідності переосмислення технології трансляції чи ретрансляції, сприйняття і перетворення те, що називається – інформація. Інформація у загальному сенсі є мірою розподілу матерії та енергії у просторі та в часі. Розглядаючи інформацію, що передається, за допомогою певної послідовності цінностей, наприклад алфавіту, а передачу і прийом цієї інформації за допомогою послідовних виборів з цього алфавіту, Р.Хартлі вів поняття кількості інформації за допомогою логарифму, загальної кількості можливої послідовності символів, а одиницею вимірювання цієї інформації визначив основу цього логарифму [13, с. 11].

Право на інформацію є основоположним правом по відношенню до всіх інших конституційних прав і свобод, з точки зору їх використання та застосування, адже їх забезпечення та реалізація неможливі без повної, достовірної інформації щодо змісту, особливостей кожного окремо взятого права та свободи [96, с.107].

На сучасному етапі свого існування, світ переживає масові трансформації в соціально-економічній сфері, спричинені широкомасштабним впровадженням та використанням цифрових технологій. Людство спостерігає за значущими змінами, що відбуваються у всіх аспектах суспільного життя через поступове формування цифрової економіки, без якої вже складається враження про неможливість людського існування.

Очевидно, що подібні економічні перетворення, які неможливо ігнорувати законодавцем, повинні стати основою правотворчої діяльності будь-якої країни, що зацікавлена в сталому розвитку своєї економіки. Удосконалення законодавства в широкому розумінні, враховуючи його недоліки та переваги, повинно визначати не лише юридичну, а й економічну практику.

Така позиція надзвичайно важлива в умовах розвитку “цифрової реальності”, коли технології ставлять виклик традиційним правовим структурам і виникають нові конфлікти та прогалини, які не можна негайно вирішити. У період, коли інформаційно-комунікаційний сектор стрімко еволюціонує та є ключовим мотором інновацій, законодавець здійснює лише повільні та неоднозначні кроки у напрямку правового регулювання, оскільки ще не повністю визначив його траєкторію та можливі наслідки для господарської сфери. Цифровізація не є системним, послідовним чи структурно-однорідним явищем, але при цьому вона забезпечує суттєве галузеве та територіальне охоплення, тим самим формує перед вітчизняною юридичною практикою нові виклики, послаблюючи сприйняття кордонів та сфер впливу правових галузей. Насправді це знаходить своє прояв як у конкуренції законодавчих, підзаконних норм, і у виявленні суміжних інститутів задля встановлення взаємодоповнюючого регулювання. Правової системи необхідно своєчасно відстежувати та коректно реагувати на прискорену динаміку суспільних відносин. Цифрова економіка виявила сфери, які не пристосовані за окремими аспектами до порядку, що змінюється. Таке відставання можна пояснити відсутністю ефективних

правових механізмів державного управління, забезпеченням інформаційної безпеки, захистом інтелектуальної власності у віртуальному середовищі, застосуванням венчурного капіталу в IT-сфері, застосуванням особливих правових режимів та іншими причинами. Позитивного економічного ефекту в рамках цифрової економіки реалістично досягти можливо лише за наявності гнучкого та адаптивного до нових реалій публічно-правового регулювання. Сучасні держави лише перебувають на шляху побудови цілісної системи регулювання інформаційних відносин у період цифровізації, зокрема України.

Державна інформаційна політика – це діяльність держави, спрямована на формування та регулювання середовища, в якому задовольняються інформаційно- комунікативні потреби громадян України, суспільства і держави [83].

Цифрова трансформація може відбуватися у системі громадського управління двома способами. Перший – традиційний та еволюційний: збереження та поступове вдосконалення існуючих відомчих інформаційних систем, створення нових систем, покращення обміну між ними та поступова їх інтеграція. Це повільний та трудомісткий шлях. Недоліком такого варіанту є збереження нестримно застарілих технологій управління, що гальмують трансформаційні процеси. Головні сучасні переваги цього варіанта – забезпечення якості даних та можливість швидкої зміни процесів. Крім того, при цьому сценарії зберігається тенденція, коли відомства, оперуючи своїми бюджетами на інформацію, автоматизують свої процеси, зберігають їхню архаїчність. Другий шлях – це цифрова трансформація існуючих процесів та структур управління, що ґрунтується на можливостях того, що принесло нові технології [25, с. 28].

Перетворення системи керівництва, яке реалізовують країни ЄС, відзначається конкретним впровадженням цифрових технологій. Для забезпечення довгострокової конкурентоспроможності України необхідно створити новий рівень організації державного управління та державної

служби. Цього можна досягти лише шляхом перегляду загальної концепції функціонування влади, впровадження нових моделей управління процесами і інформацією, а також розроблення шляхів їх реалізації в умовах сучасності.

Сфера публічного управління потребує введення новітніх технологій управління, що можливо здійснити через інформаційну систему. Держава, управляючи суспільством, вносить зміни у методи взаємодії із суспільством (наприклад, під час надання адміністративних послуг). Державне управління має багато визначень. На думку деяких авторів, державне управління в основному займається організацією державної політики та програм, а також поведінкою чиновників (як правило, необраних), офіційно відповідальних за їх поведінку [6]. Інші фахівці в цій галузі визначають державне управління як усі процеси, організації та приватні особи (останні діють на офіційних посадах та ролях), пов’язані з виконанням законів та інших норм, прийнятих або виданих законодавчими, виконавчими органами та судами. А в інших джерелах державне управління розглядається як використання управлінських, політичних та правових теорій та процесів для виконання законодавчих, виконавчих та судових повноважень для надання державних регуляторних та службових функцій.

Слід виділяти такі групи механізмів публічного управління та / або публічної політики:

1) організаційні та інституційні;

2) нормативні правові та інші правові документарні (правові програмні, адміністративно-розпорядчі, концептуально-доктринальні);

3) соціальні;

4) політичні;

5) судові;

6) фінансово-економічні;

7) інформаційні.

Організаційний механізм публічного управління та/або публічної політики представляє собою структурно-функціональну єдність

різноманітних юридично визначених способів (методів) та процедур, що можуть бути застосовані або обов'язково використовуються для адміністративно-розпорядчих, організаційних та інших дій, які здійснюються посадовими особами публічної адміністрації. Ці дії спрямовані на забезпечення публічного управління та/або публічної політики у вирішенні конкретного комплексу взаємопов'язаних проблем або виконанні однієї функції (або кількох пов'язаних функцій) публічної влади.

Організаційні механізми в інформаційній сфері утворені різними органами центральної виконавчої влади, регіональними органами публічної влади та іншими суб'єктами публічного адміністрування.

Нормативно-правовий механізм публічного управління та/або публічної політики є визначеною сукупністю юридичних інструментів (правових методів, матеріальних і процесуальних норм права, технічних стандартів, актів правозастосування), що передбачені в межах компетенції органу публічного управління з метою забезпечення його функцій і виконання повноважень щодо конкретного предмета відання або питання.

Нормативний механізм утворюють основні закони, законодавчі та підзаконні нормативно-правові акти. В Україні така система є складною, бо відносяться до цього механізму акти різних органів виконавчої влади, акти Президента України та інших органів влади.

Орієнтацію на впровадження інформаційного суспільства було започатковано Стратегією інтеграції України до ЄС 1998 року. Така орієнтація отримала впровадження у таких актах:

1) Законі України «Про Концепцію Національної програми інформатизації";

2) Законі України «Про Національну програму інформатизації" від 01.12.2022 № 2807-IX;

3) Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" від 09.01.2007 № 537-V [71];

4) Постанові КМУ № 1134 «Про Національну систему індикаторів

розвитку «інформаційного суспільства»;

5) План заходів з інформатизації був затверджений Розпорядженням КМУ від 15.08.2007 р. [64];

6) Стратегії розвитку інформаційного суспільства [81];

Рекомендації парламентських слухань з питань розвитку інформаційного суспільства та в галузі інформаційно-телекомунікаційних технологій і розвитку інформаційного простору в Україні, схвалені Постановою Верховної Ради України 2005 року, акцентували увагу органів влади та суспільства в цілому на питаннях інформатизації суспільства. Було з'ясовано проблемні питання на той час і вектори розвитку інформаційного законодавства.

Поряд з тим, продовжують бути чинними зазначені вище закони про інформатизацію України, а підписаний Президентом України Володимиром Зеленським Закон України від 01.12.2022 № 2807-IX «Про Національну програму інформатизації", який набрав чинності 01 березня 2023 року, є революційним, так як на законодавчому рівні водить нові та значно осучаснює такі терміни, як: електронна демократія, електронне урядування, інформатизація, модернізація, програми інформатизації, проект інформатизації, робота з інформатизації, створення засобу інформатизації, цифрова технологія, цифровізація. Також у п. 2 ст. 2 зазначеного закону визначені особливості реалізації державної політики у сфері інформатизації для забезпечення потреб та розвитку інформаційного суспільства, впровадження інформаційно-комунікаційних та цифрових технологій.

Національна програма інформатизації формується, виходячи з долгострокових пріоритетів соціально-економічного, науково-технічного, національно-культурного розвитку країни, з урахуванням світових тенденцій розвитку та досягнень у сфері інформатизації. Програма спрямована на вирішення завдань розвитку інформаційного суспільства, підвищення ефективності та результативності державного управління, національної безпеки і оборони.

Всі вище вказані нормативно-правові акти утворюють засади та практично-правове підґрунтя процесу формування інформаційного суспільства в сучасній Україні.

Соціальний механізм публічного управління та / або публічної політики – сформовані або збудовані в певній логіці (топології) і певною формою відносини (в тому числі опосередковані) між публічною адміністрацією та товариством або його сегментом (як об'єктом і одночасно (опосередковано) суб'єктом публічного управління), а також реалізований в рамках цих відносин комплекс повторюваних і відтворюються дій, опосередковано дозволяють забезпечити досягнення цілей і рішення задач публічного управління.

Інституційний механізм публічного управління та / або публічної політики – це певним чином внутрішньо структурована сукупність – система (або її сегмент) – органів публічного управління, а також сукупність посад публічної адміністрації, за допомогою функціонування яких (виконання повноважень за якими) реалізуються зазначені управління і політика.

Засіб публічного управління та / або публічної політики – це відтворюється управлінське дію, що дозволяє впливати на об'єкт публічного управління.

Міра (як тип інструменту) публічного управління та / або публічної політики – це дискретне і партикулярне дію публічної адміністрації щодо реалізації публічного управління або разова сукупність таких дій.

В принципі, міра – це той же засіб, тільки відрізняється разова і прив'язане до конкретних умов.

К. Лайа, Т. Папаїоанну і Дж. Сміт вказують, що вибір інструменту публічного управління завжди є політичним вибором, і в результаті вибір палітри інструментів публічного управління здійснюється найчастіше таким чином, що занадто мало уваги приділяється тому, наскільки оптимально вони можуть бути зістиковано між собою і скомбіновані. Вибір політичних інструментів в цілому відображає політичну культуру і що склалася в

державі політичну обстановку. Необхідність залучення суб'єктів з боку приватного сектора також може бути визначальним фактором при виборі інструменту публічної політики [106, с.4-5].

Державне управління України в умовах зростання кількості завдань, ініціатив, проектів та одночасної оптимізації витрат має базуватися саме на технологічних та цифрових формах забезпечення безперебійного функціонування. Підвищення прозорості та ефективності державних інститутів можна досягти, зокрема, шляхом уніфікації та стандартизації державних управлінських та ділових процесів, а також використання аутсорсингу для непрофільних функцій [79].

Державна інформаційна політика представляє собою один із аспектів державної стратегії. Водночас, вона виступає як елемент і внутрішньої, і зовнішньої політики держави. Ця політика є регулюючою функцією органів публічного управління, спрямованою на розвиток інформаційної сфери як у суспільстві, так і на державному рівні. Вона охоплює не лише телекомунікації, інформаційні системи чи засоби масової інформації, але і всі аспекти виробництва та відносин, пов'язаних із створенням, зберіганням, обробкою, демонстрацією, передачею інформації у всіх її формах.

Інструментами інформаційної політики здійснюється структурування інформації, розпорядником якої є орган влади. На теперішній час кожний орган влади має спеціалізовану службу, відділ або підприємство, що здійснює адміністрування тих ресурсів, які є в наявності у цього органу влади.

Основними напрямками та інструментами державної інформаційної політики є: забезпечення доступу громадян до інформації; створення систем та мереж інформації під керівництвом держави; посилення матеріально-технічних, фінансових, організаційних, правових та наукових засад інформаційної діяльності; забезпечення ефективного використання інформації; сприяння постійному оновленню, збагаченню та зберіганню національних інформаційних ресурсів; створення єдиної системи захисту інформації; підтримка міжнародного співробітництва в галузі інформації та

забезпечення “інформаційного суверенітету України”; сприяння задоволенню інформаційних потреб українців за кордоном [13, с. 172].

Узагальнивши думки науковців слід підкреслити такі риси державної політики щодо цифровізації управлінських процесів:

1. Системне суспільне явище, що відноситься до категорії соціально-політичних феноменів, в яких фіксуються найважливіші тенденції інформатизації управлінських процесів.

2. Цілеспрямоване управління процесами суспільного розвитку, що проявляється у практичному, організуючому і регулюючому впливу держави на суспільну життєдіяльність людей. Такий вплив має на меті упорядкувати, зберегти чи перетворити певні суспільні відносини з використанням примусу.

3. Певний вид діяльності щодо реалізації владних функцій. Характеризується певними формами і методами реалізації.

4. Складова частина системи політичної влади, що виконує певні функції і завдання, а також реалізує надані повноваження органів публічної влади.

5. Найважливіший фактор модернізації, реалізації соціальних, політичних, економічних і технологічних змін. Найчастіше цей фактор орієнтовано на майбутнє.

6. Одночасно наука й мистецтво, один з видів публічної професійної діяльності, домінантою якого є протиріччя між об’єктивним характером управління та суб’єктивним способом його здійснення.

Останнім часом усе більше вплив на публічне управління здійснюється за допомогою глобалізації. На думку В. Б. Дзюндзюка одним з позитивних наслідків глобалізації є розповсюдження демократії, а демократія – це завжди дотримання чітких, зрозумілих правил, що діють для всіх оформлених у вигляді нормативно-правових актів. Так само без наявності подібних правил не можлива ефективна співпраця між різними акторами публічного управління. Демократичних режим науковець вважає уособленням раціональної форми влади, а також ґрунтується на певних цінностях, однією з яких є невтручання в

особисте життя людини, його віддільність від професійної діяльності [16].

Намагання впроваджувати нові системи без урахування інституційного контексту все одно призводять до узгоджень та появи гібридів, але виявляються надто витратними. Навпаки, коли такий компроміс планується заздалегідь, результати виявляються ефективнішими. Рішення в галузі електронного уряду, хоча вони можуть здаватися успішними, не повинні бути просто запозичені; вони повинні бути цілеспрямовано пристосовані до існуючих інституційних систем. Перехід до електронних послуг – це не лише технологічний, а й соціальний процес з вираженою культурною складовою. Стабільність вітчизняної бюрократичної культури, спрямованої на підтримку закритості та непрозорості в ухваленні рішень, призводить до того, що розроблені в межах цих правил закони виявляються малоефективними.

Інформаційна політика постійно знаходиться у стані динаміці. При чому групи механізмів інформаційного забезпечення (правові, економічні, соціально-культурні, організаційні тощо) зазнають постійних змін.

Нова система управління країною стане технологічною, нормативною і культурною основою майбутнього розвитку. Запропонована Президентом України концепція “держави у смартфоні” може виконувати роль такої основи. Це абсолютно новий спосіб організації та виконання функцій державних органів, який базується на інтегрованих та цифровізованих процесах та передових технологіях (єдина система збору та зберігання даних, цифрова інфраструктура, автоматизоване прийняття рішень і таке інше).

Для того щоб закони почали функціонувати, їх необхідно адаптувати до існуючої інституційної системи. Впровадження інтеграційних інструментів надання електронних послуг сприяє підвищенню якості та спрощенню та скороченню термінів отримання публічних послуг. Ці інструменти базуються на реалізації принципу єдиного вікна під час надання публічних послуг, що передбачає виключення або максимальне обмеження участі заявників у процесах збирання інформації з різних інстанцій і надання цієї інформації до інших інстанцій. У наукових джерелах зустрічають різні

підходи до класифікації інформації, яка передається і отримується органами державної влади. У дисертації за назвою «Правове регулювання відносин щодо отримання органами державної влади України інформації" її автор – І.М.Сопілко, виділив такі критерії класифікації: 1) режим доступу до інформації (відкритий та ІзОД); 2) метод поширення інформації (ОДВ отримують документовану і публічно оголошену інформацію); 3) суб'єкти отримання (інформація, яку можуть отримувати органи законодавчої, виконавчої та судової влади); 4) форма взаємодії органу державної влади при отриманні інформації (інформація, яка надається іншими суб'єктами самостійно та інформація, що вимагається від органу державної влади) [90].

Державна інформаційна політика є різновидом державної політики, як зовнішньої так і внутрішньої тому науковці розкривають поняття державної інформаційної політики через категорію «влада». Це пояснюється тим, що держава здійснює вплив на різні сфери суспільних відносин через діяльність уповноважених органів публічної влади. За допомогою державної політики забезпечуються розробка цільових орієнтирів, критеріїв оцінки ефективності політик, які відповідають прийнятій у державі доктрині.

Державна інформаційна політика встановлює способи виробництва, накопичення й зберігання актуальних даних про процеси управлінського характеру. Державна інформаційна політика визначає механізми адаптації, інтерпретації, впорядкування відомостей про суб'єктів управління, про фізичних та юридичних осіб, про їхні данні та їхню діяльність.

Державна інформаційна політика здатна гармонізувати суспільство. Головне – це забезпечити відповідний захист від втручання у бази даних.

Ставлячись до поняття «інформація» як до філософської категорії, можна сказати, що процеси її використання та обробки є нескінченними. Отже до поняття державної інформаційної політики слід відносити характерні риси влади, державних інституцій, інформацій. Компоненти інформаційної діяльності, що наведені на рис.1.1, дають можливість осягнути масиви інформації, різноплановість способів їх передачі та зберігання,

складність регулювання інформаційної діяльності.

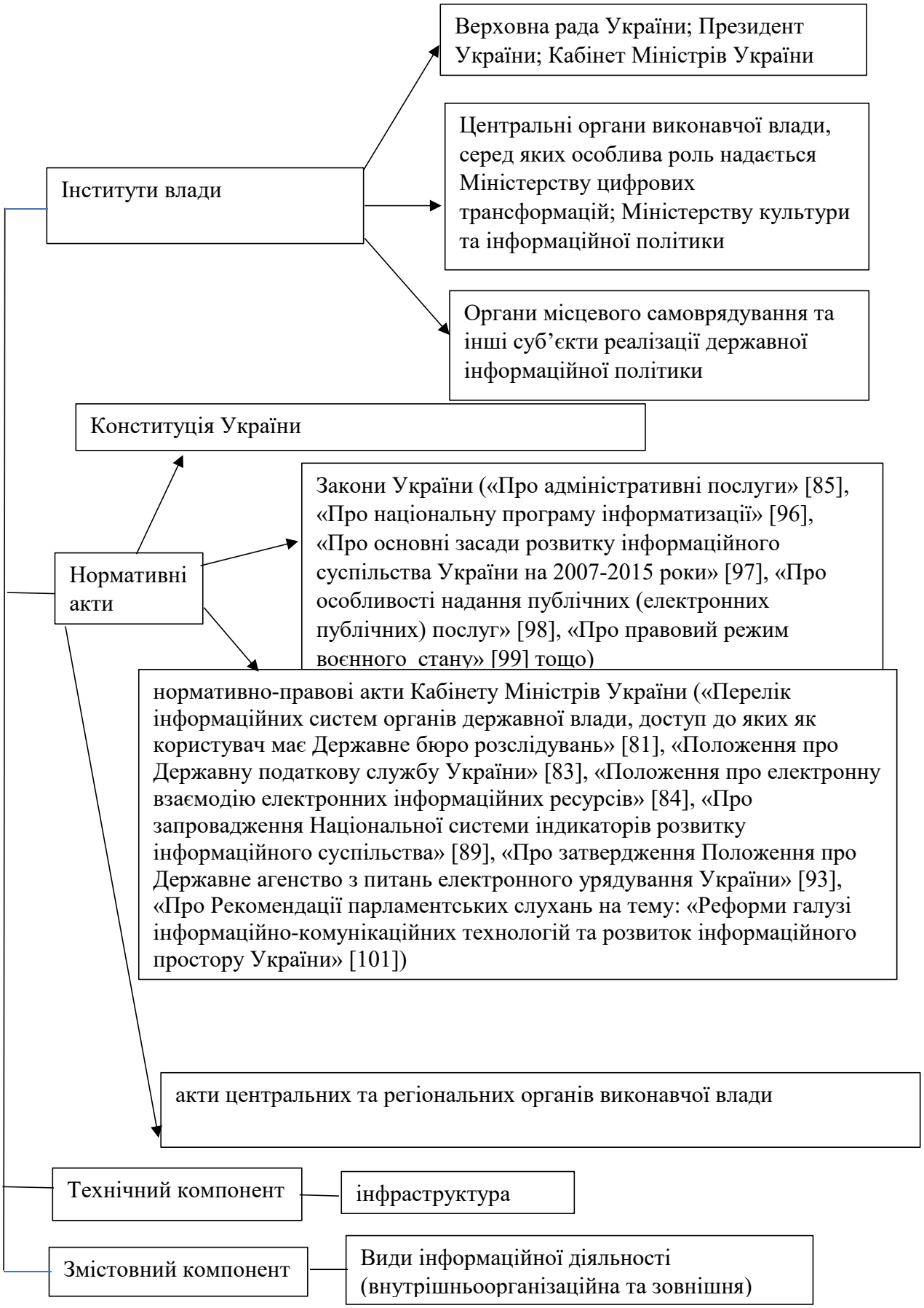

Рис. 1.1. –Компоненти механізму інформаційного забезпечення органів публічної влади

Державна інформаційна політика забезпечує: формування політики, що відбувається на рівні уряду, президента та парламенту; проєктування нових векторів політики; упровадження політики; визначення проблем, що виникають під час реалізації державних програм та стратегій; пошук розв'язання проблем; оцінювання ефективності упроваджених векторів цієї політики.

Така трансформація інформаційних зв'язків держави і громадянина має багато загроз, тому вчені особливо досліджують кібербезпеку. У контексті книги «Cyberpower and national security» кібер використовується для охоплення технічних, інформаційних та людських елементів. Деніел Кюль визначає кіберсилу як операційну область, створену для використання електроніки та електромагнітного спектру для створення, зберігання, модифікації, обміну та використання інформації через взаємопов'язані та Інтернет-інформаційні системи та пов'язані з ними інфраструктури. Це визначення є широким і технічно сфокусованим, є корисною платформою, з якої можна почати обговорення [104].

Переваги цифрової економіки також очевидні для більшості науковців, серед яких – Т. Салаєв, О. Орлова [88; 48]. Вони підтверджують у публікаціях, що цифровізація дає можливість досягти такого: динамічний розвиток, зниження витрат на платежі (особливо онлайн, де вартість послуг істотно менша), відкриття нових джерел доходу. Крім того, відкривається можливість для підприємств виходити на світовий ринок та підвищувати доступність товарів і послуг у будь-якій країні світу.

Такі можливості здатні реалізуватися лише за умови належної інформаційної безпеки в сучасних державах. Інформаційне забезпечення сьогодні здійснюється на основі правових актів, основні з яких наведено в таблиці 1.1. Слід зазначити, що розподіл актів за юридичною силою груповано у таблиці і виділено різними кольорами.

Визначено ознаки інформаційного забезпечення органів публічної адміністрації наступним чином:

Таблиця 1.1

Нормативно-правові, яким визначено підстави інформаційного забезпечення та інформаційної безпеки в правоохоронних органах України

№	Назва нормативно-правового акту
1	Закон України «Про основні засади забезпечення кібербезпеки України»
2	Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»
3	Закон України «Про електронні комунікації»
4	Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» від 26 серпня 2021 року № 447/2021»
5	Указ Президента України «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України»
6	Постанова Кабінету Міністрів України від 16.05.2023 № 497 «Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж»
7	Постанова Кабінету Міністрів України від 04.04.2023 № 299 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі»
8	Постанова Кабінету Міністрів України від 29.12.2021 № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту»
9	Постанова Кабінету Міністрів України від 23.12.2020 № 1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки»
10	Постанова Кабінету Міністрів України від 09.10.2020 № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури»
11	Постанова Кабінету Міністрів України від 19.06.2019 № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»

Продовження таблиця 1.1

12	Постанова Кабінету Міністрів України від 11.04.2012 № 295 «Про затвердження Правил надання та отримання телекомунікаційних послуг»
13	Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах»
14	Постанова Кабінету Міністрів України від 16.11.2002 № 1772 «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах»
15	Наказ Адміністрації Держспецзв'язку від 15.01.2016 № 20 «Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті», зареєстрований у Міністерстві юстиції України 05.02.2016 за № 196/28326
16	Наказ Адміністрації Держспецзв'язку від 02.12.2014 № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах», зареєстрований у Міністерстві юстиції України 28.01.2015 за № 90/26535
17	Наказ Адміністрації Держспецзв'язку від 10.06.2008 № 94 «Про затвердження Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах», зареєстрований у Міністерстві юстиції України 07.07.2008 за № 603/15294
18	Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджені наказом Адміністрації Держспецзв'язку від 03.07.2023 № 570
19	Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджені наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601

1. Це безперервний процес, який включає різноманітні види

інформаційної діяльності представників органів публічної адміністрації, їх посадових осіб та інших учасників.

2. Методи реалізації інформаційного забезпечення включають створення, використання, дослідження, зберігання, захист, передавання, обробка та знищення інформації.

3. Основний ресурс – це інформація, а її вид, якість, обсяг, структура, форма, строк та носії визначаються інформаційними потребами та правами органів публічної адміністрації.

4. Засобами інформаційного забезпечення є інформаційні системи, мережі, ресурси та технології, побудовані на сучасних засадах обчислювальної та комунікаційної техніки.

5. Реалізація інформаційного забезпечення включає комплекс заходів, таких як нормативно-правові, організаційно-управлінські, науково-технічні та інші.

6. Основною метою є задоволення інформаційних потреб та забезпечення реалізації інформаційних прав органів публічної адміністрації [4, с.406].

Наведені способи інформаційного забезпечення повною мірою відносяться до діяльності правоохоронних органів України.

За висновками авторів навчального посібника «Основи публічного права України» правоохоронна діяльність – окремий вектор діяльності державних органів.

Правоохоронну діяльність в Україні здійснюють державні та недержавні організації, створені відповідно до законодавства. Їхня діяльність не може обмежувати права і свободи людини. Держава забезпечує соціальний захист працівників правоохоронних органів і їхніх сімей. В Україні заборонено створення збройних формувань, не передбачених законом. Правоохоронні органи виконують функції контролю, нагляду, досудового слідства та захисту прав і свобод громадян. Вони мають спеціалізацію, державно-владні повноваження та можливість застосовувати

примусові заходи.

Правозахисні організації, як державні, так і недержавні, займаються захистом прав фізичних та юридичних осіб від правопорушень. Вони надають правову допомогу для відновлення прав і відшкодування збитків. Основні групи правозахисних організацій включають органи юстиції, Уповноваженого Верховної Ради з прав людини та міжнародні правозахисні організації.

Отже, правоохоронні організації в Україні виконують важливу роль у забезпеченні правопорядку та захисті прав громадян [49, с.195-196].

Ось кілька варіантів перефразування тексту з використанням синонімів, зберігаючи при цьому основний зміст:

Виходячи з наведеного, можна виділити такі характеристики інформаційно-правового забезпечення діяльності правоохоронних органів:

1. Це комплекс заходів, пов’язаних зі збиранням, обробкою, аналізом та зберіганням даних про адміністративні правопорушення або злочини.

2. Представляє собою сукупність джерел інформації, необхідної для виконання правоохоронними органами своїх функцій.

3. Спрямований на оптимізацію процесу прийняття рішень та підвищення ефективності роботи правоохоронних органів.

4. Реалізується за допомогою спеціалізованих інструментів та методик.

5. Впливає на правову свідомість громадян, сприяючи дотриманню закону [43, с.130].

Таким чином, можна стверджувати про певні успіхи України в напрямку електронного урядування. Досить швидкими темпами наша держава рухається до стандартів урядування, які існують у країнах-членах ЄС.

1.2 Сутність і особливості інформаційної безпеки в правоохоронній системі

В умовах сучасних викликів, особливо після 2014 року, виникла гостра потреба в розробці ефективних правових механізмів захисту інформаційної безпеки України. Це передбачає визначення правових засад організації та координації дій суб'єктів забезпечення інформаційної безпеки, а також розробку пріоритетних напрямів державної політики в цій сфері [11].

На становлення і розвиток законодавства України у сфері національної безпеки і оборони протягом всього часу впливали політичні фактори надзвичайного характеру, що мало негативний вплив на його ефективність у надзвичайних ситуаціях. Крім того, свій вплив на розвиток законодавства здійснювала і недосконаліть окремихзаконодавчих актів, які регламентували діяльність державних органів.

Інформаційна безпека – це ступінь захищеності життєво важливих інтересів особи і громадянина, суспільства і держави, при якому уникнута завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційний та психологічний впливи, умисне спричинення негативних наслідків застосування інформаційних технологій [83].

Розвиток інформаційно-комунікаційних технологій та процесів породжує не тільки військові, але й інформаційні конфлікти. Україна, зазнаючи війни, опинилася в центрі не лише воєнних подій, але й об'єктом інформаційної агресії. У зв'язку з цим розвиток та забезпечення інформаційної безпеки стає вкрай актуальними для нашої країни та для досягнення перемоги. Вимагається додатковий аналіз та оцінка інформаційних загроз, а також потреба у вдосконаленні організаційного та правового забезпечення інформаційної безпеки.

Погоджуємося з напрацюваннями Салаєва, характеризуючи поняття інформаційної безпеки України доцільно виділяти у його змісті такі правові ознаки: 1) це відповідний якісний стан суспільних відносин, що включає у себе аспекти створення, використання, розповсюдження та обробки інформації, зокрема в сфері захисту; 2) за допомогою інформаційної безпеки досягається охорона та захист інформаційних потреб та інтересів людини, суспільства та держави в процесі отримання та доступу до достовірної інформації, розповсюдження, створення та використання інформації відповідно до законодавства. Метою є захист особистих прав людини, зокрема, нерозголошення конфіденційної інформації. Інформаційна безпека також забезпечує суспільні та загальнодержавні інтереси через формування відповідної інформаційної політики, представлення держави в інформаційному просторі (включаючи міжнародний), використання та обробку достовірної та точної інформації, отриманої з належних джерел. Також до завдань інформаційної безпеки належить запобігання випадкам розголошення інформації, яка є державною чи іншою законодавчо охоронюваною таємницею. 3) сукупність визначених законодавством правових, організаційних, матеріально-технічних засобів, що є об’єктивною інституційною структурою, цілісний механізм, за допомогою якого і забезпечується встановлення та підтримання стану захищеності інформаційного простору [88, с.32].

Процедури безпеки визначають, як захистити ресурси і які механізми виконання політики, тобто як реалізовувати політику безпеки. По суті процедури безпеки становлять інструкції для виконання оперативних завдань. Очевидно, що процедури стосуються такої форми організаційно-адміністративних методів, як обов’язковий припис. На даному етапі доцільним є також комплексне використання узгоджувальних та рекомендованих складових. Етап контролю з боку суб’єкта правління у змістовому плані передбачає диференціювання за рівнями, виходячи з логіки побудови управлінського циклу.

Велика кількість загроз інформаційній безпеці призводить до таких можливих небезпек: можливість використання інформаційних технологій та механізмів для здійснення ворожих актів агресії проти громадян; незаконне використання інформаційних ресурсів іншої держави; нелегальна діяльність в інформаційному просторі з метою створення дестабілізації суспільства [46]; Використання інформаційної інфраструктури для поширення інформації, спрямованої на підняття міжрасової та міжнаціональної ворожнечі, а також поширення ідей та теорій, що пропагують ненависть, дискримінацію чи насильство; маніпулювання інформацією з метою викривлення стійких моральних, етичних та культурних цінностей [47]. Це потребує не лише змін у законодавстві, а й зміни загалом державної політики в інформаційній сфері.

Перед виникненням конфлікту в нашій країні існувало законодавство, яке врегульовувало питання інформаційної безпеки. Однак російська агресія викликала потребу у концептуальних змінах у цьому аспекті. Таким чином, під час початку конфлікту керівництво країни прийняло ряд змін та доповнень до нормативно-правових актів, що регламентують забезпечення інформаційної безпеки. Так, Верховна Рада України прийняла Закон України «Про внесення змін до деяких законодавчих актів України з метою посилення кримінальної відповідальності за виготовлення та розповсюдження забороненої інформаційної продукції». Цей закон зміцнив кримінальну відповідальність в інформаційній сфері. Крім того, іншими законодавчими актами внесено зміни до Кримінального кодексу України, які передбачають відповідальність за незаконну фото- та відеозйомку під час війни, а також здійснено корективи в питання розслідування відповідних злочинів з метою спрощення слідчих процедур [60].

Президент України актом № 152/2022 на виконання Рішення Ради національної безпеки та оборони України “Про реалізацію єдиної інформаційної політики в умовах воєнного стану” введе в дію правовий режим єдиної інформаційної політики в Україні. У рамках цього рішення був

створений Центр протидії дезінформації при Раді національної безпеки та оборони України [76].

Нині важливе значення у сфері інформаційної безпеки відіграє Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” [69]. У системі захисту під охороною перебувають дані, які обробляються, а також програмне забезпечення, призначене для опрацювання цих даних.

Власник системи зобов’язаний забезпечити захист інформації в системі відповідно до умов, визначених у договорі, укладеному між ним та володільцем інформації, якщо інше не передбачено законом.

На запит володільця інформації власник системи повинен надавати відомості щодо захисту інформації в системі.

Після введення воєнного стану було винесено зміни до законодавства щодо технічного адміністрування реєстрів, порядків надання адміністративних послуг, укладенням договорів з отримувачами послуг. Під особливим захистом держави опинилися підприємства, які мають важливе значення для національної економіки в інформаційній сфері [7].

Важливим нормативно-правовим актом є Стратегія інформаційної безпеки [92; 100], що є основою захищеного інформаційного простору України [31].

За висновками А. Крупнової система суб’єктів адміністративно-правового забезпечення інформаційної безпеки містить у собі широке коло структур як державної, так і недержавної приналежності, що неминуче породжує приватні, відомчі інтереси, взаємне суперництво. Їхня діяльність має чітко вписуватися в річище єдиної, цілеспрямованої державної інформаційної політики, що являє собою сукупність цілей, які відображають національні інтереси України в інформаційній сфері, і тому вона потребує ефективної координації на всіх наявних рівнях. Загальне регулювання діяльності різних суб’єктів забезпечення інформаційної безпеки в умовах воєнного стану повинен узяти на себе орган, що має значний вплив і

авторитет. Незважаючи на те, що центральним органом виконавчої влади зі спеціальним статусом у сфері інформаційної безпеки є Національна комісія, що здійснює державне регулювання з питань інформаційної безпеки, вважаємо, що в умовах сьогодення, в цьому питанні, вона має передати всі свої повноваження РНБО України, яка вже займається координацією та здійсненням контролю за діяльністю органів виконавчої влади у сфері інформаційної безпеки в умовах воєнного стану. У структурі Ради слід створити Міжвідомчу комісію із забезпечення інформаційної безпеки. І саме така Комісія, наділена відповідними повноваженнями, через Раду національної безпеки і оборони України підпорядкована безпосередньо Президенту України, має виконувати багатопланову роль розробника політики у сфері забезпечення інформаційної безпеки та координатора її здійснення в непростих умовах, в яких існує країна [40, с.276].

Суб'єкти забезпечення інформаційної безпеки можна розподілити на три групи (рис. 1.2).

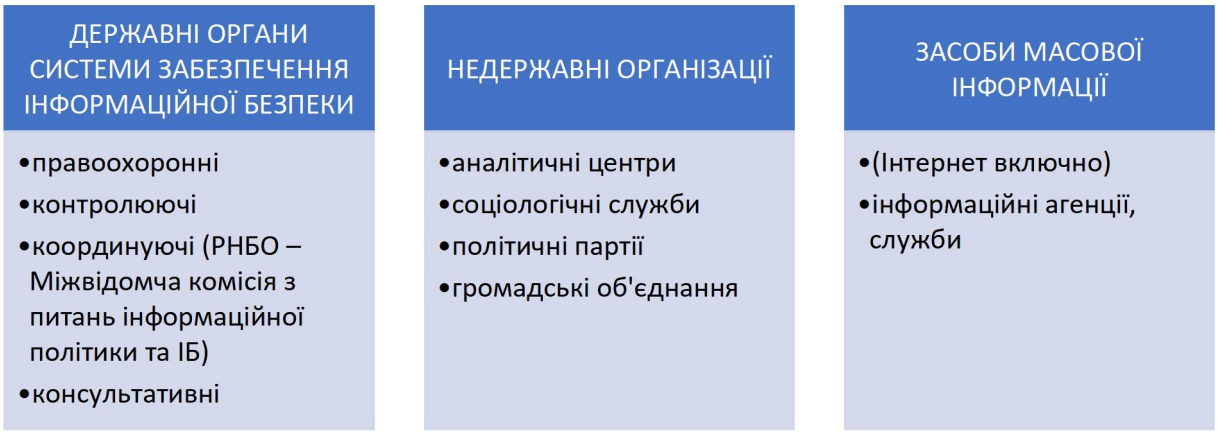

Рис.1.2 – Групи суб'єктів, які забезпечують інформаційну безпеку [використано джерело 37]

Основні функції системи забезпечення інформаційної безпеки України:

1. Створення та забезпечення діяльності державних органів - елементів системи інформаційної безпеки, що включає:

– створення правових основ побудови, розвитку та функціонування системи;

– формування організаційної структури системи та її окремих елементів, визначення та раціональний розподіл їх функцій;

– комплексне забезпечення діяльності елементів системи: кадрове, фінансове, матеріально-технічне, інформаційне тощо;

– підготовка елементів системи до виконання покладених на них функцій відповідно до їх призначення.

2. Управління діяльністю системи інформаційної безпеки, що включає:

– розробку стратегії та планування конкретних заходів щодо забезпечення інформаційної безпеки;

– організацію та безпосереднє управління системою та її структурними елементами;

– оцінку ефективності заходів, витрат на заходи щодо забезпечення інформаційної безпеки та їх наслідків.

Стратегія інформаційної безпеки визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних [91].

3. Реалізацію планових та оперативних заходів щодо забезпечення інформаційної безпеки, що включає:

– визначення національних інтересів та їх пріоритетів в інформаційній сфері;

– прогнозування, виявлення та оцінка можливих загроз, дестабілізуючих факторів та конфліктів в інформаційній сфері, причин їх виникнення, а також наслідків їхнього прояву;

– попередження та усунення впливу загроз та дестабілізуючих факторів на національні інтереси в інформаційній сфері;

– локалізація, деескалація та вирішення інформаційних конфліктів;

– усунення наслідків інформаційних конфліктів чи впливу дестабілізуючих чинників.

Потенційними загрозами інформаційній безпеці є: 1) кібератаки; 2) помилка співробітника; 3) неефективна безпека кінцевої точки; 4) інсайдерські загрози; 5) неправильні конфігурації; 6) соціальна інженерія.

4. Міжнародне співробітництво в галузі забезпечення інформаційної безпеки, яке включає:

– розробку нормативної правової бази, що регулює інформаційні відносини держав та їх взаємодію у сфері забезпечення інформаційної безпеки;

– приєднання до існуючих та формування нових двосторонніх та багатосторонніх структур (організацій), діяльність яких спрямована на спільне вирішення завдань забезпечення інформаційної безпеки;

– участь у роботі управлінських, виконавчих та забезпечувальних підрозділів цих структур (організацій), спільна реалізація планових та оперативних заходів [45].

Інформаційна безпека, заснована на принципах, що склалися десятиліттями, постійно розвивається, щоб захистити все більш гібридні та багатохмарні середовища в умовах загроз, що постійно змінюються. Враховуючи еволюцію цих загроз, кілька команд повинні працювати разом, щоб оновити як технології, так і процеси, що використовуються для цього захисту.

РОЗДІЛ 2
АНАЛІЗ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОРГАНІВ МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ УКРАЇНИ

2.1 Аналіз інформаційного забезпечення органів Міністерства внутрішніх справ України

Українська держава вимагає від правоохоронних органів збирати та обробляти інформацію про правопорушення, осіб, які їх вчинили, та інші пов’язані дані. Ця інформація зберігається в спеціальних базах даних і використовується для прийняття обґрунтованих рішень, забезпечення безпеки громадян та ефективної боротьби зі злочинністю. Сьогодні інформація виступає одним із головних елементів у багатьох сферах державного управління та є важливим фактором суспільних відносин. Зміни, що відбуваються на сучасному етапі в Україні, насамперед пов’язані зі зростанням великих обсягів інформації та її швидкої зміни. Тому саме на державу покладається завдання забезпечення доступу громадян України до об’єктивної інформації, пов’язаної з усіма сферами життєдіяльності.

Якщо проаналізувати довоєнний стан ІКТ у ВВП України, то його частка становила понад 4% та мала потенціал зростання. За підсумками 2021 року вітчизняний ІТ-сектор зріс на 36% порівняно з показниками 2020 року, досягнувши при цьому позначки 6,8 млрд доларів США експорту комп’ютерних послуг. Наразі частка експорту ІТ-послуг України становить близько 2,7 ВВП країни. До початку війни Україна була одним із європейських лідерів за рівнем розвитку сфери відкритих даних та становила шосте місце у рейтингу European Open Data Maturiti 2021. Сервісами на їх основі щомісяця користувалося близько семи мільйонів українців. Частка ВВП, генерована сферою відкритих даних, становила від 8 до 13%. На

початок 2022 р. рівень покриття волоконно-оптичними мережами сільського населення та рівень покриття інтернетом 4G становив 89% [82].

Для зберігання та обміну інформацією між правоохоронними органами створені спеціальні бази (банки) даних, до яких вносяться ті чи інші відомості щодо фізичних та юридичних осіб, окремих фактів чи явищ. Так, наприклад, відповідно до Закону про Національну поліцію, підрозділи поліції в особі їх посадових осіб, наповнюють та підтримують в актуальному стані бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України [43, с.130] (див. дод.А).

Упровадження цифрових послуг здійснюється в Україні за підтримки міжнародних донорів, деякі проєкти фінансуються Швейцарською агенцією, Фондом Східна Європа.

CERT-UA – це Урядова команда реагування на комп'ютерні надзвичайні події України, яка створена і функціонує в складі Державної служби спеціального зв'язку та захисту інформації України. Починаючи з 2009 року ця команда є акредитованим членом Форуму команд реагування на інциденти безпеки FIRST(https://www.first.org/members/teams/cert-ua) [56]. Завдання CERT-UA визначено на рис. 2.1.

У період січня-лютого 2024 року Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA вжила заходів для запобігання реалізації злочинного плану, який передбачав проведення деструктивного впливу на три українські організації з урядового та енергетичного секторів. Протягом цього часу, у зв'язку з фактами деструктивних кібератак, проведено комп'ютерно-технічні дослідження в інформаційно-комунікаційних системах (ІКС) трьох організацій, серед яких були фінансовий сектор, охорона здоров'я та інформаційні технології.

У більшості випадків первинний несанкціонований доступ до ІКС об'єкта атаки був отриманий заздалегідь (протягом року і більше). Зловмисники використовували скомпрометовані облікові записи VPN, а

також вразливості в налаштуваннях і програмному забезпеченні публічно доступних інформаційних систем для проникнення до мережі.

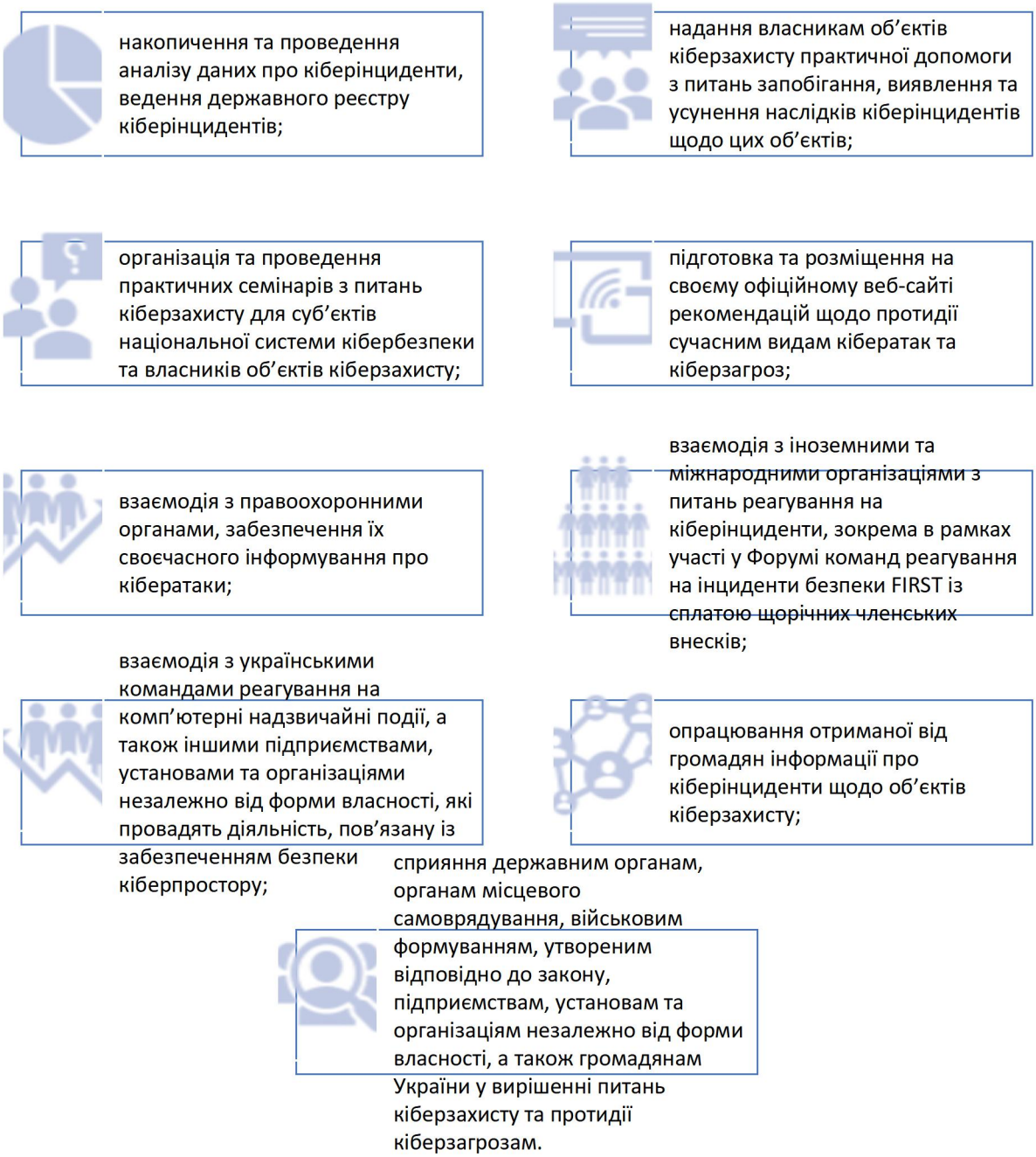

Рис. 2.1 – Завдання CERT-UA [використано джерело 56]

Крім того, проведено аналіз кількох інцидентів, пов’язаних з кібершпигунством щодо Сил безпеки і оборони України, здійснених угрупуваннями UAC-0028 (APT28) та UAC-0003 (Turla), зокрема, з використанням модифікованого шкідливого програмного забезпечення KAZUAR.

У першому кварталі 2024 року найбільш активною загрозою стало угрупування найманців UAC-0050, яке пов’язане з правоохоронними структурами Росії. Це угрупування, оголосивши про припинення діяльності під "брендом" DaVinci Group за кілька днів до російського вторгнення у 2022 році, останнім часом активно намагається привернути увагу. Станом на 22 лютого 2024 року зафіксовано і досліджено не менше 15 кампаній, під час яких зловмисники використовували щонайменше п’ять різновидів шкідливих програм: REMCOS RAT, QUASAR RAT, VENOM RAT, REMOTE UTILITIES та LUMMASTEALER. Незважаючи на те, що лише невелика частина "здобутків" публікується в Telegram-каналі, тактика угрупування нагадує діяльність брокерів первинного доступу. Враховуючи масовість атак і використання програм, спрямованих на викрадення автентифікаційних даних, скомпрометовані логіни, паролі та сертифікати можуть створити технічні умови для отримання несанкціонованого доступу до ІКС організацій для подальшого розвитку атак на їх "внутрішні" ресурси.

Щодо угрупування UAC-0010 CERT-UA вживає цілеспрямовані заходи протидії. Однак, враховуючи масштаби уражень, боротьба з шкідливими програмами та наслідками їхньої діяльності може вимагати об’єднання зусиль не лише на рівні основних суб’єктів забезпечення кібербезпеки України, а й із залученням міжнародних технологічних стейкхолдерів.

Успішній реалізації більшості кібератак сприяє халатність керівників та виконавців, які не звертають уваги на інформацію про актуальні кіберзагрози, що публікується на офіційному вебсайті та в MISP CERT-UA, а також в інших доступних джерелах. Це супроводжується повторними помилками,

такими як відсутність двохфакторної автентифікації, недостатня сегментація мережі, зокрема у частині обмеження адміністративного доступу, а також відсутність управління поверхнею атаки (вразливе програмне забезпечення, "відкриті порти" тощо) [97].

Уряд України поставив за мету суттєво покращити роботу Міністерства внутрішніх справ за допомогою інформаційних технологій. Для досягнення цієї мети розроблена масштабна програма інформатизації, яка передбачає створення єдиної інтегрованої системи, що об'єднає всі інформаційні ресурси МВС. Ця система дозволить поліцейським швидше обмінюватися інформацією, приймати більш обґрунтовані рішення та ефективніше боротися зі злочинністю. Серед пріоритетних проєктів можна виділити розвиток системи "112", створення єдиного реєстру зброї та модернізацію системи безпеки дорожнього руху [27]. У додатку А зображено напрямки інформатизації в системі МВС.

Успіхи України у впровадженні відкритого урядування неодноразово відзначались на міжнародному рівні. У 2016 році електронна система закупівель ProZorro стала переможцем премії OGP Awards, а у 2021 році система Prozorro.Продажі отримала першу премію OGP Impact Award Europe. Також відзначалися досягнення України щодо прозорого процесу підготовки планів дій.

Україна активно представлена в Ініціативі на місцевому рівні. Три українські міста - Тернопіль, Вінниця та Хмельницький - є учасниками програми OGP Local та впроваджують власні плани дій. На Глобальному саміті Партнерства у грудні 2021 року Хмельницький отримав 1-шу, а Вінниця 3-тю премії OGP Local Innovation Award Europe за досягнення на локальному рівні.

План дій із впровадження Ініціативи «Партнерство «Відкритий Уряд" у 2021-2022 роках містить 14 зобов'язань, які відповідають основним принципам Партнерства: забезпечення доступу до інформації, прозорості та підзвітності, громадської участі.

У 2022 році військова агресія росії проти України обмежила проведення публічних подій, однак це не завадило провести Тиждень Відкритого Уряду. Серед інших заходів Тижня, Секретаріатом Кабінету Міністрів спільно з Координаційною радою організовано стратегічну сесію «Віримо в перемогу - плануємо майбутнє!", під час якої представники урядового та громадського секторів спільно працювали над визначенням актуальних викликів і проблемних питань, що вийшли на порядок денний під час війни, а також інструментів відкритого урядування, які можуть допомогти їх подолати.

Процес реалізації Ініціативи «Партнерство «Відкритий Уряд" в Україні висвітлюється на офіційному веб-сайті Кабінету Міністрів України (https://www.kmu.gov.ua) та сторінці у Facebook (https://www.facebook.com/ogpUkraine). Тут розміщується інформація про Координаційну раду, новини та події, які відбуваються в межах Ініціативи, а також щоквартальна інформація про стан виконання зобов'язань плану дій.

До плану дій включено 14 заходів, якими передбачено як продовження реалізації попередніх зобов'язань, так і реалізацію нових. Так, продовжено роботу із: забезпечення прозорості публічних фінансів та системи публічних закупівель; відкриття інформації про бенефіціарних власників; реалізації Ініціативи прозорості видобувних галузей; забезпечення прозорості інфраструктури. Водночас до плану дій увійшли такі нові напрями, як запровадження державної політики відкритої науки, забезпечення цифрової доступності для осіб з інвалідністю та забезпечення відкритого доступу до гендерно дезагрегованих даних.

Розвиток інформаційного суспільства характеризується за рахунок зростання нової інформації та знань. Знання стали товаром, попит на який зростає з кожним днем. В даний час недостатньо просто знати, необхідно постійно оновлювати отримані знання.

Інформатизація суспільства пришвидшується. Нові інформаційні та комунікаційні технології призводять до радикальної переоцінки цінностей та

потреб сучасного ринку.

Можна припустити, що специфікою розвитку інформаційного суспільства є такі:

– вирішення проблеми інформаційного навантаження;

– пріоритет інформаційного ресурсу проти іншими видами ресурсів;

– поява інформаційної економіки;

– глобальний характер поширення інформаційних технологій;

– автоматизація формування колективних знань;

– наявність вільного доступу до колективних знань через застосування інформаційних технологій;

– збільшення частки самозайнятості у суспільному виробництві за рахунок впровадження мережевих технологій;

– нові можливості електронної освіти та дистанційного навчання.

Вищевикладене дозволяє припустити, що у найближчому майбутньому економічним суб'єктам доведеться постійно відстежувати та швидко коригувати свою діяльність з урахуванням формування та розвитку інформаційного суспільства, щоб забезпечити адаптивність економіки за умови перманентних змін у бізнесі.

Інформаційне забезпечення органів державної влади сьогодні здійснюється з використанням інноваційних підходів. За допомогою інформаційних технологій активно розвиваються самостійна діяльність органів публічної влади щодо створення, переробки та збереження інформації; відбувається інформаційна взаємодія як підрозділів органів державної влади, так і різних суб'єктів публічного управління між собою; забезпечується реалізація прав громадян на інформацію; проводяться контрольні заходи; здійснюється спільне використання державних ресурсів тощо.

2.2 Дослідження стану інформаційної безпеки в органах Міністерства внутрішніх справ України

На сьогодні інформація виступає одним із головних елементів у розвитку управлінських відносин. Упродовж всієї історії людства, інформація, виступаючи одним із ключових ресурсів цивілізаційного розвитку, відігравала важливу роль у суспільній життєдіяльності і продовжує відігравати її й донині. Однак, зараз, без перебільшення можна стверджувати, що інформаційні та комунікаційні технології стали найважливішим засобом підвищення ефективності управління практично в усіх сферах людської діяльності.

Захист державних інформаційних ресурсів електронного урядування передбачає забезпечення цілісності й вірогідності інформації; охорону конфіденційності інформації, доступ до якої обмежений законом або відповідно до закону; реалізацію права на інформацію [1, с.89].

За даними Держспецзв’язку, у третьому кварталі 2023 року було зафіксовано 355 кібератак, що на 46% більше, ніж у попередньому кварталі. Найпопулярнішими шкідливими програмами були SmokeLoader, Agent Tesla та Formbook. Проросійські хакерські угруповання, такі як "Народная CyberArmy" та BLUENET, здійснили 202 атаки, що становить 9% від загальної кількості." [94].

Генеральний прокурор Андрій Костін у Києві провів зустріч з колегами з Міністерства юстиції США Натаном Бруксом та Тімом Ранком, а також з юридичним радником Посольства США в Україні Джаредом Кімболом і аташе ФБР з правових питань Крісом Гейгером. Учасники обговорили стратегії розслідування російських кіберзлочинів, скоєних проти України та її партнерів.

За словами Генерального прокурора А.Костіна: «Обсяги кібероперацій Росії проти України невпинно зростають. Зафіксовано більш ніж 800 спроб

кібератак на державні установи та сервіси. Серед цих цілей – об'єкти енергетичної інфраструктури, які постійно знаходяться під загрозою» [2].

За сучасних умов бере участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку Департамент кіберполіції Національної поліції України, що є міжрегіональним підрозділом, який відповідає за боротьбу з кіберзлочинністю в межах України. Департамент відповідно до покладених на нього завдань (рис. 2.2).

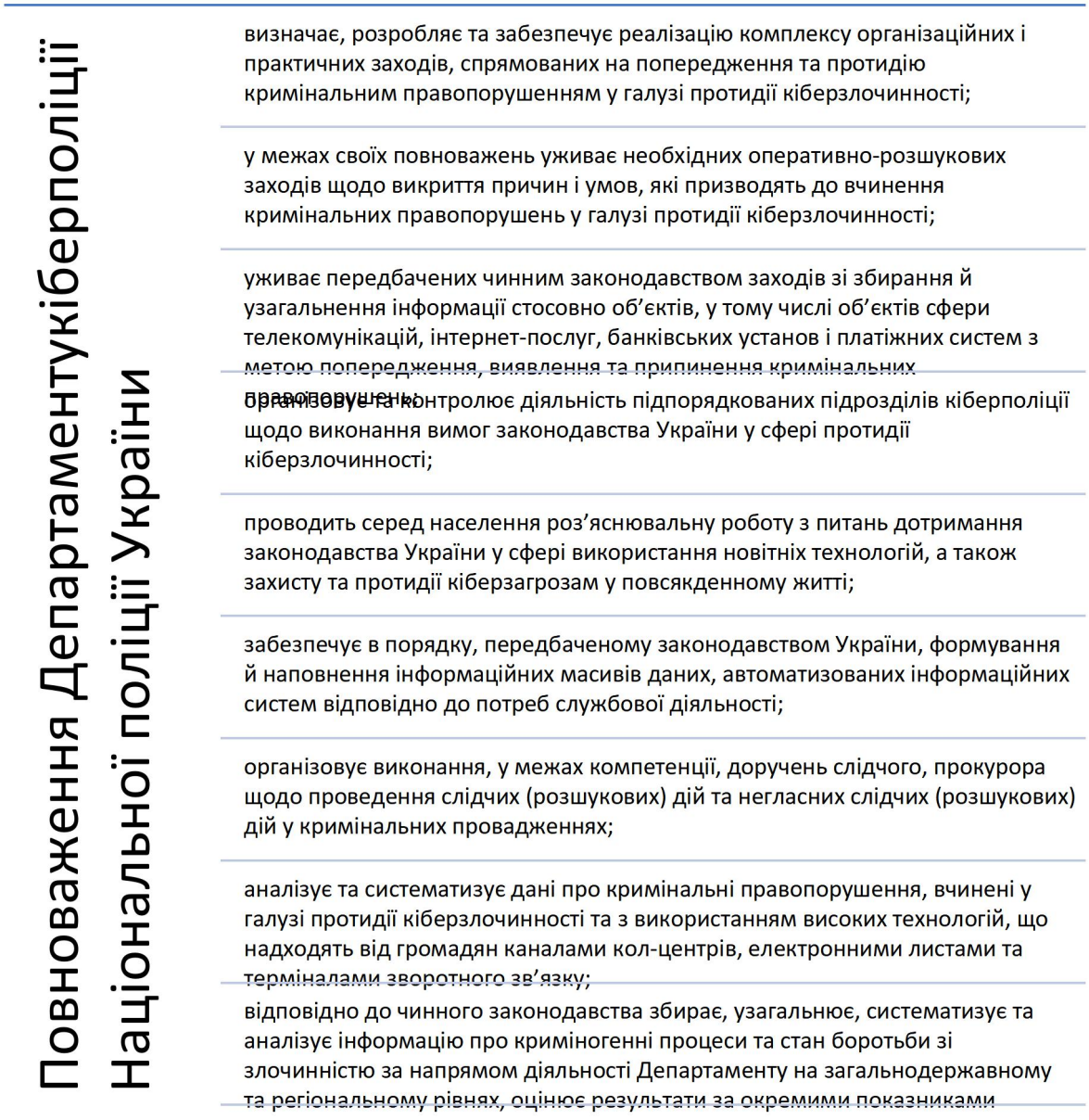

Рис.2.2 – Основні повноваження Департамент кіберполіції Національної

поліції України [використано джерело 65]

За словами Генерального прокурора А.Костіна: «Правоохоронні органи України рішуче налаштовані й надалі посилювати діяльність в інформаційній сфері та впроваджувати інноваційні методи розслідування, щоб зробити кіберпростір безпечнішим і ефективно протидіяти новим загрозам» [2].

У 2023 році Кіберполіція викрила понад 3600 кіберзлочинів. Паралельно було здійснено 18 міжнародних спецоперацій у цій галузі. Про це повідомила Кіберполіція на своїй сторінці у Facebook.

Звіт про роботу Кіберполіції за 2023 рік свідчить про виявлення понад 3600 кіберзлочинів. Завдяки оперативному супроводу Кіберполіції, понад 1700 осіб було притягнуто до відповідальності за вчинення понад 3700 злочинів, що на 59% перевищує показник попереднього року. До суду було направлено матеріали щодо 42 організованих злочинних угруповань, що на 83% більше, ніж у 2022 році.

Минулого року також відбулося 18 міжнародних спецоперацій за участі правоохоронців з Грузії, Швейцарії, Чехії, Ізраїлю, Норвегії, Нідерландів, Франції, Німеччини та США.

Завдяки оперативному супроводу Кіберполіції до суду було направлено обвинувальні акти щодо понад 4000 злочинів. Загальна сума відшкодованих збитків (з урахуванням арештованого та вилученого майна) склала майже 144 мільйони гривень. Крім того, було заблоковано майже 13 тисяч шкідливих веб-ресурсів [21].

Практика поліції по боротьбі з порушеннями інформаційного законодавства дає можливість стверджувати, що досягнення інформаційної безпеки можна розглядати як управлінських процес, який складається з кількох стадій. Їх можна визначити так:

1. Досягнення цілей, поставлених на стадії проектування.
2. Реалізація прийнятих управлінських рішень.
3. Поетапна реалізація плану безпеки.

У результаті контролю утворюється контур зворотного зв’язку, який дозволяє суб’єкту управління порівнювати поточні результати з цільовими показниками, ураховувати зміни навколишнього середовища та адекватність вірогідних побудов. Залежно від величини неузгодженості формується коригуючий вплив. Очевидно, що етап контролю пов’язаний із попередніми етапами управління і механізм зворотного зв’язку забезпечує циклічність управління.

Суттєво, що усі вищезазначені етапи взаємопов’язані між собою, передбачається неперервність процесу удосконалення системи інформаційної безпеки. Це обумовлено, по перше, складністю системи, а по-друге, динамічними змінами внутрішніх факторів та зовнішнього оточення. Зокрема, розширенням спектра актуальних загроз, появою нових загроз, зміною внутрішньої структури організації та її зовнішніх зв’язків, переглядом меж периметра безпеки.

При розгляді питань управління забезпеченням інформаційної безпеки організації крім формальних побудов базису програмно-цільовими методами необхідне проведення досліджень «неформальної” складової, обумовленої поведінкою ключових акторів об’єкта управління. Перифразуючи Еріха Фромма про тематиці, можна сказати, що система безпеки тільки тоді функціонує ефективно, коли члени організації досягають такого типу поведінки, при якому вони хочуть діяти так, як вони повинні діяти як члени даної організації. Вони повинні бажати робити те, що об’єктивно необхідне організації. Слід побудувати систему інформаційної безпеки організації цілеспрямовано виконувати, доповнивши формальний каркас моделлю користувача. Останні, у свою чергу, крім характеристик, що визначають статус та роль суб’єктів інформаційних відносин, повинні містити ситуаційні та динамічні поведінкові характеристики щодо раціональності та опортуністичної спрямованості дій з погляду інтересів забезпечення інформаційної безпеки.

Гарантування дотримання інформаційних прав громадян і в той же час

забезпечення інформаційної безпеки здійснюється через інститут Уповноваженого Верховної Ради України з прав людини.

Протягом 2022 року 1370 громадян звернулися до Уповноваженого із скаргами на порушення їхніх прав на отримання публічної інформації.

За Звітом Уповноваженого Верховної Ради України з прав людини є порушення інформаційних прав громадян. Ця уповноважена особа забезпечила висвітлення по категоріях порушення прав у сфері інформатизації на своєму сайті [98, с.197-198].

Крім того, внаслідок введення правового режиму воєнного стану та збройної агресії Мінцифри тимчасово призупинило функціонування Єдиного державного вебпорталу відкритих даних (далі – Портал) з метою захисту інтересів національної безпеки, огляду публічних даних. Використання відкритих даних, які були опубліковані на Порталі, сприяє аналізу державної політики, контролю за діями уряду, збільшенню громадської участі в процесі прийняття рішень, полегшує прийняття кращих рішень в економіці і тощо.

Після відновлення роботи Порталу 1 серпня 2022 р., деякі розпорядники інформації, незважаючи на вимоги статті 10-1 Закону України «Про доступ до публічної інформації" та розпорядження КМУ від 21 жовтня 2015 р. № 835 «Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних», не оприлюднюють на Порталі набори відкритих даних, які підлягаю [98, с.199].

Цифровізація повинна іти рука об руку з підвищенням рівня довіри і безпеки. Забезпечення інформаційної безпеки, кібербезпеки, захист персональних даних, недоторканність особистого життя та прав користувачів цифрових технологій є важливими передумовами для одночасного розвитку цифрового середовища та ефективного управління ризиками, пов'язаними з ним.

Головною умовою поєднання принципу прозорості управлінської діяльності в органах ДПС та забезпечення інформаційної безпеки є створення оптимальних умов інформування населення України про діяльність органів

публічної влади, про публічні фінанси, про результати оподаткування та боротьби з податковими правопорушеннями та системи заходів з протидії кібератак. Основні заходи з впровадження інформаційної безпеки визначено Стратегією інформації безпеки, що затверджена Указом Президента України від 28 грудня 2021 року. Цим Указом визначена необхідність посилення спроможностей забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, а також забезпечення прав та свобод кожного громадянина. Досягнення цієї мети передбачає застосування заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії. Це включає спеціальні інформаційні операції держави-агресора, спрямовані на підрив державного суверенітету, територіальної цілісності України та забезпечення інформаційної стійкості суспільства та держави. Важливо створити ефективну систему взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвивати міжнародну співпрацю у сфері інформаційної безпеки на принципах партнерства та взаємної підтримки.

Органи МВС використовують у своїй роботі різні електронні ресурси, що підлягають захисту відповідно до методичних рекомендацій, що запроваджують опис застосованих механізмів кіберзахисту до систем електронного документообігу, визначених національними та міжнародними стандартами, нормативними документами технічного захисту інформації, керівництвами та практиками, враховуючи підхід до класифікації заходів кіберзахисту, який описаний у Методичних рекомендаціях щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджених наказом Адміністрації Держспецзв’язку від 06 жовтня 2021 року № 601 [63].

Основними напрямами гарантування інформаційної безпеки України є забезпечення стійкості та ефективної взаємодії. Для досягнення цих цілей

необхідно реалізувати такі стратегічні завдання.

Спрямованість 1. Протидія дезінформації та інформаційним операціям, зокрема від держави-агресора, що націлені на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності країни, поширення пропаганди війни, насильства та жорстокості, підтримку конфліктів на національній, етнічній, расовій, релігійній основі, а також вчинення терористичних актів та порушення прав і свобод людини.

Друга стратегічна мета полягає в здійсненні повноцінного розвитку української культури та уміцненні української громадянської ідентичності.

Третя стратегічна мета передбачає підвищення рівня медіакультури та медіаграмотності у суспільстві. Необхідно забезпечити захист українського суспільства від негативного впливу дезінформації та маніпулятивної інформації, а також забезпечити стабільну соціальну відповідальність та ефективне функціонування медіасередовища. У таких умовах українське суспільство може ефективніше протистояти державі-агресору та залишатися стійким перед різноманітними загрозами, зокрема в інформаційній сфері.

Четверта стратегічна мета передбачає гарантування прав особи на збирання, зберігання, використання та розповсюдження інформації, свободу висловлення власних поглядів і переконань, захист особистого життя, забезпечення доступу до об’єктивної та достовірної інформації. Також важливо забезпечити захист прав журналістів, гарантування їх безпеки під час виконання професійних обов’язків і протидію поширенню незаконного контенту.

П’ята стратегічна ціль пов’язана з реінтеграцією громадян, які проживають на окупованих територіях України та на деокупованих територіях.

Шоста стратегічна мета передбачає створення ефективної системи стратегічних комунікацій. Основною метою цієї системи є забезпечення ефективної інформаційної взаємодії та діалогу між органами державної влади,

органами місцевого самоврядування та громадськістю у справах, пов’язаних із кризовими ситуаціями. Також, система спрямована на утвердження позитивного іміджу України, інформаційне підтримання просування інтересів держави у світі. Ефективна організація міжнародної інформаційної діяльності дозволить Україні проводити активні інформаційні заходи, повідомляти світову спільноту про події в Україні та на її тимчасово окупованих територіях, прогрес у реформах та позитивні зміни в державі, незважаючи на наявну збройну агресію. Це також включає інформування міжнародних партнерів про ключові рішення органів державної влади щодо стратегічних питань розвитку країни, що сприятиме кращому розумінню внутрішньої та зовнішньої політики України, забезпечить міжнародну підтримку та покращить імідж країни як надійного та передбачуваного партнера [92].

Така концепція у свою чергу відповідає європейським принципам відкритості публічного управління та доступу до публічної інформації. Підвищення прозорості та ефективності державних інститутів можна досягти, зокрема, шляхом стандартизації та уніфікації управлінських та ділових процесів, а також використання аутсорсингу для непрофільних функцій.

РОЗДІЛ 3
УДОСКОНАЛЕННЯ ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ В УМОВАХ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

3.1 Напрямки покращення електронної інформаційної взаємодії між інформаційно-комунікаційними системами

Положення про цифрову взаємодію цифрових інформаційних ресурсів, що затверджено постановою КМУ від 8 вересня 2016 р. № 606, визначає загальні принципи здійснення обміну цифровими даними, крім інформації, що становить державну таємницю, між суб'єктами цифрової взаємодії з цифровими інформаційними ресурсами при наданні адміністративних послуг та виконанні інших повноважень відповідно до покладених на них завдань [31].

Реалізація зазначених проєктів спрямована на упорядкування системи електронної взаємодії інформаційних ресурсів. Підзаконними актами її визначено як інформаційно-телекомунікаційна система призначена для автоматизації та технологічного забезпечення обміну електронними даними між учасниками електронної взаємодії, які взаємодіють з електронних інформаційних ресурсів під час надання адміністративних послуг та виконання інших повноважень відповідно до покладених на них завдань. Учасники системи включають в себе органи державної влади, органи місцевого самоврядування та суб'єкти господарювання, які мають зареєстрований шлюз безпечного обміну в ядрі системи.

Взаємодія електронних ресурсів має відбуватися за певними правилами, які сформульовані у вигляді принципів. До таких віднесено: технологічну нейтральність; дотримання правил законодавства про захист персональних

даних; використання єдиних норм електронної взаємодії суб'єктів публічного адміністрування; можливості повторного використання даних та програмних засобів; зменшення інформаційного дублювання.

З цього приводу Генпрокурор підкреслив, що за сучасних умов рф реалізує інформаційні кампанії з метою дестабілізації українського суспільства та атакує телекомунікаційні системи, щоб позбавити громадян доступу до мобільного зв'язку та інтернету [2].

Суб'єктами системи є:

1) держатель системи;

2) адміністратор системи;

3) учасник системи;

4) суб'єкт електронної взаємодії.

Держателем та замовником системи є Мінцифри.

Модель цифрових прав передбачає наявність тісного взаємозв'язку таких прав з особистістю, особливий порядок реалізації, а також розпорядження ними з урахуванням вимог законодавства та правил інформаційної системи. У їхньому переліку можна назвати право бути забутим, право на доступ до інформаційних даних про себе, право на розпорядження контентом користувача, право на участь у голосуванні з питань місцевого значення з використання мережі Інтернет та інше. Категорія цифрових прав перебуває в етапі свого становлення і це перелік прав перестав бути вичерпним.

Підключенню до системи підлягають державні електронні інформаційні ресурси, отримання даних з яких необхідне суб'єктам владних повноважень під час надання адміністративних послуг та здійснення інших повноважень відповідно до покладених на них завдань.

Можливості роботи з цифровою інформацією призводять не лише до змін процедурних аспектів реалізації тих чи інших прав та обов'язків публічних органів, а й до змістовного розширення їхньої компетенції. При

цьому слід зазначити, що їхні цілі збігаються щодо якіснішого та ефективного виконання покладених на них функцій.

Доступ суб'єктів владних повноважень до інтерфейсів прикладного програмування надається з метою здійснення повноважень відповідно до покладених на них завдань, зокрема для надання адміністративних послуг.

Обсяг та структура даних, до яких надається доступ через інтерфейси прикладного програмування, визначаються відповідно до потреб суб'єкта владних повноважень, що запитує ці дані, та зазначаються у договорі щодо інформаційної взаємодії. Суб'єкт владних повноважень не має права запитувати обсяг та структуру даних більше, ніж йому необхідно для надання адміністративних послуг або здійснення повноважень відповідно до покладених на нього завдань.

Суб'єкти електронної взаємодії надають дані через інтерфейси прикладного програмування (веб-сервіси) іншим суб'єктам електронної взаємодії, що є суб'єктами владних повноважень, на безоплатній основі [55].

Велике досягнення в реалізації інформаційної політики – це створення державних реєстрів. Станом на 1 вересня 2023 року діє близько 100 реєстрів, що адмініструють суб'єкти публічного адміністрування. Деякі з них наведено в таблиці 3.1.

Сьогодні фактичне оцифрування даних, пов'язане з перенесенням та накопиченням інформації в інформаційних системах і на сьогоднішній день найбільш активно відбувається в багатьох сферах, без здійснення їх подальшої обробки не відповідає сучасним можливостям цифровізації та не підвищує ефективність управлінської діяльності.

Перелічені вище процедури у майбутньому мають бути врегульовані відповідно до стандартів ЄС. Кожна сфера державного управління повинна бути забезпечена етичними правилами. Такі висновки сформулював Гавриленко Н.В. у своїй науковій статті [8, с.42].

Етичні засади не є єдиною перспективною проблемою, яку слід вирішити. Європейські експерти постійно наголошують на необхідності

підвищувати прозорість до публічних фінансів. Така проблема навіть стає умовою надання України фінансової підтримки від країн ЄС.

Таблиця 3.1

Деякі інформаційні системи органів державної влади [використано джерело 54]

Назва органу влади	Назва інформаційної системи
МВС	функціональні підсистеми єдиної інформаційної системи МВС та пріоритетні електронні інформаційні ресурси суб'єктів єдиної інформаційної системи МВС
Мінфін	автоматизована інформаційна система "Держбюджет"
Мінфін	інформаційно-аналітична система управління плануванням та виконанням місцевих бюджетів "LOGICA"
Мін'юст	Державний реєстр обтяжень рухомого майна
Мін'юст	Державний реєстр актів цивільного стану громадян
Мін'юст	Державний реєстр речових прав на нерухоме майно
Мін'юст	Державний реєстр актів цивільного стану громадян
Мін'юст	Єдиний державний реєстр юридичних осіб, фізичних осіб - підприємців та громадських формувань
Мін'юст	Єдиний реєстр довіреностей
ДПС	інформаційно-комунікаційна система "Податковий блок"
ДПС	Державний реєстр фізичних осіб - платників податків

Дослідимо окремий аспект відкриття публічної інформації стосовно публічних коштів, якими розпоряджаються різні органи публічної влади.

Україна приєдналась до Ініціативи "Партнерство "Відкритий Уряд" у 2011 році та вже реалізувала п'ять національних планів дій. У межах Ініціативи проведені глобальні реформи у сферах публічних закупівель, розкриття інформації про бенефіціарних власників, забезпечення прозорості продажів державного майна, впровадження Ініціативи прозорості видобувних галузей, розкриття інформації про публічні фінанси, впровадження інструментів електронної демократії та ін.

Спеціальними принципами інформаційної взаємодії є: достовірність і

повнота інформації, яка надається органам державної влади; своєчасність отримання ОДВ інформації; отримання ОДВ інформації про особисте життя за згодою фізичної особи (за винятком випадків, визначених законом, і лише в інтересах національної безпеки); рівності прав ОДВ та інших учасників інформаційних відносин на отримання відкритої інформації; закріплення відповідальності за порушення права отримання інформації від органів державної влади; використання законно затверджених засобів для отримання інформації від органів державної влади; закріплення у законодавстві обов'язку фізичних та юридичних осіб надавати інформацію на законний запит відповідних органів державної влади; узгодження з власником інформації питань, пов'язаних з передачею отриманих цінних відомостей третім сторонам; визначення оплати за передачу інформації органам державної влади, коли майнові права на цю інформацію переходять до держави [90].

Наведені принципи інформаційного забезпечення органів державної влади реалізують різні органи державної влади. У процесі інформатизації суспільства задіяні не лише органи державної влади, а й суб'єкти громадянського суспільства. Проаналізуємо деяких суб'єктів реалізації інформаційної політики в Україні в цьому розділі дипломної роботи.

Відповідно до Положення про Державне агентство з питань електронного урядування України [66] Державне агентство з питань електронного урядування України відповідало протягом останніх п'яти років за впровадження політики Уряду щодо електронного урядування, інформатизації, розвитку інформаційного суспільства, формування і використання національних електронних інформаційних ресурсів, цифровізації органів державної влади.

Плідної роботи потребує впровадження електронних публічних послуг. Це такі послуги, що забезпечують органи державної влади, органи місцевого самоврядування, підприємства, установи, організації, що перебувають у їх управлінні.

Ця послуга може включати адміністративні процедури, в тому числі автоматизовані, та надається за допомогою інформаційно-телекомунікаційних систем. Доступ до неї може здійснюватися на основі подання заяви (звернення, запиту), яка надходить у електронній формі через інформаційно-телекомунікаційні системи, включаючи використання Єдиного державного веб-порталу електронних послуг, або без подання такої заяви (звернення, запиту).

Електронні послуги в комплексі надаються з використанням інформаційно-телекомунікаційних систем, включаючи Єдиний державний веб-портал електронних послуг.

Надання комплексної електронної послуги відбувається на підставі заяви (звернення, запиту) суб'єкта звернення, яку він формує та подає до суб'єкта надання публічних (електронних публічних) послуг, використовуючи програмні засоби інформаційно-телекомунікаційних систем, включаючи Єдиний державний веб-портал електронних послуг, та прикладає до неї документи/відомості (при необхідності їх надання) для отримання електронних публічних послуг в рамках комплексної електронної послуги.

Інформаційно-телекомунікаційні системи, включаючи Єдиний державний веб-портал електронних послуг, надають можливість суб'єкту звернення обирати електронні публічні послуги, які він бажає отримати в рамках комплексної електронної послуги.

У випадку, якщо отримання електронної публічної послуги, що входить до складу комплексної електронної послуги, передбачає отримання іншої електронної публічної послуги відповідно до законодавства, такі послуги надаються в порядку їх послідовності.

Обмін інформацією між державними органами зазвичай відбувається через спеціальну систему електронної взаємодії. Якщо така система недоступна, дозволяється використовувати інші засоби зв'язку, але з обов'язковим захистом інформації. При цьому завжди дотримуються вимоги законів про електронні документи, захист персональних даних та захист

інформації в інформаційних системах.

Електронна взаємодія посилюється між різними органами влади. У тому числі – правоохоронними. Прикладом може бути затверджений порядок електронної інформаційної взаємодії між інформаційно-комунікаційними системами та передачі органами реєстрації інформації до Єдиного державного демографічного реєстру [14].

Цим положенням встановлено, що інформаційна взаємодія відбувається із використанням засобів системи електронної взаємодії державних електронних інформаційних ресурсів.

У разі відсутності технічної можливості щодо передачі даних із використанням каналів зв'язку системи електронної взаємодії державних електронних інформаційних ресурсів інформаційна взаємодія суб'єктів інформаційних відносин може відбуватися із використанням інших інформаційно-комунікаційних систем із застосуванням у них відповідних комплексних систем захисту інформації з підтвердженою відповідністю за результатами державної експертизи в порядку, встановленому законодавством.

Обмін інформацією здійснюється в електронній формі з дотриманням вимог Законів України "Про електронні довірчі послуги", "Про захист персональних даних", "Про захист інформації в інформаційно-комунікаційних системах" [14].

З метою реалізації механізму надання Державною податковою службою України інформації з Державного реєстру фізичних осіб - платників податків (далі - Державний реєстр) та автоматизації процесу електронної інформаційної взаємодії між Єдиною судовою інформаційно-телекомунікаційною системою (далі - ЄСІТС) та Державним реєстром було затверджено відповідне положення [67], яке полегшує роботу податкових органів та органів судового адміністрування.

Для покращення взаємодії органів державної влади з інформаційними системами та задоволення потреб громадян, а також підвищення

ефективності надання адміністративних послуг доречними є такі пропозиції.

1. Розробити Інформаційну стратегію: створити стратегію, визначальну місце та роль інформаційних систем у роботі органів державної влади, а також конкретні цілі щодо покращення обслуговування громадян.

2. Доступність та зручність: в умовах військового конфлікту ресурси можуть бути обмежені, включаючи електроенергію та підключення до Інтернету. Інформаційні системи повинні бути адаптовані до обмежень доступності ресурсів та вміти працювати в умовах обмежених можливостей, а також мають бути спроектовані таким чином, щоб бути зручними та простими у використанні навіть для людей без технічної освіти.

3. Розробка веб-порталів та мобільних програм: розробити більш зручні та інтуїтивно зрозумілі веб-портали та мобільні програми для доступу до послуг та інформації. Забезпечити адаптивний дизайн, який дозволить користувачам отримати доступ до послуг з будь-якого пристрою.

4. Поліпшення інтерфейсів користувача: зробити інтерфейси інформаційних систем більш зрозумілими і зручними для користувачів. Включити можливість використання різних мов та адаптувати інтерфейси для людей з обмеженими можливостями.

5. Електронний виборчий процес: розглянути можливість запровадження електронного голосування та електронного внесення змін до виборчого реєстру для полегшення виборчого процесу.

6. Забезпечення безпеки та конфіденційності: гарантувати надійний захист персональних даних користувачів та забезпечити конфіденційність інформації. Використовувати сучасні технології шифрування та заходи безпеки.

7. Впровадження електронного документообігу: впровадження електронного обміну документами між державними органами та громадянами/організаціями. Скорочення використання паперових документів для покращення екологічних показників.

8. Постійна підтримка та навчання: надання технічної підтримки

користувачам та реагування на їх запити. Проведення навчальних та інформаційних кампаній щодо використання інформаційних систем.

9. Участь у зворотному зв’язку: створення механізмів збору відгуків та пропозицій користувачів щодо покращення інформаційних систем та адміністративних послуг. Активна робота щодо покращення системи на основі отриманих відгуків.

10. Публікація відкритих даних: забезпечення доступу до відкритих даних, пов’язаних із діяльністю державного органу, для стимулювання інновацій та залучення громадськості.

11. Співпраця зі сторонніми розробниками: співробітництво з приватними компаніями та розробниками для створення додатків та рішень, які полегшать доступ до послуг.

12. Забезпечення доступності: забезпечення доступності інформаційних систем для всіх категорій користувачів, у тому числі людей з обмеженими можливостями [37, с.302-303].

Стратегічні документи, які затверджені у 2021 році [91], фіксують актуальні напрямки розвитку інформаційного суспільства, які мають досягти такого результату як «ефективне функціонування системи стратегічних комунікацій». Загалом ефективна стратегічна комунікація має вирішальне значення для успіху будь-якої корпоративної стратегії. Це вимагає чітких повідомлень , зрозумілих усім. Крім того, компанії повинні переконатися, що залучають менеджерів на ранній стадії та вибирають відповідні методи комунікації.

3.2 Заходи щодо ефективного захисту інформаційного простору

Слід погодитися з В. О. Кучером , що в умовах російської агресії одним із пріоритетів для держави має стати забезпечення принципів законності та

верховенства права. Роль держави полягає в утвердженні та забезпеченні прав та свобод людини, що випливає зі змісту ст. 3 Конституції України та є головним обов'язком держави. В умовах воєнного стану держава неспроможна в повній мірі гарантувати права людини, оскільки військова агресія російської федерації потребує від держави здійснювати непопулярні заходи, які обмежують окремі права людини для забезпечення безпеки та ефективності оборонних дій. Однак це не означає, що права та свободи осіб повинні повністю ігноруватися. Україна повинна вживати заходи для гарантування дотримання прав. Для цього необхідно удосконалювати нормативно-правове регулювання захисту прав людини та приведення його у відповідність до вимог міжнародних стандартів. В умовах воєнного стану пріоритетним напрямом має стати впровадження кіберстратегій, які враховують потенційні кіберзагрози та визначають заходи забезпечення безпеки в цифровому просторі. Необхідно створити ефективний механізм, який би гарантував державну інформаційну безпеку і дотримання прав людини, зокрема на тимчасово окупованих територіях. Розв'язання цих проблем вимагає комплексного підходу, який включатиме в себе технічні заходи безпеки, законодавчі та регуляторні ініціативи державно-правових інституцій [42, с.129].

З виділенням фінансування розпочав діяльність інститут безпеки штучного інтелекту. Його створення означає, що Канада йде нога в ногу з такими лідерами галузі, як Великобританія, США та Японія, які зовсім нещодавно відкрили свої інститути. Тенденція посилення уваги до дослідження безпекових аспектів використання штучного інтелекту зумовлена підвищенням рівня ризиків та загроз внаслідок стрімкого розвитку нових технологій. Намір створення інституту невдовзі після Саміту з безпеки штучного інтелекту в Блечлі-парку у листопаді 2023 р. озвучив Ф.-Ф.Шампань, міністр інновацій, науки та промисловості Канади. В момент завершення написання статті стало відомо про укладення угоди між новоствореними інститутами Канади та Великобританії (листопад 2023 р.), в

якій визначені ключові напрями співробітництва, зокрема: обмін досвідом, спільні дослідження, світові стандарти та ін. [73]. Державна політика Канади в галузі розвитку штучного інтелекту тісно пов'язана з міжнародними ініціативами з приводу управління штучним інтелектом. По-перше, Канада є активною учасницею різних форм міжнародного співробітництва, впливаючи на їхній порядок денний та прийняті рішення. Зокрема, минулого року вона очолила Тематичну робочу групу зі штучного інтелекту міжнародної міжурядової мережі Цифрових Націй, зосередившись на виробленні єдиного підходу до відповідального використання штучного інтелекту в діяльності уряду [10]. По-друге, Канада вдосконалює регулювання створення та використання технологій штучного інтелекту через запровадження міжнародних ініціатив. Наприклад, рішень міжнародного форуму «Групи семи» в рамках Хіросімського процесу зі штучного інтелекту, насамперед Міжнародних керівних принципів для організацій, які розробляють передові системи штучного інтелекту та Міжнародного кодексу поведінки для організацій, які розробляють передові системи штучного інтелекту [9]. Позитивний вплив на розвиток галузі має й освітня політика. В Канаді існує майже 150 навчальних програм різних рівнів, споріднених зі сферою створення та використання технологій штучного інтелекту.

Результати досліджень науковців показують, що з прийняттям Стратегії Канада стрімко розвиває свій науково-дослідницький потенціал у сфері штучного інтелекту. До головних організаційних чинників, завдяки яким вона досягла високого рівня розвитку галузі, можемо віднести наступні: 1) створення науково-дослідницької інфраструктури під управлінням CIFAR, до якої на початках увійшли три національні інститути, а сьогодні долучається інститут безпеки штучного інтелекту; 2) залучення та утримання кваліфікованих кадрів, серед них – іноземні дослідники та науковці (CIFAR AI Chairs); 3) формування екосистеми штучного інтелекту, яка отримує фінансову підтримку і від органів влади, і від неприбуткових організацій, і від приватного сектору; 4) сприяння зміцненню довіри населення через

забезпечення концепції відповідального штучного інтелекту, а також збільшення кількості осіб з високою кваліфікованістю зі штучного інтелекту; 5) виведення результатів досліджень з теоретичного рівня у площину практики в процесі їхньої комерціалізації, передумовою якої є сприяння патентуванню нових технічних рішень з використанням штучного інтелекту; 6) пошук збалансованих правових рамок для галузі штучного інтелекту, насамперед у вигляді кодифікованого закону з абревіатурою AIDA, на основі дотримання прав людини та з врахуванням суспільних настроїв; 7) розробка вимог та правил для стандартизації в сфері штучного інтелекту, яка відображає тенденції управління штучним інтелектом на міжнародному рівні та здійснюється Канадською радою зі стандартів; 8) активна участь в міжнародному співробітництві, що стає дедалі глибшим та ширшим, охоплюючи не тільки спільні ініціативи з іншими високорозвиненими державами «Групи семи», як-от Хіросімський процес. Такі чинники варто враховувати при удосконаленні державної політики України в сфері штучного інтелекту, створюючи передумови для реалізації та забезпечення зростання характерного для українців високого інтелектуального потенціалу [10, с.176].

Погоджуємося з висновками М. В. Александрової, що результативність впровадження електронного врядування в державному управлінні України повинна базуватись на:

1) врахуванні обставин щодо ліквідації цифрової нерівності в частині забезпечення рівного доступу до володіння комп’ютерами та гаджетами, а також щодо можливості вільного доступу до мережі Інтернет та відповідно доступу до публічної інформації;

2) розумінні місця та ролі громадянина в управлінні державою, тому що за умов упровадження моделей електронної демократії громадяни отримують і ряд обов’язків щодо прийнятих ними рішень;

3) формуванні у громадян довіри до електронних послуг, зокрема в частині інформаційної безпеки та гарантованості безпеки персональних

даних;

4) запровадженні в державному управлінні планування як важливого та водночас забутого складника забезпечить можливість громадянам брати участь в обговоренні стратегічних та нормативних документів щодо розвитку різноманітних сфер суспільного життя держави [1, с.5].

Досвід індустріально розвинутих країн засвідчує, що інформаційно-комунікаційні технології не лише виконують допоміжні функції в діяльності органів влади, а стали їхнім невід'ємним компонентом. Зокрема, можна вказати на взаємозв'язок між їхнім розвитком і здатністю різних організаційних структур вирішувати свої завдання: підвищувати конкурентоспроможність – для комерційних структур, ефективніше задовольняти потреби суспільства – для органів державної влади та місцевого самоврядування. Таким чином, інформатизація суспільства для функціонування правоохоронних органів – це перспективний напрямок розвитку нових технологій надання адміністративних послуг, проведення контролю та забезпечення рівня законності.

У той же час, на сьогодні гостро виявились і негативні аспекти, пов'язані з інформацією, зокрема її достовірністю, захистом, розповсюдженням тощо. Крім того, спостерігаються агресивні прояви інформаційної війни, що визначає необхідність не лише захисту, а й розроблення відповідної інформаційної стратегії (концепції). Недосконаліть управлінських процесів підтверджують соціологічні опитування населення України щодо довіри до органів публічної влади. Так, за результатами опитування у вересні 2023 року, що проводив Центр Разумкова більшість респондентів висловлюють недовіру політичним партіям (не довіряють 74%), державному апарату (чиновникам) (72%) [51].

Це зумовлює необхідність наукового обґрунтування удосконалення правового регулювання відносин, що виникають з приводу отримання органами державної влади України інформації, визначенні підходів до уніфікації термінів та понять, що використовуються у нормотворчій

діяльності, а також опублікування необхідної інформації органами публічної влади, у тому числі й податковими органами.

Сьогодні слід доповнювати державні заходи «забезпеченням прозорості управління публічними фінансами». З прийняттям Закону України «Про публічні послуги» і набуття ним чинності кардинально змінився процес використання коштів публічних фондів. Усі розпорядники бюджетних коштів, усі державні органи та комунальні підприємства та заклади зобов'язані виконувати норми цього Закону, оскільки вони мають оплачувати послуги через електронну систему закупівель. Це така ІТС, що має комплексну систему захисту інформації з підтвердженою відповідністю. Вона забезпечує проведення закупівель, створення, розміщення, оприлюднення, обмін інформацією і документами в електронному вигляді, до складу якої входять веб-портал Уповноваженого органу, авторизовані електронні майданчики, між якими забезпечено автоматичний обмін інформацією та документами.

Міжнародні організації, у тому числі і європейські, досліджують управлінські процеси в Україні та визначили чотири найважливіші напрямки реформування. Один із них – досягнення прозорості в сфері управління. Цей принцип, що визначений Концепцією цифрової економіки та суспільства, реалізується за допомогою використання цифрових технологій.

Цифрові технології відкривають нові можливості для залучення громадян до участі в суспільних та політичних процесах.

Традиційні (оф-лайн) демократичні процеси можуть бути переведені до цифрового формату. В Україні електронна демократія перебуває на початковому етапі розвитку і тісно пов'язана із суспільно-політичними явищами.

Головними складовими розвитку електронної демократії є е-парламент, е-голосування, е-правосуддя, е-медіація (досудове вирішення спорів), е-референдуми, е-консультації, е-петиції, е-політичні кампанії, е-опитування.

Одним з найбільш перспективних в умовах України напрямів розвитку

є електронне голосування виборців. Це найпростіша форма електронної демократії, однак її реалізація містить велику кількість політичних та організаційних викликів. Водночас саме ця форма поступово впроваджується в різних країнах світу. Оснащення процесу голосування громадян електронними засобами є питанням оптимізації виборчих технологій в Україні. Електронне голосування та вибори за відповідних умов можуть бути більш чесними, прозорими та ефективними, ніж традиційні.

Голосування через Інтернет полегшує доступ до процедури волевиявлення для значно більшої кількості громадян, підвищує загальну оперативність отримання результатів голосування, дає можливість скористатися своїм виборчим правом дистанційно.

Можливість електронного голосування в Україні дозволить залучити до виборчого процесу набагато більшу кількість громадян, особливо молодь, що покращить репрезентативність та якість виборів [36].

Отже, забезпечення прозорості управлінських процесів має велике значення. Тому державній установі «Відкриті публічні фінанси», яка виступає адміністратором порталу Єдиного вебпорталу використання публічних коштів (spending.gov.ua), слід виправити функціональні відмінності структури Порталу для відповідності вимогам, визначеним у пункті 7 Порядку адміністрування Єдиного вебпорталу використання публічних коштів, затвердженого постановою Кабінету Міністрів України від 14.09.2015 № 694 [98, с.214].

Прозорість бюджету – це проблема, якою переймаються уряди демократичних держав. Не виключенням є Україна. Мета удосконалення управлінських процесів у цій сфері – підвищення прозорості та доступності інформації про бюджет і розширення можливостей для її аналізу [80].

Одним із найбільш помітних для громадян України результатів трансформації управлінської діяльності стала можливість здійснення відкритої комунікації та отримання інформації – офіційні, нормативно-правові документи публікуються не лише у періодичних друкованих засобах

масової інформації, а й розміщуються у мережевих виданнях; органи державної влади та місцевого самоврядування публічно транслюють в інформаційних системах та власних сайтах, у мережі Інтернет заходи, пов'язані з прийняттям управлінських актів; вільний доступ до відкритих та інших даних може бути отриманий особами майже будь-якої миті часу, а не за попереднім запитом; прийом людей, зустрічі офіційних осіб країни ведуться за рахунок коштів відеоконференції та інше.

Якщо порівняти з Європейським Союзом, Україна має схожі принципи захисту персональних даних. В Україні діє Закон України "Про захист персональних даних", метою якого є захист прав та свобод громадян України від неправомірного використання їх персональних даних. Закон встановлює правила збору, зберігання, обробки та передачі персональних даних, а також відповідальність за їхнє неправомірне використання.

Доступ до інформації можна визначити як право шукати, отримувати та поширювати інформацію, якою володіють державні органи. Воно є невід'ємною частиною основного права на свободу вираження поглядів, як визнається статтею 19 Загальної декларації прав людини (1948 р.), яка зазначає, що основоположне право на свободу вираження поглядів включає свободу «шукати, отримувати та поширювати інформацію та ідеї будь-якими засобами та незалежно від кордонів".

ЮНЕСКО допомагає державам-членам дотримуватися та виконувати міжнародні договори та угоди, норми та стандарти, що стосуються універсального доступу до інформації, сприяючи розвитку суспільства знань. Доступ до інформації базується на цих міжнародно визнаних правах і охоплює основні принципи належного управління: участь, прозорість і підзвітність. Перешкоди для доступу до інформації можуть підірвати здійснення громадянських і політичних прав, а також економічних, соціальних і культурних прав. ЮНЕСКО надає засновані на фактичних даних і, у відповідних випадках, інтегровані політичні рекомендації, щоб допомогти країнам реалізувати Порядок денний на період до 2030 року та

звітувати про них, зокрема шляхом включення конституційних, законодавчих та/або політичних гарантій доступу громадськості до інформації. ЮНЕСКО надає урядам і організаціям громадянського суспільства потенціал для збору, аналізу та збільшення доступності високоякісних, своєчасних і надійних даних.

Національні уряди, головні носії обов'язків, відповідальні за прогрес у досягненні ЦСР, зобов'язані відстежувати та звітувати про прогрес у виконанні своїх зобов'язань і дій щодо гарантування доступу громадськості до інформації. Було запроваджено індикатор для відстеження прогресу щодо «кількості країн, які приймають і впроваджують конституційні, законодавчі та/або політичні гарантії доступу громадськості до інформації», приділяючи увагу двом основним компонентам такого прогрес: «прийняття» та «реалізація» [44].

Особи, чиї права на звернення до органів державної влади, органів місцевого самоврядування, посадових та службових осіб, а також право на отримання інформації та право на невтручання в особисте життя у зв'язку з обробкою їх персональних даних було порушено, можуть звернутися до суду або до Уповноваженого Верховної Ради України з прав людини для захисту своїх прав [17].

Можливо забезпечити підвищення прозорості та ефективності державних інститутів, зокрема, шляхом стандартизації та уніфікації державних управлінських та бізнес-процесів, а також застосування аутсорсингу для непрофільних функцій органів державної влади. Щодо діяльності МВС – потрібно завершувати роботу по впровадженню системи електронних послуг і вдосконалити інформаційну взаємодію сервісних центрів МВС з іншими суб'єктами публічної адміністрації.

Перехід людства до епохи інформаційного суспільства є стрімким і незворотнім, він торкається всіх сфер людської діяльності і, перш за все, державного та державного управління, де цифровізація відбуватиметься прискореними темпами і стане основним інструментом виконання функцій

держави та адміністративні послуги. Публічне управління нової ери матиме мережевий автоматизований характер, що усуне корупцію та суб'єктивізм у процесах прийняття державно-управлінських рішень, покращить якість публічних послуг, що надаються громадянам, мінімізує витрати на утримання державних службовців та загалом підвищить ефективність та результативність орган державної влади. За таких умов Україна, яка наразі перебуває поза руслом глобальної цифровізації систем державного управління, має терміново надолужувати та скорочувати «цифровий розрив» від провідних країн світу, для чого необхідно прийняти стратегічне законодавство (концепцію, стратегія, дорожня карта, Цифровий порядок денний України тощо) для розробки відповідної державної політики та проведення повномасштабної цифрової трансформації в практиці державного управління [110, с.54].

Виявлені в роботі позитивні та негативні сторони інформатизації управлінських процесів в нашій державі дають можливість здійснити проміжний висновок. Внаслідок необхідних змін відбулося спрощення бюрократичних процесів; збільшено швидкість прийняття рішень з окремих питань; створено єдину базу даних про громадян; усі державні установи та служби доступні через єдиний веб-сайт; підвищено професійні вимоги до їхньої роботи. Комп'ютеризований контроль забезпечує можливість обміну інформацією в режимі реального часу через вертикальні та горизонтальні зв'язки між центральними та місцевими органами влади, що допомагає зменшити дублювання функцій, а також цифровий розрив між різними регіонами України. Шляхом впровадження електронної інфраструктури для адміністрування та вирішення прикладних завдань метою є підвищення ефективності та поліпшення публічних послуг.

Пропонується для ефективного захисту інформаційного простору здійснити таке:

1.Посилити відповідальність за спам: ввести адміністративні санкції за масове розсилання небажаної кореспонденції без згоди користувачів.

2.Забезпечити фільтрацію шкідливого контенту: зобов’язати інтернет-провайдерів блокувати доступ до сайтів, що пропагують насильство, порнографію та інші заборонені матеріали.

3.Створити резервні копії важливих даних: розмістити національні бази даних на віддалених серверах у різних країнах для їх збереження та захисту від втрати.

ВИСНОВКИ

У роботі здійснено теоретичне узагальнення управлінських питань у сфері інформатизації та запропоновано заходи з подальшої цифровізації управлінських процесів та забезпечення інформаційної безпеки в правоохоронних органах.

Під час дослідження з'ясовано, що інформаційна політика як соціальне явище, маючи багарівневу структуру, значно ширше за змістом, ніж державна інформаційна політика, де суб'єктом виступає держава. Держава не може брати на себе вирішення всіх проблем інформаційного сектору. Існують також інші суб'єкти інформаційної політики, наприклад: політичні партії, громадські об'єднання, підприємницькі структури, трудові колективи тощо.

Інформаційне забезпечення органів публічної влади за останні десять років кардинально змінилося у бік максимального використання електронних технологій. Разом із тим сучасні умови діяльності органів влади вимагають адекватної реакції з боку органів публічної влади України.

У сфері публічного управління цифровізація значно вплинула на зміст компетенції публічних органів. Зміни, як було виявлено, виражені в змісті та кількості функцій державних і муніципальних органів, при цьому структурно-системні зміни пов'язані з такими аспектами управлінської діяльності, як: реалізація наявних повноважень, вибудовування міжвідомчої взаємодії, надання адміністративних послуг.

Встановлено, що майбутнє правоохоронних органів нерозривно пов'язане з розвитком інформаційних технологій. Впровадження сучасних ІТ-рішень відкриває нові можливості для підвищення ефективності роботи правоохоронців, покращення якості надання послуг громадянам та забезпечення безпеки держави. Інвестиції в розвиток інформаційних систем – це інвестиції в безпечне майбутнє України.

Якщо говорити про інформаційне забезпечення правоохоронців, то можна виділити такі основні моменти: 1) we процес збору, обробки та аналізу інформації про правопорушення; 2) це всі документи та дані, які потрібні поліції для роботи; 3) це інструмент для прийняття правильних рішень та ефективної роботи правоохоронців; 4) це спеціальні методи та засоби, які використовуються для роботи з інформацією; 5) це вплив на те, як люди розуміють закон і намагаються його дотримуватися.

Виявлено позитивні та негативні сторони інформатизації правоохоронних органів. Позитивні моменти виявлено у діяльності органів публічної влади на деокупованих територіях, які не маю змоги доставити оригінали документів у територіальні органи державної влади, що контролюють і координують діяльність тих, хто перебуває на деокупованих територіях. Негативні аспекти стосуються можливостей атак на ІТС, що забезпечують рух публічної та службової інформації.

Сучасний період розвитку цифрового суспільства характеризується стрімкою інформаційно-цифровою трансформацією суспільних відносин та процесів. Головною причиною суттєвих зрушень у суспільному розвитку становив науковий та технічний прогрес, заснований на впровадженні раніше невідомих методів у роботі з різноманітною інформацією. Каталізатором досягнутих змін також стало повсюдне поширення та активне проникнення цифрових каналів зв'язку, при цьому інтенсивний розвиток інформаційної інфраструктури характерний як для розвинених, так і країн. Мережа цифрових каналів зв'язку поступово продовжує своє поширення, розширення та охоплює все нові й нові території і, таким чином, дозволяє вільно шукати, отримувати, передавати, виробляти та розповсюджувати цифрову інформацію.

Відмічено зростання оперативності здійснення управлінських дій, появу нових механізмів контролю за ними, включаючи, власне, і інструментарій громадського контролю. Безумовно, цифровізація не призводить до тотального викорінення наявних проблем, пов'язаних із

можливими зловживаннями службовим становищем, корупційними ризиками, порушеннями галузевого законодавства.

Виявлено недоліки правового регулювання інформаційного забезпечення правоохоронної діяльності на сучасному етапі: неповноту, нечіткість та суперечності. Для ефективного функціонування електронного урядування необхідне оновлення законодавства з урахуванням сучасних цифрових технологій.

Важливим аспектом є захист персональних даних, особливо в умовах, наприклад, воєнного стану. Ефективність використовуваних методів реагування на інциденти, їх адаптивність до швидко змінюючихся обставин і систематичне тестування можуть виявитися критичними для збереження конфіденційної інформації. Освіта користувачів щодо можливих загроз та підготовка до них є важливим чинником у зменшенні ризику кіберзлочинності.

Ключові засоби захисту персональних даних в умовах військового стану включають фізичний захист об’єктів інформаційної інфраструктури, захист інформаційних систем і мереж, кібербезпеку та криптографічний захист даних, а також екстрені процедури реагування на інциденти. Для посилення захисту персональних даних важливо проводити освітні заходи, підвищувати обізнаність користувачів, створювати спеціалізовані підрозділи захисту персональних даних, розробляти та впроваджувати стратегії кібербезпеки, а також здійснювати міжнародне співробітництво та обмін досвідом.

Створення спеціалізованих підрозділів для забезпечення безпеки даних є ефективним, але витратним рішенням, яке потребує відповідної інфраструктури та кваліфікованих фахівців. Ці підрозділи можуть оперативно реагувати на загрози, здійснюючи моніторинг і виконуючи розширений аналіз ризиків.

Можливо забезпечити підвищення прозорості та ефективності державних інститутів, зокрема, шляхом стандартизації та уніфікації

державних управлінських та бізнес-процесів, а також застосування аутсорсингу для непрофільних функцій органів державної влади.

Міжнародне співробітництво є додатковим активом у боротьбі з кіберзлочинністю, зокрема в умовах воєнного конфлікту. Співпраця та обмін досвідом між країнами може підвищити рівень захисту даних та прискорити виявлення та реагування на потенційні загрози.

Рекомендується спрямовувати зусилля влади на створення умов для добровільного подання інформації органам державної влади та відповідно закріплення цього в законодавстві; розробку механізмів інформаційної безпеки та їх визначити у концепції інформаційної безпеки в правоохоронних органах.

Згідно з урядовою стратегією, інформатизація в системі МВС має на меті підвищити ефективність роботи правоохоронних органів за допомогою сучасних технологій. З 2018 року реалізується масштабна програма інформатизації, яка передбачає створення єдиної інформаційної системи МВС, розвиток електронних сервісів та модернізацію інфраструктури. Пріоритетними проєктами є "Безпечна країна", "Система 112" та інші, спрямовані на забезпечення безпеки громадян і ефективну роботу правоохоронних органів.

Пропонується для посилення інформаційної безпеки в нашій державі:

1. Ввести адміністративну відповідальність за спам: систематичне розсилання небажаних повідомлень без згоди одержувача.

2. Заборонити поширення шкідливого контенту в мережі: запровадити фільтрацію для блокування сайтів з насильством, порнографією та іншим забороненим матеріалом.

3. Створити захищені бази даних: зберігати важливу інформацію на віддалених серверах для забезпечення її безпеки та доступності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Александрова М. В. Адміністративно-правове забезпечення інформаційної безпеки у сфері електронного урядування: дис. … доктора філософії за спеціальністю 081 Право. − ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом». Київ, 2024. 236 с.

2. Андрій Костін: Зафіксовано понад 800 спроб кібератак рф на державні установи та сервіси України. – Режим доступу : https://www.gp.gov.ua/ua/posts/andrii-kostin-zafiksovano-ponad-800-sprob-kiberatak-rf-na-derzavni-ustanovi-ta-servisi-ukrayini

3. Безкровний Ю.А. Адміністративно-правовий режим воєнного стану. *Науковий вісник Ужгородського Національного Університету. Серія* ПРАВО. 2024. Випуск 83: частина 2. С. 139-142. DOI https://doi.org/10.24144/2307-3322.2024.83.2.19

4. Блінова Г. О. Адміністративно-правові засади інформаційного забезпечення органів публічної адміністрації в Україні: актуальні питання теорії та практики : дис. … д.ю.н. спец. 12.00.07 / Г. О. Блінова ; Запорізький національний університет. - Запоріжжя, 2019. - 545 с.

5. Блохіна О. Адміністративно-правове регулювання діяльності поліції при забезпеченні публічної безпеки та порядку в умовах воєнного стану в Україні. *Міжнародна та національна безпека: теоретичні і прикладні аспекти:* Матеріали VIII Міжнародної науково-практичної конференції (ДДУВС, 15.03.2024). Частина І. Дніпро, 2024. С. 452-454. DOI: 10.31733/15-03-2024/1/452-454

6. Войтович Р. В., Пірен М. І., Надольний І. Ф. Керівник в органах державної влади та місцевого самоврядування / Р. В. Войтович, М. І. Пірен, І. Ф. Надольний. - Київ : Центр сприяння інституційному розвитку державної служби, 2006. – 243 с.

7. Встановлення місцевих податків та зборів як вплив на місцевий

економічний розвиток : методичні рекомендації у сфері місцевого економічного розвитку / Асоціація міст України. – 2023. – Режим доступу : https://decentralization.gov.ua/uploads/library/file/848/mer_2023.pdf

8. Гавриленко Н. Інформація в умовах цифровізації публічно-правового управління / Н. Гавриленко // Економічний простір. – 2023. – №187. – С. 39-43. – Режим доступу : https://doi.org/10.32782/2224-6282/187-6

9. Гачкевич А. Хіросімський процес зі штучного інтелекту. Аналітично-порівняльне правознавство. *Юридична Україна*. 2019. № 7. С.574–583. DOI: https://doi.org/10.24144/27886018.2024.03.98.

10. Гачкевич А., Файник А., Федюра В. Організаційні чинники зростання науково-дослідницького потенціалу Канади у сфері штучного інтелекту. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО*. 2024. Випуск 83: частина 2. С. 139-142. DOI https://doi.org/10.24144/2307-3322.2024.83.2.24

11. Данильян О. Г., Дзьобань О. П., Калиновський Ю. Ю., Олєйніков Д. О. Інформаційна безпека: філософське та організаційно-правове підґрунтя рефлексії національних інтересів України ; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2024. 224 с.

12. Денисенко К. В. Реалізація цифрових та інформаційних прав людини в умовах воєнного стану / К. В. Денисенко, І. С. Борко, О. М. Косов // Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. – 2023. – Випуск 77: частина 1. – С.90-94. – DOI : https://doi.org/10.24144/2307-3322.2023.77.1.14

13. Державна інформаційна політика : навч. посіб. / заг. ред. В. Б. Дзюндзюка. – Харків: Ви-во ХарРІ НАДУ «Магістр”, 2012. – 344 с.

14. Деякі питання декларування і реєстрації місця проживання та ведення реєстрів територіальних громад: Постанова Кабінету Міністрів України від 7 лютого 2022 р. № 265. – Режим доступу : https://zakon.rada.gov.ua/laws/show/265-2022-%D0%BF#n367

15. Джига Т. В. Сучасний стан, проблеми і перспективи розвитку в

Україні електронних адміністративних послуг / Т. В. Джига ; Національний інститут стратегічних досліджень при Президентові України. – Режим доступу : http://www.niss.gov.ua/articles/1716

16. Дзюндзюк В. Б. Розвиток публічного управління у XXI сторіччі: тенденції та виклики / В. Б. Дзюндзюк // Актуальні проблеми державного управління : зб. наук. пр. – Харків : Вид-во ХарРІ НАДУ «Магістр”, 2013. – № 1 (43). – С. 9–17.

17. Для ДПС важливим є недопущення порушень інформаційних прав платників податків та їх права на приватність / Сайт Державної податкової служби України. – Режим доступу : https://tax.gov.ua/baneryi/vseukrainskiy-tijden-prava/print-399278.html

18. Європейський Союз позитивно оцінив імплементацію реформ в Україні : річний звіт ЄС. – Режим доступу: http://eu-ua.org/novyny/yevropeyskyy-soyuz-pozytyvno-ocinyv-implementaciyu-reform-v-ukrayini-richnyy-zvit-yes?fbclid=IwAR2eIsDn0nZ1C0vim_gjIS8YJ1gI0nyvPKtuh_D0AK-imPjIqUcRsHbF-b4 (дата звернення: .04.11.2024).

19. Єдиний державний портал адміністративних послуг. – Режим доступу : poslugy.gov.ua

20. Желновач Є. Г. Правові аспекти інформаційного суспільства в Україні в умовах воєнного стану / Є. Г. Желновач // Юридичний бюлетень. – 2023. – №28. – С. 100-109. – DOI : https://doi.org/10.32850/LB2414-4207.2023.28.14

21. За 2023 рік кіберполіція виявила понад 3600 кіберзлочинів – Режим доступу : https://suspilne.media/673484-za-2023-rik-kiberpolicia-viavila-ponad-3600-kiberzlociniv/

22. Звіт Кабінету Міністрів України про виконання Плану дій із впровадження Ініціативи «Партнерство «Відкритий Уряд” у 2021-2022 роках. – Режим доступу : chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.kmu.gov.ua/storage/a

pp/sites/1/17-civik-2018/partnerstvo/zvit-ogp-2021-2022_.pdf

23. Звіт про результати аудиту ефективності виконання повноважень органами виконавчої влади в частині реєстрації та обліку платників податків : затверджено Рішенням Рахункової палати від 11.07.2023 р. № 14-2. – Режим доступу : http://rp.gov.ua/upload-files/Activity/Collegium/2023/14-2_2023/Zvit_14-2_2023.pdf

24. Звіт про стан виконання Плану заходів з реалізації стратегічних цілей діяльності ДПС на 2021 рік : затвердженого наказом ДПС від 30.07.2020 р. № 376 (зі змінами). – Режим доступу : https://tax.gov.ua/diyalnist-/plani-ta-zviti-roboti-/430665.html

25. Інструменти забезпечення ефективності, результативності та якості діяльності органів державної влади / заг. ред. В. Купрія. – Київ : Центр адаптації державної служби до стандартів Європейського Союзу, 2017. – 178с.

26. Інтелектуальні інформаційні технології та системи. – Режим доступу : http://nbuv.gov.ua/sites/default/files/all_files/references/201603/vtdo_ro_7.pdf

27. Інформатизація системи МВС. – Режим доступу : https://mvs.gov.ua/uk/ministry/projekti-mvs/informatizaciya-sistemi-mvs-ukrayini

28. Калєніченко Н. ДПС оцифровано майже 99 % сервісів та послуг / Н. Калєніченко. – Режим доступу : https://tax.gov.ua/media-tsentr/novini/455002.html

29. Капля О.М. Правове регулювання інформаційної безпеки громадянина під час воєнного стану / О. М. Капля. – Режим доступу : http://journals.maup.com.ua/index.php/expert/article/view/2329/2811

30. Кастельс М. Інформаційне суспільство та держава добробуту. Фінська модель / Мануель Кастельс, Пекка Хіманен. – Київ : Вид. «Ваклер”, 2006. – 232 с.

31. Катерлін І. Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав громадян / І. Б. Катерлін // Актуальні проблеми вітчизняної юриспруденції. – 2022. – № 1. – Режим

доступу : http://apnl.dnu.in.ua/1_2022/25.pdf

32. Клімова С. М. Оптимізація інформаційно-правового забезпечення управління публічними фінансами / С. М. Клімова // Правова держава. – 2018. – № 32. – С. 85–92.

33. Клімова С. М. Посилення захисту інформації про публічні фінанси в Україні з урахуванням стандартів Європейського Союзу / С. М. Клімова // Правові засади діяльності правоохоронних органів : матеріали VI Міжнародної науково-практичної конференції, 5-6 грудня 2019 р. – Харків : Точка, 2019. – С. 39–41.

34. Конституція України : прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 року. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/254к/96-вр

35. Концепція розвитку системи електронних послуг в Україні : схвалено розпорядженням Кабінету Міністрів України від 16 листопада 2016 р. № 918-р. – Режим доступу : https://zakon.rada.gov.ua/laws/show/918-2016-%D1%80#Text

36. Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки: схвалено розпорядженням Кабінету Міністрів України від 17 січня 2018 р. № 67-р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text

37. Коцюба К. Взаємодія органів публічної влади та інформаційних систем органів публічної влади в контексті надання адміністративних послуг населенню. *Науковий вісник: Державне управління*. 2023. 2(14). С.302-303. – Режим доступу : https://nvdu.undicz.org.ua/index.php/nvdu/article/view/331/295

38. Кравчук В. О. Захист персональних даних в умовах воєнного стану / В. О. Кравчук // Юридичний науковий електронний журнал. – 2022. – № 9. – С. 319–321. – DOI : https://doi.org/10.32782/2524-0374/2022-9/77

39. Критерії визначення підприємств, установ та організацій, які мають важливе значення для галузі національної економіки в інформаційній сфері : затверджено наказом Міністерства культури та інформаційної

політики від 10.03.2023 р. № 106. – Режим доступу : https://zakon.rada.gov.ua/laws/show/z0513-23#Text

40. Крупнова А. Система суб'єктів адміністративно-правового забезпечення інформаційної безпеки в Україні. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО*. 2024. Випуск 83: частина 2. С. 277-287. DOI https://doi.org/10.24144/2307-3322.2024.83.2.40

41. Купріянова А. О. Забезпечення відновлення функцій держави на деокупованих територіях територіальних громад органами і підрозділами Міністерства юстиції України / А. О. Купріянова // Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування. – 2023. – Том 34 (73). – № 1. – DOI : https://doi.org/10.32782/TNU-2663-6468/2023.1/23

42. Кучер В. О. Права людини та інформаційна безпека в умовах військової агресії. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО*. 2024. Вип. 81: Ч. 1. С. 125-130. DOI https://doi.org/10.24144/2307-3322.2024.81.1.19

43. Мігалатюк В. В. Інформаційне забезпечення адміністративної діяльності правоохоронних органів. *Наукові записки. Серія: Право | Scientific notes. Series: Law.* 2024. Вип. 16. С. 128-132. DOI: https://doi.org/10.36550/2522-9230-2024-16-128-132

44. Моніторинг та звітність щодо доступу до інформації. – Режим доступу : https://www.unesco.org/en/monitoring-access-information

45. Мохор В. В., Цуркан В. В., Дорогий Я. Ю., Штифурак Ю. М. Структури архітектури систем управління інформаційною безпекою. *Informatics & Mathematical Methods in Simulation*, 2019. № 9(4).

46. Наливайко Л. Р. Інформаційна безпека та інформаційна політика в Україні: конституційноправовий аспект / Л. Р. Наливайко // Вісник Запорізького державного університету. – 2003. – № 1. – С. 60–65.

47. Наливайко Л. Р. Теоретико-правова характеристика взаємодії органів судової влади та інститутів громадянського суспільства : монографія / Л. Р. Наливайко, В. М. Олійник. – Дніпро : ДДУВС, 2019. – 192 с.

48. Орлова О.С. Правове регулювання господарської діяльності в умовах цифровізації / О. С. Орлова // Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. – 2023. – Вип. 77: ч. 1. – DOI : https://doi.org/10.24144/2307-3322.2023.77.1.31

49. Основи публічного права України : навч. посібник / кол. авт. ; за заг. ред. к.ю.н., проф. А.Ю. Олійника, к.ю.н., доц. М.І. Кагадія. – К. : КНУТД ; Дніпро : Ліра ЛТД, 2017. – 448 с.

50. Особливості плати за землю в період воєнного стану. Хто та за яких умов може не платити. Останні законодавчі зміни // Децентралізація : інтернет-ресурс. – 2023. – 8 грудня. – Режим доступу : https://decentralization.gov.ua/news/16602

51. Оцінка громадянами ситуації в країні. Довіра до соціальних інститутів, політиків, посадовців та громадських діячів. Ставлення до проведення загальнонаціональних виборів в Україні до завершення війни (вересень 2023р.) / Сайт Українського центру економічних та політичних досліджень ім. О. Разумкова. – Режим доступу : https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/otsinka-gromadianamy-sytuatsii-v-kraini-dovira-do-sotsialnykh-instytutiv-politykiv-posadovtsiv-ta-gromadskykh-diiachiv-stavlennia-do-provedennia-zagalnonatsionalnykh-vyboriv-v-ukraini-do-zavershennia-viiny-veresen-2023r

52. Оцінка діяльності центрів надання послуг у 40 містах України // Центр політико-правових реформ (ЦППР). – 2015. – 24 грудня. – Режим доступу : http://pravo.org.ua/ua/news/20871203-otsinka-diyalnosti-tsentriv-nadannya-poslug-u-40-mistah-ukrayini.

53. Пак Н. Громадський контроль діяльності органів публічної влади: сутність та механізми здійснення / Н. Пак, Є. Воронець // Молодий вчений. - 2021. – № 9 (97). – С. 138-142. – DOI : https://doi.org/10.32839/2304-5809/2021-9-97-28

54. Перелік інформаційних систем органів державної влади, доступ до яких як користувач має Державне бюро розслідувань : затверджено

постановою Кабінету Міністрів України від 15 вересня 2023 р. № 1004. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1004-2023-%D0%BF#Text

55. Положення про електронну взаємодію електронних інформаційних ресурсів : затверджено постановою КМУ від 8 вересня 2016 р. № 606. – Режим доступу : https://ips.ligazakon.net/document/KP160606?an=19&ed=2022_11_18

56. Про CERT-UA. – Режим доступу : https://cert.gov.ua/about-us

57. Про адміністративні послуги : Закон України від 06.09.2012 р. № 5203-VI // Верховна Рада України : офіційний веб-портал. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/5203-17.

58. Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів : Закон України від 15.03.2022 р. № 2130-IX. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2130-20#Text

59. Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції : Закон України від 03.03.2022 р. № 2110-IX // Голос України. – 2022. - № 56. – Режим доступу : https://zakon.rada.gov.ua/ laws/show/2110-20#Text

60. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану : Закон України від 24.03.2022 р. № 2160-IX // Голос України. – 2022. – № 67. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2160-20#n10

61. Про державну допомогу суб’єктам господарювання: Закон

України від 01.07.2014 №1555. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1555-18#Text

62. Про запровадження Національної системи індикаторів розвитку інформаційного суспільства : постанова Кабінету Міністрів України від 28.11.2012 р. № 1134-2012-п // Урядовий кур'єр. – 2012. – № 234. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1134-2012-%D0%BF#Text

63. Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту систем електронного документообігу, затверджено наказом Адміністрації Держспецзв'язку від 30.08.2023 № 773. – Режим доступу : https://zakon.rada.gov.ua/rada/show/v0773519-23#Text

64. Про затвердження плану заходів з виконання завдань, передбачених Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" : розпорядження Кабінету Міністрів України від 15.08.2007 р. № 653-р. – Режим доступу : https://zakon.rada.gov.ua/laws/show/653-2007-%D1%80#Text

65. Про затвердження Положення про Департамент кіберполіції Національної поліції України: наказ Національної поліції України 10.11.2015 №85.

66. Про затвердження Положення про Державне агентство з питань електронного урядування України : постанова Кабінету Міністрів України від 1 жовтня 2014 р. № 492. (втратила чинність на підставі Постанови КМУ № 645 від 27.06.2023 р.). – Режим доступу : https://zakon.rada.gov.ua/laws/show/492-2014-%D0%BF#Text

67. Про затвердження Порядку електронної інформаційної взаємодії між інформаційно-комунікаційними системами Державної податкової служби України та Державної судової адміністрації України: накази Міністерства фінансів України, Державної судової адміністрація України від 24.06.2024 № 304/262; реєстрація Мін'юст України від 05.07.2024 № 1020/42365. – Режим доступу : https://zakon.rada.gov.ua/laws/show/z1020-24#Text

68. Про затвердження форм документів, що складаються при проведенні заходів державного нагляду (контролю) щодо дотримання вимог законодавства у сфері електронних довірчих послуг : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 24.12.2020 р. № 842. – Режим доступу : https://zakon.rada.gov.ua/laws/show/z0178-21#n15

69. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286. – Режим доступу : https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

70. Про Національну програму інформатизації : Закон України від 01.12.2022 р. № 2807-IX // Голос України. – 1998. – № 65. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2807-20#Text

71. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 р. № 537-V // Відомості Верховної Ради України (ВВР). – 2007. – № 12. – Ст. 102. – Режим доступу : https://zakon.rada.gov.ua/laws/show/537-16#Text

72. Про особливості надання публічних (електронних публічних) послуг : Закон України від 15.07.2021 р. № 1689-IX // Голос України. – 2021. – № 149. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1689-20#Text

73. Про правовий режим воєнного стану : Закон України від 12.05.2015 р. № 389-VIII // Голос України. – 2015. – № 101. – Режим доступу : https://zakon.rada.gov.ua/laws/show/389-19#Text

74. Про публічні закупівлі : Закон України від 25.12.2015 р. № 922-VIII // Голос України. – 2016. – № 30. – Режим доступу : https://zakon.rada.gov.ua/laws/show/922-19#Text

75. Про Рекомендації парламентських слухань на тему: «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України": постанова Верховної Ради України від 31.03.2016 р. № 1073-VII // Відомості Верховної Ради (ВВР). – 2016. – № 17. – Ст. 191. –

Режим доступу : https://zakon.rada.gov.ua/laws/show/1073-19#Text

76. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» : Указ Президента України від 19 березня 2022 року № 152/2022 // Урядовий кур'єр. – 2022. - № 62. – Режим доступу : https://zakon.rada.gov.ua/go/152/2022

77. Про співробітництво територіальних громад : Закон України 17.06.2014 р. № 1508-VII // Голос України. – 2014. – № 138. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1508-18#Text

78. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації : розпорядження Кабінету Міністрів України від 3 березня 2021 р. № 167-р // Урядовий кур'єр. – 2021. - № 50. – Режим доступу : https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text

79. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації : розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р // Урядовий кур'єр. – 2018. - № 88. – Режим доступу : https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#n13

80. Про схвалення Стратегії реформування системи управління державними фінансами на 2022-2025 роки та плану заходів з її реалізації : розпорядження Кабінету Міністрів України від 29 грудня 2021 р. № 1805-р // Урядовий кур'єр. – 2022. – № 13. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1805-2021-%D1%80#Text

81. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386-р // Урядовий кур'єр. – 2019. – № 143. – Режим доступу : https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text

82. Проект плану відновлення України : матеріали робочої групи «Діджиталізація" // URC2022 : Конференція з питань відновлення України.

Лондон, 21-22 червня. – Режим доступу : https://www.kmu.gov.ua/storage/app/sites/1/recoveryrada/ua/digitization.pdf (дата звернення: 05.10.2023).

83. Проєкт Концепції інформаційної безпеки України // OSCE. – Режим доступу : https://www.osce.org/files/f/documents/0/2/175056.pdf

84. Радзієвська О. Г. Проблеми забезпечення прав і безпеки людини в інформаційній сфері / О. Г. Радзієвська // Забезпечення прав людини: національний та міжнародний виміри : зб. матеріалів І Всеукраїнської науково-практичної конференції (м. Вінниця, 10 грудня 2021 року). – Вінниця, 2022. – С. 111-116.

85. Разумей Г. Ю. Діджиталізація публічного управління як складник цифрової трансформації України / Г. Ю. Разумей, М. М. Разумей // Публічне управління та митне адміністрування. – 2020. – № 2 (25). – С.139-145. – DOI : https://doi.org/10.32836/2310-9653-2020-2.25

86. Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні : схвалені Постановою Верховної Ради України від 1 грудня 2005 року № 3175-IV. – Режим доступу : https://zakon.rada.gov.ua/laws/show/3175-15#Text

87. Ряполов А. П. Теоретико-правова характеристика інформаційної безпеки в умовах воєнного стану / А. П. Ряполов // Modernization of science and its influence on global processes. – 2023. – April 14. – С. 41-43.

88. Салаєв Т. Г. Адміністративно-правове забезпечення інформаційної безпеки у митній сфері : дис. … доктора філософії з галузі знань 08 «Право" за спеціальністю 081 «Право" / Т. Г. Салаєв // Інститут законодавства Верховної Ради України. – Київ, 2021. – 250 с.

89. Серебро М. В. Адміністративно-правові засади використання та розвитку інформаційних технологій в Україні. *Право і суспільство*. 2024. №4. DOI https://doi.org/10.32842/2078-3736/2024.4.33

90. Сопілко І. М. Правове регулювання відносин щодо отримання органами державної влади України інформації : дис. … к.ю.н. / І. М. Сопілко ;

Кримський юридичний інститут Одеського державного університету внутрішніх справ, 2010.

91. Стратегія інформаційної безпеки: затверджено Указом Президента України від 28 грудня 2021 року № 685/2021. – Режим доступу : https://zakon.rada.gov.ua/laws/show/685/2021#Text

92. Стратегія національної безпеки України : указ Президента України від 14 вересня 2020 р. № 392/2020. – Режим доступу : https://zakon.rada.gov.ua/laws/show/392/2020?find=1&text= %D0%BE%D1%82%D1%80%D0%B8%D0%BC%D0%B0%D0%BD%D0%BD%D1%8F+%D1%83%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B6%D1%83#w2_1

93. Тимощук В. П. Адміністративні послуги: проблеми теорії, законодавства і практики в Україні / В. П. Тимощук // Адміністративне право і процес : науково-практичний журнал заснований Київським національним університетом імені Тараса Шевченка. – Режим доступу : http://applaw.knu.ua/index.php/arkhiv-nomeriv/3-9-2014-jubilee/item/383-administratyvni-posluhy-problemy-teoriyi-zakonodavstva-i-praktyky-v-ukrayini-tymoshchuk-v-p

94. У III кварталі 2023 р. кількість зареєстрованих кіберінцидентів зросла на 46% - Держспецзв'язку. – Режим доступу : https://interfax.com.ua/news/telecom/943392.html

95. Фурашев В. М. Електронне інформаційне суспільство України: погляд у сьогодення і майбутнє : монографія / В. М. Фурашев, Д. В. Ланде, О. М. Григор'єв, О. В. Фурашев. – К. :Інжинірін, 2005. – 164 с.

96. Фурман В. В. Право на інформацію в системі конституційних прав людини і громадянина. *Правничий часопис Донецького національного університету імені Василя Стуса.* 2024. №1. С. 100-110. DOI: https://doi.org/10.31558/2786-5835.2024.1.11 https://jpchdnu.donnu.edu.ua/article/view/16164/16058

97. Щодо обстановки в сфері кібер на 23-24 лютого 2024 року. – Режим доступу : https://cert.gov.ua/article/6277822

98. Щорічна доповідь про стан додержання та захисту прав і свобод людини і громадянина в Україні за 2022 рік / Уповноважений Верховної Ради України з прав людини. – Режим доступу : https://ombudsman.gov.ua/report-2022/

99. AI Allies: UK and Canada Sign New AI Safety Partnership. URL: https://nationalsecuritynews. com/2024/05/ai-allies-uk-and-canada-sign-new-ai-safety-partnership/ (дата 05.06.2024 р.). звернення:

100. Bryhinets O. Problems of intellectual property in the national security system of the country / O. Bryhinets, R. Shapoval, A. Bakhaieva, V. Pchelin, A. Fomenko // Entrepreneurship and Sustainability. - 2021. - № 8(3). - P. 471-486.

101. Council Regulation (EC) № 2012/2002 of 11 November 2002 establishing the European Union Solidarity Fund // Official Journal. L 311, 14/11/2002. - P. 0003–0008. – Режим доступу : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002R2012 (accessed: 05.10.2021).

102. Digital Nations Shared Approach to the Responsible Use of Artificial Intelligence in Government (2023). URL: https://www.leadingdigitalgovs.org/canada (дата звернення: 05.06.2024 р.).

103. Hryshko A. Uberization of public authorities: consolidation of innovative approaches to interaction with citizens in the conditions of transparent activity / A. Hryshko // Молодий вчений. – 2021. – № 1(1). – С. 38-41. – Режим доступу : http://nbuv.gov.ua/UJRN/molv_2021_1%281%29__10

104. Kramer F. D. Cyberpower and national security / F. D. Kramer, S. H. Starr, L. K. Wentz (Eds.). - Nebraska : Potomac Books, Inc, 2019.

105. Leheza Y. Principles of law: Methodological approaches to understanding in the context of modern globalization transformations / Y. Leheza, L. Nalyvaiko, O. Sachko, V. Shcherbyna, O. Chepik-Trehubenko // Ius Humani. Law Journal. – 2022. – 11 (2). – P. 55-79. – DOI : https://doi.org/https://doi.org/10.31207/ih.v11i2.312

106. Lyall C. The Limits to Governance: The Challenge of Policymaking for the New Life Sciences / C. Lyall, T. Papaioannou, J. Smith. – Farnham : Ashgate Publishing Limited, 2009. – 284 p.

107. Minakova Ye. Public participation in the mechanism of prevention and anti-corruption in ukraine / Ye. Minakova, I. Nalyvaiko // KELM (Knowledge, Education, Law, Management). – 2022. – № 7 (51). – P.167-173.

108. Nalyvaiko L. R. Transparency as a democratic standard of the government functioning / L. R. Nalyvaiko // Evropský Politický a Právní Diskurs. – 2014. – Svazek 1., 4. vydání. – C. 51-62.

109. Pratchett L. Understanding e-democracy developments in Europe / L. Pratchett // International Centre of Excellence for Local e-Democracy. – United Kingdom : [s. n.], 2006. – Режим доступу: http://www.dmu.ac.uk.

110. Shandryk Viacheslav. Digitalization of public administration systems as a relevant component of the information society era. *Eurasian Academic Research Journal.* 2021 № 38. P. 54-61.

111. Urintsov A. I. Information society as an environment for creating new knowledge / A. I. Urintsov, V. V. Dik, N. A. Kameneva, Ye. V. Makarenkova // Науковий вісник Національного гірничого університету. – 2014. – № 4. – С. 113-120. – Режим доступу : http://nbuv.gov.ua/UJRN/Nvngu_2014_4_21

ДОДАТКИ

Додаток А

Напрямки інформатизації роботи органів МВС [використано джерело 27]

Додаток Б

Інформація про стан виконання заходів плану дій із впровадження Ініціативи “Партнерство “Відкритий Уряд” у 2021 - 2022 роках [22]

Орган виконавчої влади, відповідальний за виконання заходу	Основні кроки	Опис результатів
1	2	3
Забезпечення використання інструментів електронної демократії у взаємодії органів виконавчої влади з громадянами, інститутами громадянського суспільства		
Мінцифри, Секретаріат Кабінету Міністрів України	1. Розроблення нормативно-правових актів для врегулювання питань функціонування онлайн- платформи “ВзаємоДія”	У зв’язку з повномасштабним вторгненням рф роботу було призупинено. Відповідно до підпункту 3 пункту 4 Положення Мінцифри відповідно до покладених на нього завдань здійснює заходи щодо створення та забезпечення функціонування, зокрема онлайн-платформи взаємодії органів виконавчої влади з громадянами та інститутами громадянського суспільства. Інформаційна сторінка про онлайн-платформу взаємодії органів виконавчої влади з громадянами та інститутами громадянського суспільства (платформа ВзаємоДія) доступна за посиланням. Водночас, через повномасштабне вторгнення рф в Україну та з метою збереження цілісності та конфіденційності інформації, недопущення несанкціонованого втручання та спотворення даних, залишено можливість використання онлайн-платформи взаємодії органів виконавчої влади з громадянами та інститутами громадянського суспільства (платформа ВзаємоДія) виключно у частині простору електронних конкурсів.
Мінцифри	2. Визначення вимог до модулів другого етапу впровадження онлайн- платформи “ВзаємоДія” (для подання електронних звернень громадян, запитів на публічну інформацію,	У зв’язку з повномасштабним вторгненням рф роботу було призупинено. Проведено аналітичну роботу та спільно з партнерами підготовлено “policy paper” щодо електронних петицій публічних консультацій та електронних опитувань, на основі чого розроблятимуться технічні вимоги до відповідних модулів. Водночас, через повномасштабне

	голосування під час формування складу громадських рад при органах виконавчої влади, проведення електронних консультацій, електронних опитувань тощо)	вторгнення рф в Україну та з метою збереження цілісності та конфіденційності інформації, недопущення несанкціонованого втручання та спотворення даних, залишено можливість використання онлайн-платформи взаємодії органів виконавчої влади з громадянами та інститутами громадянського суспільства (платформа ВзаємоДія) виключно у частині простору електронних конкурсів.
Мінцифри	3. Розроблення модулів другого етапу впровадження онлайн-платформи “ВзаємоДія”	У зв’язку з повномасштабним вторгненням рф роботу було призупинено
Мінцифри	4. Проведення інформаційної кампанії щодо використання онлайн-платформи “ВзаємоДія”	У зв’язку з повномасштабним вторгненням рф роботу було призупинено. Громадські організації було залучено до тестування модуля онлайн-платформи ВзаємоДія “Конкурси проєктів інститутів громадянського суспільства” шляхом розміщення анкети та проведення відбору на інформаційних ресурсах Мінцифри, Секретаріату Кабінету Міністрів та програми “Електронне врядування. Онлайн-платформа «ВзаємоДія” працює у режимі дослідної експлуатації та доступна за посиланням: https://vzaemo.diia.gov.ua/. 13.09.2021 р. презентовано модуль “Простір електронних конкурсів” онлайн-платформи “ВзаємоДія”. Водночас, через повномасштабне вторгнення рф в Україну та з метою збереження цілісності та конфіденційності інформації, недопущення несанкціонованого втручання та спотворення даних, залишено можливість використання онлайн-платформи взаємодії органів виконавчої влади з громадянами та інститутами громадянського суспільства (платформа ВзаємоДія) виключно у частині простору електронних конкурсів.

Продовження додатку Б

Утворення національного центру компетенцій в сфері відкритих даних		
1	2	3
Мінцифри	1. Внесення змін до нормативно-правових актів	Виконано. 03.03.2021 р. прийнято постанову Кабінету Міністрів № 407 “Про внесення змін до постанов Кабінету Міністрів України, якою, передбачено забезпечення створення та функціонування Центру компетенцій в сфері відкритих даних “Дія. Відкриті дані”.
Мінцифри	2. Введення в дослідну експлуатацію національного центру компетенцій в сфері відкритих даних	Виконано. Створено демо-версію, розроблено дизайн Центру компетенцій в сфері відкритих даних “Дія. Відкриті дані”, підготовлено контент-план для його наповнення.
Мінцифри	3. Введення в експлуатацію національного центру компетенцій в сфері відкритих даних	Виконано. 18.05.2021 р. введено в експлуатацію Центр компетенцій в сфері відкритих даних “Дія. Відкриті дані”, який є невід’ємною частиною Єдиного державного веб-порталу відкритих даних.

Додаток В

Система заходів кіберзахисту

Категорія заходів кіберзахисту	Опис	Заходи кіберзахисту
1	2	3
Клас заходів кіберзахисту "Ідентифікація ризиків кібербезпеки" (ID)		
ID.AM Управління активами	Описуються дані, персонал, пристрої та носії інформації, інформаційні системи, що дозволяють забезпечити стале функціонування СЕД, а також описується політика управління ризиками.	ID.AM-1 ID.AM-2 ID.AM-3 ID.AM-4 ID.AM-5 ID.AM-6
ID.BE Середовище надання життєво важливих послуг та функцій	Формування обов'язків персоналу щодо забезпечення кібербезпеки, а також рішень з управління ризиками у сфері кібербезпеки.	ID.BE-1 ID.BE-2 ID.BE-3 ID.BE-4 ID.BE-5
ID.GV Управління безпекою	Формування правил, процедур і процесів для управління й моніторингу впроваджених нормативних, екологічних та експлуатаційних вимог, а також вимог щодо забезпечення кібербезпеки.	ID.GV-1 ID.GV-2 ID.GV-3 ID.GV-4
ID.RA Оцінка ризиків	Визначення ризиків у сфері кібербезпеки для СЕД.	ID.RA-1 ID.RA-2 ID.RA-3 ID.RA-4

Продовження додатку В

		ID.RA-5 ID.RA-6
ID.RM Стратегія управління ризиками організації	Визначення пріоритетів, обмежень, допустимого рівня ризику для підтримки рішень щодо зниження ризиків кібербезпеки.	ID.RM-1 ID.RM-2 ID.RM-3
ID.SC Управління ризиками системи постачання	Визначення пріоритетів, обмежень, допустимого рівня ризику щодо системи постачання для підтримки рішень щодо ризиків, пов'язаних із системою постачання послуг третіми особами.	ID.SC-1 ID.SC-2 ID.SC-3 ID.SC-4 ID.SC-5
Клас заходів кіберзахисту "Кіберзахист" (PR)		
PR.AC Управління ідентифікацією, автентифікацією та контроль доступу	Забезпечення доступу до фізичних і логічних ресурсів СЕД та пов'язаних з ними об'єктів тільки для авторизованих користувачів, адміністраторів або процесів. Управління здійснюється з урахуванням встановленого допустимого рівня ризику несанкціонованого доступу.	PR.AC-1 PR.AC-2 PR.AC-3 PR.AC-4 PR.AC-5 PR.AC-6 PR.AC-7

Продовження додатку В

PR.AT Обізнаність та навчання	Забезпечення інформування та обізнаності співробітників організації та партнерів організації щодо питань кіберзахисту СЕД. Співробітники мають освіту або пройшли спеціалізовану підготовку для покращення інформованості з питань кібербезпеки, пройшли належну підготовку для виконання своїх обов'язків щодо забезпечення кіберзахисту СЕД відповідно до встановлених політик, правил, процедур та угод.	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5
PR.DS Безпека даних	Забезпечення управління інформацією та документацією з метою захисту конфіденційності, цілісності та доступності інформації.	PR.DS-1 PR.DS-2 PR.DS-3 PR.DS-4 PR.DS-5 PR.DS-6 PR.DS-7 PR.DS-8
PR.IP Процеси та процедури кіберзахисту	Забезпечення підтримання та управління політикою (правилами) безпеки, процесами та процедурами, які використовуються для управління захистом СЕД.	PR.IP-1 PR.IP-2 PR.IP-3 PR.IP-4 PR.IP-5 PR.IP-6 PR.IP-7 PR.IP-8 PR.IP-9 PR.IP-10 PR.IP-11 PR.IP-12
PR.MA Технічне обслуговування	Технічне обслуговування та ремонт компонентів СЕД виконуються з дотриманням правил та процедур безпеки.	PR.MA-1 PR.MA-2

Продовження додатку В

PR.PT Технології кіберзахисту	Управління технічними рішеннями (технологіями) кіберзахисту з метою забезпечення безпеки та стійкості СЕД з дотриманням правил, процедур з безпеки.	PR.PT-1 PR.PT-2 PR.PT-3 PR.PT-4 PR.PT-5
Клас заходів кіберзахисту "Виявлення кіберінцидентів" (DE)		
DE.AE Аномалії та кіберінциденти	Своєчасне виявлення аномальної активності та передбачення потенційного впливу кіберінцидентів.	DE.AE-1 DE.AE-2 DE.AE-3 DE.AE-4 DE.AE-5
DE.CM Безперервний моніторинг кібербезпеки	Відстеження безпеки СЕД через дискретні інтервали для виявлення кіберінцидентів та перевірки ефективності заходів кібербезпеки.	DE.CM-1 DE.CM-2 DE.CM-3 DE.CM-4 DE.CM-5 DE.CM-6 DE.CM-7 DE.CM-8
DE.DP Процеси виявлення кіберінцидентів	Підтримання і тестування процесів й процедур виявлення кіберінцидентів для забезпечення своєчасного та адекватного оповіщення про аномальні кіберінциденти.	DE.DP-1 DE.DP-2 DE.DP-3 DE.DP-4 DE.DP-5
Клас заходів кіберзахисту "Реагування на кіберінциденти" (RS)		

Продовження додатку В

RS.RP Планування реагування	Процеси та процедури в СЕД реагування на кіберінциденти виконуються та підтримуються з метою забезпечення своєчасного реагування на виявлені кіберінциденти.	RS.RP-1
RS.CO Комунікації	Координація заходів з реагування між внутрішніми та зовнішніми партнерами організації (у разі доцільності).	RS.CO-1 RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5
RS.AN Аналіз	Проведення аналізу кіберінцидентів для забезпечення адекватних заходів реагування та підтримки відновлення.	RS.AN-1 RS.AN-2 RS.AN-3 RS.AN-4 RS.AN-5
RS.MI Мінімізація наслідків	Виконання заходів з метою запобігання поширенню кіберінциденту, мінімізації його наслідків та унеможливлення його повторення.	RS.MI-1 RS.MI-2 RS.MI-3
RS.IM Удосконалення	Удосконалення заходів з реагування шляхом врахування досвіду з поточних або виконаних заходів виявлення/реагування.	RS.IM-1 RS.IM-2
Функція кібербезпеки "Відновлення стану кібербезпеки" (RC)		

Продовження додатку В

RC.RP Планування відновлення	Процеси та процедури відновлення в СЕД виконуються та підтримуються з метою своєчасного відновлення.	RC.RP-1
RC.IM Удосконалення	Планування відновлення та процеси відновлення удосконалюються шляхом урахування отриманого досвіду.	RC.IM-1 RC.IM-2
RC.CO Комунікації	Заходи з відновлення координуються з внутрішніми та зовнішніми партнерами організації, такими як координаційні центри, постачальники електронних комунікаційних мереж та/або послуг, власники атакуючих систем, інші групи реагування на інциденти, пов'язані з інформаційною та/або кібербезпекою (CSIRT).	RC.CO-1 RC.CO-2 RC.CO-3