Чорноморський національний університет імені Петра Могили
(повне найменування вищого навчального закладу)

Навчально-науковий інститут публічного управління та адміністрування
(повне найменування інституту, назва факультету (відділення))

кафедра публічного управління та адміністрування
(повна назва кафедри (предметної, циклової комісії))

«Допущено до захисту»
Завідувач кафедри публічного
управління та адміністрування
_____ О.Н. Євтушенко
“____” _____2024 року

КВАЛІФІКАЦІЙНА РОБОТА
на здобуття ступеня вищої освіти
магістр
(ступінь вищої освіти)

на тему: **БЕЗПЕКОВІ ПИТАННЯ ФУНКЦІОНУВАННЯ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В СФЕРІ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ВОЄННОГО СТАНУ**

Керівник: кандидат наук з державного управління, доцент
Шульга Анастасія Алімівна
(вчене звання, науковий ступінь, П.І.Б.)

Рецензент: доктор політичних наук, професор
Євтушенко Олександр Никифорович
(посада, вчене звання, науковий ступінь, П.І.Б.)

Виконала: студентка VI курсу 637МЗ групи
Бондарєва Інеса Миколаївна
(П.І.Б.)

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

ОПП: «Місцеве самоврядування»

Миколаїв – 2024 рік

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЕА	– електронний архів
ЕД	– електронний документ
ЕДО	– електронний документообіг
ЕЦП	– електронний цифровий підпис
ЄС	– Європейський Союз
ІКТ	– інформаційно-комунікаційні технології
ООН	– Організація Об’єднаних Націй
ОПУ	– Офіс Президента України
СЕДО	– система електронного документообігу
ЦНАП	– центр надання адміністративних послуг

ВСТУП

Актуальність теми роботи. Актуальність теми даного дослідження є очевидною, оскільки низька ефективність чинної системи публічного управління в Україні, з огляду на динамічний та іноді непередбачуваний вплив сучасних факторів геополітичної конкуренції, глобалізації та гострих форм інформаційного протиборства, вимагає перегляду всієї концепції функціонування цієї системи. Це необхідно для її адаптації до сучасних умов глобалізації, розвитку громадянського та інформаційного суспільства, а також для створення сервісної та «сильної» держави.

Електронне урядування, як нова форма організації публічного управління, завдяки широкому впровадженню новітніх ІКТ, забезпечує якісно новий рівень відкритої взаємодії між державою та суспільством, а також надання максимально повного спектру публічних послуг для всіх категорій громадян і суб'єктів господарювання. Це вимагає пошуку та впровадження нових підходів, принципів і методів для формування та реалізації відповідної публічної політики й управління. Також є потреба у запровадженні інноваційних методів підготовки, перепідготовки та підвищення кваліфікації кадрів для органів влади, а також формування управлінської еліти, яка володіла б цими методами і могла їх ефективно впроваджувати у життя суспільства і держави. Чільне місце з-поміж усього цього займає саме СЕДО, забезпечення безпеки якої, особливо сьогодні, коли Україна більше десяти років протистоїть російській військовій агресії. Зважаючи на це, так важливо не втратити свою ідентичність та відстояти власні кордони, забезпечити сучасне й ефективне публічне управління, в центрі якого дотримання прав і свободи людини та громадянина.

Стан наукової розробки теми. Дослідженню загальних питань ЕДО присвячені роботи таких науковців як: А.І. Семенченк, В.М. Бабаєв, С.О. Гайдученко, Н.В. Грицяк, В.М. Дрешпак, А.О. Ільїна, О.А. Липський,

М.М. Новікова та ін. Особливості функціонування СЕДО в сфері вітчизняного публічного управління відображені у наукових роботах: В.Л. Бурячок, Р.В. Киричок, В.Д. Лагутіна, І.О. Ляшенко, А.О. Серенок, Т.С. Ярової й ін.

Метою роботи є дослідження безпекових питань функціонування СЕДО в сфері публічного управління в умовах воєнного стану.

Зазначена вище мета досягається постановкою таких **завдань**:

- розглянути загальні засади ЕДО в сфері публічного управління;
- охарактеризувати різновиди СЕДО в органах публічної влади та навести їх переваги;
- окреслити загрози та описати можливості захисту інформації в системах електронного урядування, як важливої складової безпеки держави в умовах воєнного стану;
- визначити проблеми розвитку СЕДО в сфері публічного управління та сформулювати способи їх вирішення;
- виявити недоліки і прогалини у безпечному функціонуванні систем електронного урядування та запропонувати шляхи їх усунення.

Об’єктом роботи є функціонування системи документообігу в сфері публічного управління.

Предметом роботи є безпекові питання функціонування СЕДО в сфері публічного управління.

Методи дослідження. Методологічну основу роботи складають загальнонаукові та спеціальні методи дослідження. Формально-логічний метод використано для розкриття змісту основних понять дослідження. За допомогою порівняльно-правового методу розглянуто нормативне забезпечення функціонування СЕДО в сфері публічного управління. На основі системного і структурно-функціонального методів охарактеризовано різновиди СЕДО в органах публічної влади та наведено їх переваги. Використання причино-наслідкового аналізу дало змогу окреслити загрози та описати можливості захисту інформації в системах електронного урядування, як важливої складової безпеки держави в умовах воєнного стану. За

допомогою системно-аналітичного методу та методу прогнозування сформульовано напрями посилення безпеки функціонування СЕДО в сфері публічного управління в умовах воєнного стану. На основі методу групування зроблено відповідні висновки проведеного дослідження.

Наукова новизна дослідження. Дана робота є самостійним науковим дослідженням у сфері публічного управління, в якому авторкою отримано науково обґрунтовані результати, що висвітлюють безпекові питання функціонування СЕДО в сфері публічного управління в умовах воєнного стану. Основні положення кваліфікаційної роботи, які визначають її наукову новизну, полягають: у виявленні факторів, що впливають на вирішення організаційних проблем інтеграції всього комплексу публічних послуг для задоволення потреб громадян та функціональних аспектів публічного управління; у визначенні перспективних напрямів розвитку ЕДО, сервісів на основі сучасних технологій та важливість кіберзахисту в умовах війни.

Практичне значення одержаних результатів полягає у тому, що на основі аналізу здобутків вітчизняної й зарубіжної наукової літератури у кваліфікацій роботі сформульовано способи вирішення проблем розвитку СЕДО в сфері публічного управління та запропоновано шляхи усунення недоліків і прогалин у безпечному функціонуванні систем електронного урядування, які можуть бути використані у практичній діяльності публічних службовців.

Апробація результатів дослідження. Основні положення та висновки дослідження апробовано у формі однієї доповіді на XXVII Всеукраїнській щорічній науково-методичній конференції «Могилянські читання – 2024: досвід та тенденції розвитку суспільства в Україні: глобальний, національний та регіональний аспекти» (м. Миколаїв, 6-10 листопада 2024 р.).

Структура роботи. Робота складається зі вступу, трьох розділів, які об’єднують шість підрозділів, висновків, списку використаних джерел та одного додатку. Загальний обсяг роботи складає 85 сторінок, основного тексту 77 сторінок. Список використаних джерел налічує 62 найменування. Робота містить 10 рисунків.

РОЗДІЛ 1
ЗАГАЛЬНІ ЗАСАДИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В СФЕРІ ПУБЛІЧНОГО УПРАВЛІННЯ

1.1. Поняття та сутність електронного документа й електронного документообігу

Основою інформаційно-аналітичного забезпечення діяльності організації є обробка документів, які необхідно створювати, фіксувати та обліковувати у визначеній формі.

Документи застосовуються в різних сферах знань, діяльності людини та суспільного життя. Вони є предметом вивчення багатьох наукових дисциплін, тому поняття «документ» має кілька значень і залежить від контексту його використання та галузі.

Згідно зі ст. 1 Закону України «Про інформацію», документ є «матеріальним носієм, що містить інформацію, і виконує основні функції збереження та передачі цієї інформації в часі та просторі» [42]. В інших джерелах документ описується як «структурована одиниця інформації, призначена для сприйняття людиною, яка оформлена та зафіксована на матеріальному носії відповідно до встановлених вимог, з дотриманням певної форми подання та формуванням обов'язкових ознак» [10, с. 7]. Це такі три ключові ознаки як:

- функціональність – чіткість у межах існуючих соціальних відносин щодо очікуваного впливу документа (включаючи подальші дії) на його отримувачів після отримання та ознайомлення з його змістом;
- санкціонованість – визначеність фізичної та/або юридичної особи, яка в певний момент відповідає за існування документа;
- реєстрація – чітка ідентифікація документа серед інших

документів.

Відповідно до ст. 5 Закону України «Про електронні документи та електронний документообіг», ЕД визначається як «документ, інформація в якому зафіксована у вигляді електронних даних» [27]. Цей документ містить обов'язкові реквізити, склад і порядок розміщення яких регулюється законодавством. ЕД може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму, що дозволяє відображати його дані за допомогою електронних пристроїв або на папері, у формі, що забезпечує сприйняття його змісту людиною.

Обов'язковими реквізитами ЕД є дані, без яких він не може слугувати підставою для обліку і не матиме юридичної сили.

Згідно зі ст. 6 вказаного Закону України, обов'язковим реквізитом ЕД є ЕЦП, який використовується для ідентифікації автора та/або підписувача ЕД іншими учасниками електронного документообігу, а також підтверджує його цілісність [27]. Завершення створення ЕД відбувається шляхом накладання ЕЦП. Важливо зазначити, що лише ЕЦП має правовий статус, який прирівнюється до власноручного підпису (печатки), тоді як інші види електронного підпису такого статусу не мають.

Оригіналом ЕД, відповідно до ст. 7 зазначеного Закону, вважається електронний варіант документа, що містить обов'язкові реквізити, включаючи ЕЦП автора. У випадку, якщо ЕД надсилається кільком адресатам або зберігається на декількох електронних носіях, кожен з таких електронних примірників вважається оригіналом. Якщо автор створює ідентичні за змістом та реквізитами ЕД і паперовий документ, то кожен з них є оригіналом і має однакову юридичну силу. Електронна копія ЕД засвідчується відповідно до встановленого законом порядку. Копією паперового документа для ЕД є його візуальне відображення на папері, яке також засвідчується згідно з вимогами законодавства [27].

Статус ЕД визначається його реквізитами, які можуть мати такі значення:

- версія – примірник ЕД, що знаходиться на етапі створення і відрізняється від інших примірників за змістом;
- оригінал – перший примірник ЕД, який набуває чинності, що фіксується під час реєстрації відповідним значенням спеціального реквізиту;
- дублікат – примірник ЕД, що має таку ж юридичну силу, як і оригінал;
- копія – примірник ЕД, який точно відтворює зміст оригіналу, а також всі його реквізити або їх частину;
- витяг з ЕД – копія ЕД, що відтворює частину його структур і частину змісту.

У ст. 8 Закону України «Про електронні документи та електронний документообіг» зазначено, що юридична сила ЕД не може бути оскаржена лише через його електронну форму [27]. Також визначено випадки, коли ЕД не може використовуватися як оригінал: свідоцтва про право на спадщину; документи, які відповідно до законодавства можуть бути створені лише в одному оригінальному примірнику, за винятком випадків наявності централізованого сховища оригіналів ЕД; а також в інших випадках, передбачених законом.

Життєвий цикл ЕД складається із чотирьох етапів, які реалізуються через послідовні процеси, що здійснюються за допомогою комп'ютерних технологій та засобів зв'язку (див. Рис. 1.1). Виконання операцій, пов'язаних із цими процесами, може відбуватися автоматично або під контролем користувачів інформаційно-телекомунікаційних систем. Технології створення ЕД дозволяють не лише використовувати їх на рівні з паперовими документами, але й відкривають нові можливості для їх обробки.

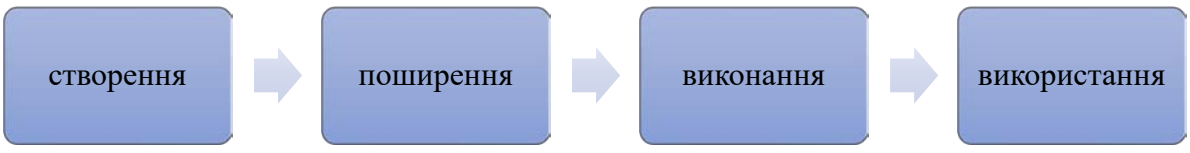

Рис. 1.1. Життєвий цикл ЕД

Основною перевагою є значне підвищення швидкості документообігу в діяльності публічно-владних суб'єктів, а також можливість укладення угод та інших правочинів за допомогою різних інформаційних технологій (наприклад, через електронну пошту, або через завантаження документу на гугл диск. що має корпоративний доступ).

Термін «документаційне забезпечення управління» (або іншими словами діловодство) почав використовуватися в науковій та практичній сферах приблизно з середини 70-х років XX ст., у зв'язку зі змінами в організаційно-технічній основі та методологічних підходах до вдосконалення, що стало можливим завдяки активному впровадженню обчислювальної техніки та нових інформаційно-телекомунікаційних технологій у сфері роботи з документами.

Діловодство розглядається як сфера діяльності, що забезпечує створення офіційних документів та організацію роботи з ними. Це включає в себе організацію руху документів від моменту їх створення або отримання до завершення виконання, що охоплює їх відправку з організації або безпосередньо в архів. У більш широкому сенсі документообіг можна визначити як інформаційну діяльність суб'єктів інформаційних відносин, яка реалізується через виконання певних дій з документами.

Система документообігу визначається як комплекс методів, інструментів і персоналу, що забезпечує функціонування документообігу відповідно до встановлених регламентів.

СЕДО є організаційно-технічною системою, яка забезпечує процеси створення, управління доступом і розповсюдження ЕД у комп'ютерних мережах, а також контроль за документами потоками в організації.

Важливу роль відіграє регулювання (регламентування) документообігу, що стосується ЕД.

Регламент документообігу – це комплекс правил, що регулюють інформаційну діяльність учасників інформаційних відносин, встановлених законодавством, нормативними актами або угодами. Він визначає ролі та

права учасників у процесах створення, володіння, використання та розпорядження документами, а також порядок оформлення та фіксації інформації на інформаційних носіях [5].

ЕДО можна розглядати як узагальнене поняття, що охоплює інформаційні технології, які забезпечують життєвий цикл електронного документа. У свою чергу, СЕДО можна охарактеризувати як автоматизовану систему обробки інформації, яка реалізує ЕДО та інтегрується з іншими системами документообігу.

Необхідність впровадження ЕД та використання можливостей електронного документообігу для різних суспільних потреб в Україні стала актуальною ще в другій половині 90-х років минулого століття. Це також було зумовлено позитивним досвідом розвинених країн у цій галузі. Проте на той час в українському суспільстві, а також в органах державної влади, не вистачало матеріально-технічної бази та усвідомлення обсягу і складності завдань, які потрібно було вирішити для досягнення цієї мети.

Зазначеними законами були визначені основні поняття та терміни в галузі електронного документообігу:

- адресат – фізична або юридична особа, якій призначений ЕД;
- дані – інформація, представлена у формі, що підходить для обробки електронними засобами;
- посередник – фізична чи юридична особа, яка відповідно до чинного законодавства здійснює приймання, передачу, доставку, зберігання чи перевірку цілісності ЕД для задоволення власних потреб або надає відповідні послуги за дорученням інших учасників СЕДО;
- ЕД – документ, інформація в якому зафіксована у вигляді електронних даних, що включає обов’язкові реквізити паперового документа;
- обов’язковий реквізит ЕД – це необхідні дані, які повинні бути присутніми в електронному документі, інакше він не може слугувати підставою для обліку та не матиме юридичної сили;
- автор ЕД – це фізична або юридична особа, яка його створила;

- ЕДО – це комплекс процесів, що включає створення, обробку, відправлення, передачу, отримання, зберігання, використання та знищення ЕД, які здійснюються з перевіркою цілісності та, за потреби, з підтвердженням факту їх отримання;
- суб'єкт ЕДО – це автор, підписувач, адресат та посередник, які отримують права та обов'язки, передбачені законом або договором, у процесі електронного документообігу [12, с. 49].

Варто виділити такі ключові принципи та завдання ЕДО:

- одноразова реєстрація документа, що забезпечує його однозначну ідентифікацію в будь-якій підсистемі;
- можливість одночасного виконання різних операцій, що сприяє скороченню часу обробки документа та підвищує оперативність виконання;
- безперервність руху документа, що дозволяє визначити відповідальну особу за його виконання (завдання) на кожному етапі життєвого циклу документа;
- єдина (або узгоджено розподілена) база документної інформації, що виключає можливість дублювання документів;
- ефективно налаштована система пошуку документів, яка дозволяє знаходити їх, маючи лише мінімальну інформацію;
- вдосконалена система звітності для різних статусів і атрибутів документів, що забезпечує можливість контролювати їх переміщення в процесах документообігу та приймати управлінські рішення на основі даних з звітів [13, с. 766].

Отже, ЕДО та електронні документопотоки є ключовими елементами роботи з документами. Використання електронних документопотоків дозволяє оптимізувати процеси, зменшити час на передачу та отримання інформації. Сьогодні можна з упевненістю говорити про широке впровадження технології ЕДО, яка об'єднує користувачів у єдиній мережі та забезпечує швидкий і зручний обмін документами відповідно до єдиних оптимальних правил і регламентів.

Що стосується України, то більшість документообігу в публічно-владних установах все ще відбувається в паперовому форматі. Однак, сучасний стан автоматизованого діловодства та документообігу в органах влади створює сприятливі технологічні умови для подальшого розвитку ЕДО та наближення його до стандартів країн ЄС.

1.2. Нормативне забезпечення функціонування системи електронного документообігу в сфері публічного управління

Необхідність державного впливу та створення окремої державної політики в сфері інформаційного суспільства визначена, перш за все, у документах Женевського (2003 р.) та Туніського (2005 р.) всесвітніх самітів з питань розвитку інформаційного суспільства [4], а також в Окінавській хартії глобального інформаційного суспільства [21] та Стратегії розвитку Європейського Союзу «Європа-2020».

З точки зору інтеграції з ЄС, при розробці національних документів важливо орієнтуватися на eIDAS (Регламент Європейського парламенту та Ради ЄС щодо електронної ідентифікації та послуг інтероперабельності) та EIF (Європейські рамки інтероперабельності). Це дозволить у майбутньому забезпечити транскордонну електронну взаємодію та надання електронних послуг між країнами. Досягнення інтероперабельності та забезпечення електронної взаємодії між різними системами органів публічної влади визначено як один з основних пріоритетів Цифрового порядку денного для Європи на 2020 рік та Європейського плану дій у сфері е-урядування на 2011–2015 роки, оскільки це є необхідною умовою для створення єдиного цифрового ринку Європи та надання транскордонних послуг.

В Україні приділяється значна увага розвитку електронного урядування. Цю сферу регулюють більше ніж 10 законів, 30 постанов та 20 розпоряджень

Кабінету Міністрів України. Серед них Закони України: «Про інформацію», «Про Національну програму інформатизації», «Про доступ до публічної інформації», «Про адміністративні послуги», «Про електронні документи та електронний документообіг», «Про електронний цифровий підпис», «Про персональні дані», «Про електронну комерцію», а також зміни до Закону України «Про звернення громадян» щодо електронних звернень та петицій, а також зміни до деяких законодавчих актів України, що стосуються особливостей подання декларацій службовими особами про майно, доходи, витрати та фінансові зобов'язання у 2016 році.

Електронне урядування є одним з ключових напрямків Стратегії сталого розвитку «Україна–2020», що є частиною Президентського плану з модернізації України. У документі зазначається, що метою реформи державного управління є створення прозорої системи управління, формування професійного інституту державної служби та забезпечення її ефективності. Впровадження цієї реформи має призвести до створення ефективної, прозорої, відкритої та гнучкої структури публічної адміністрації, яка використовує сучасні інформаційно-комунікаційні технології (е-урядування) і здатна розробляти та реалізовувати цілісну державну політику, орієнтуючись на сталий розвиток суспільства та адекватне реагування на внутрішні та зовнішні виклики [44].

Відповідно до цих та інших документів, основна роль у організації, координації та контролі відносин, що виникають під час розвитку інформаційного суспільства та впровадження електронного урядування, покладається на державу. Це стосується взаємодії між ключовими суб'єктами: державою, бізнесом, міжнародними та громадськими організаціями, а також експертним середовищем: «Створення відкритого для всіх інформаційного суспільства потребує нових форм партнерства та співпраці між органами державного управління та приватним сектором, громадянським суспільством та міжнародними організаціями ... при цьому органам державного управління належить провідна роль у розробці та здійсненні перспективних та усталених

національних електронних стратегій ...» [4].

У Державній стратегії регіонального розвитку на період до 2020 року окреслено пріоритетні напрямки розвитку регіонів, зокрема, акцентовано увагу на підвищенні ефективності роботи місцевих державних адміністрацій та вдосконаленні взаємодії між ними і фізичними та юридичними особами через впровадження системи електронного урядування [28].

На нашу думку, в Україні в цілому сформована відповідна законодавча та нормативно-правова база в сфері електронного урядування. Проте вона має ряд недоліків, таких як неповнота, декларативність, безсистемність, нечіткість, недостатня узгодженість документів та невідповідність міжнародним стандартам, зокрема європейським. Крім того, існує проблема втрати актуальності, що суттєво гальмує розвиток цієї сфери і є однією з основних причин, чому Україна втрачає свої позиції в міжнародних рейтингах розвитку інформаційного суспільства та електронного урядування.

Згідно з результатами нового дослідження ООН «Огляд електронного урядування ООН – Прискорення цифрової трансформації заради сталого розвитку», Україна в 2024 році значно покращила свої позиції у світових рейтингах цифрового урядування [62].

Зокрема, Україна стала першою у рейтингу електронної участі (E-Participation Index, EPART), піднявшись, порівняно з 2022 роком, на 56 позицій. А у рейтингу електронного урядування (E-Government Development Index, EGDI) – посіла 30-те місце, що на 16 позицій вище, ніж 2022 року [61].

Впровадження електронного документообігу повинно стати базою для регулювання взаємовідносин між учасниками в таких сферах, як електронна комерція, електронна торгівля, подання електронної звітності, а також надання електронних (адміністративних) послуг через спеціалізовані інформаційні системи та загальнодоступні мережі, зокрема Інтернет.

Для досягнення цієї мети було ухвалено два основні закони України: «Про електронний цифровий підпис» [26] та «Про електронні документи та електронний документообіг» [27]. Варто зазначити, що положення першого з

цих законів відповідають вимогам Директиви 1999/93/ЕС Європейського Парламенту та Ради Європи від 13 грудня 1999 року «Про систему електронних підписів, що використовується в межах Співтовариства» [6].

З ухваленням цих законів, за умови дотримання певних вимог, електронні цифрові підписи отримали правовий статус, рівний власноручному підпису (печатці). Також були визначені основні організаційно-правові принципи використання ЕД та впровадження ЕДО.

Відносини, що стосуються відправлення, передачі та отримання ЕД, регулюються Законом України «Про електронні документи та електронний документообіг» [27]. Зокрема, ЕД може бути відправлений та переданий автором або посередником в електронному вигляді за допомогою інформаційно-телекомунікаційних систем або шляхом надсилання електронних носіїв, на яких цей документ записано.

ЕД вважається отриманим адресатом з моменту, коли автор отримує повідомлення в електронному вигляді від адресата про його отримання, якщо інше не визначено законодавством або попередньою угодою між сторонами електронного документообігу. Перевірка цілісності ЕД здійснюється шляхом перевірки автентичності накладеного на нього ЕЦП.

З метою реалізації вказаних законів Кабінет Міністрів України ухвалив ряд постанов, які уточнили регулювання відносин у цій галузі, зокрема:

- «Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу» від 26 травня 2004 р. № 680 [32];
- «Про затвердження Порядку акредитації центру сертифікації ключів» від 13 липня 2004 р. № 903 [31];
- «Про затвердження Положення про центральний засвідчувальний орган» від 28 жовтня 2004 р. № 1451 [30];
- «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної

форми власності» від 28 жовтня 2004 р. № 1452 [33];

- «Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади» від 28 жовтня 2004 р. № 1453 [39];
- «Про затвердження Порядку обов'язкової передачі документованої інформації» від 28 жовтня 2004 р. № 1454 [35].

Вказані постанови, серед іншого, спрямовані на формування та розвиток в Україні інфраструктури відкритого ключа для забезпечення використання ЕЦП. Це, перш за все, передбачає створення її основних суб'єктів – центрального засвідчувального органу та контролюючого органу, а також засвідчувальних центрів. Формування та функціонування інших суб'єктів цієї інфраструктури, таких як центри сертифікації ключів, включаючи акредитовані центри сертифікації, здійснюється представниками бізнесу.

Безпосередньо затверджений постановою уряду № 1453 Типовий порядок здійснення електронного документообігу в органах виконавчої влади визначає основні правила документування управлінської діяльності в електронному форматі. Цей порядок регулює процеси, пов'язані з ЕД, починаючи з їх створення або отримання і закінчуючи відправленням або передачею до відповідного архіву. Усі інші дії з ЕД в органах влади виконуються відповідно до вимог, що стосуються паперових документів, які зазначені в інструкції з діловодства цього органу [39].

Типовий порядок поширюється на всі ЕД, які створюються або отримуються органами влади. Кожен державний орган, орган місцевого самоврядування, підприємство, установа чи організація, незалежно від форми власності, має можливість адаптувати загальні правила документування в електронному вигляді відповідно до своїх потреб та регламентувати дії з ЕД відповідно до чинного законодавства [39].

Орган влади може здійснювати ЕДО лише за умови використання надійних засобів ЕЦП. Це має бути підтверджено сертифікатом відповідності або позитивним висновком, отриманим в результаті державної експертизи у сфері криптографічного захисту інформації від Державної служби

спеціального зв’язку та захисту інформації України. Крім того, працівники, які підписують документи, повинні мати посилені сертифікати відкритих ключів. У цьому випадку ЕДО реалізується органом влади за допомогою спеціалізованих телекомунікаційних мереж або мереж загального користування. Відправка ЕД через мережі загального користування проводиться за рішенням керівника відповідного органу.

Відповідно до чинного законодавства, орган влади зобов’язаний дотримуватись вимог нормативно-правових актів у сфері захисту інформації. Це, зокрема, стосується положень Закону України «Про захист інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 5 липня 1994 р. №80/94-ВР [40] та Постанови уряду «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29 березня 2006 р. № 373 [36].

Формування архівів ЕД, їх подача до архівних установ та зберігання в цих установах відбувається відповідно до вимог законодавства. Зокрема, наказом Державного комітету архівів України затверджено 25 квітня 2005 р. «Порядок зберігання електронних документів в архівних установах» [34].

Основою для регулювання питань діловодства стала Постанова Кабінету Міністрів України «Про затвердження Примірної інструкції з діловодства у міністерствах, інших центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим та місцевих органах виконавчої влади» від 17 жовтня 1997 р. № 1153 [38]. Ця Інструкція встановлює порядок ведення загального діловодства, а її положення поширюються на всю службову документацію, включаючи ту, що створюється за допомогою персональних комп’ютерів. Комп’ютерні (автоматизовані) технології для обробки документної інформації мають відповідати вимогам державних стандартів та вказаній інструкції.

Деякі положення Примірної інструкції вже заклали основу для впровадження в установах СЕДО. Зокрема, в них підкреслювалося, що

механізація та автоматизація ділових процесів є необхідною умовою для раціональної організації діловодства в кожній установі. Це є засобом підвищення продуктивності та зниження витрат на управлінську працю, і має здійснюватися на основі впорядкованої системи документування управлінської діяльності, а також уніфікації та скорочення кількості використовуваних форм документів. Окрім цього, ці заходи реалізуються на всіх етапах діловодного процесу, включаючи підготовку документів, їх копіювання, оперативне зберігання та транспортування, а також контроль за виконанням. При цьому засоби механізації та автоматизації діловодних процесів повинні бути сумісними та забезпечувати можливість інтеграції в єдину систему.

У Примірній інструкції вказано, що комплекс технічних засобів має забезпечувати збір та передачу інформації, її запис на електронні носії, введення даних у персональний комп'ютер, виведення результатів, обробку інформації у вигляді машино- або відеограм, сумісність з іншими інформаційними системами, а також можливість інтеграції в єдину систему. При впровадженні нових технологій роботи з документами слід враховувати такі аспекти як:

- обґрунтованість впровадження технічних засобів;
- можливість придбання технічних засобів у встановлені терміни;
- наявність відповідних приміщень;
- потребу в залученні фахівців для обслуговування обладнання тощо [10, с. 13].

Керівник установи відповідає за ефективне використання механізованих та автоматизованих технологій обробки документів.

Обробка документів в установі виконується за стандартними схемами, що відповідають вхідним, внутрішнім та вихідним документам. При обробці вхідного документа виділяються наступні етапи: отримання, попередній аналіз, реєстрація, доповідь керівництву, організація виконання (призначення виконавців та формулювання завдань), контроль за діловодством щодо

процесу та результатів виконання, завершення справи (остаточне оформлення) та передача на зберігання.

Всі операції з ЕД, за винятком тих, що пов’язані зі специфікою його створення або отримання перед відправленням чи передачею до архіву, здійснюються в установах відповідно до вимог, які регулюють дії з паперовими документами, згідно з інструкціями з діловодства цих організацій.

Отже, нормативне забезпечення функціонування СЕДО в сфері публічного управління представлене значною кількістю законодавчих та підзаконних актів, більшість з яких є застарілими. Однак, враховуючи специфіку створення, функціонування і зберігання ЕД, актуальним залишається питання розробки потужної нормативної бази, яка б сприяла уніфікації численних діловодних процесів чи вдосконаленню вже існуючої. Окрім того, неврегульованими залишаються правові відносини щодо єдиних підходів до організації ЕДО, використання ЕЦП, ЕД та електронних інформаційних ресурсів, а також авторського права в сфері інформаційних відносин.

Висновки до Розділу 1

ЕД – це документ, інформація в якому представлена у вигляді електронних даних і містить обов’язкові реквізити. Його можна створювати, передавати, зберігати та перетворювати за допомогою електронних засобів у візуальний формат (відображення даних, що містяться в ньому, електронними засобами або на папері у формі, зручній для сприйняття людиною). У свою чергу, ЕДО є комплекс процесів, що охоплює створення, обробку, відправлення, передачу, отримання, зберігання, використання та знищення електронних документів. Ці процеси виконуються з використанням перевірки цілісності та, за необхідності, з підтвердженням факту отримання документів.

В Україні, у цілому, сформована нормативно-правова база в сфері ЕДО. Проте вона має ряд недоліків, таких як неповнота, декларативність, відсутність системності, нечіткість, недостатня узгодженість документів та невідповідність міжнародним стандартам, зокрема, європейським. Крім того, існує проблема втрати актуальності, що суттєво стримує розвиток цієї сфери і є однією з основних причин, чому Україна втрачає свої позиції в міжнародних рейтингах розвитку інформаційного суспільства та електронного урядування.

РОЗДІЛ 2
ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В СФЕРІ ВІТЧИЗНЯНОГО ПУБЛІЧНОГО УПРАВЛІННЯ НА СУЧАСНОМУ ЕТАПІ

2.1. Різновиди системи електронного документообігу в органах публічної влади та їх переваги

На сьогоднішній день на ринку України представлені системи автоматизації документообігу, які в основному є продуктами вітчизняних розробників або інтеграторів закордонного програмного забезпечення, зокрема, на базі платформи Lotus Notes/Domino від компанії IBM. Серед українських рішень можна виділити: СЕДО ОПУ, АСКОД, «Megapolis.Документообіг», «ДОК ПРОФ 2.0», «Атлас ДОК» та «FossDoc».

Перелік протестованих системи ЕДО за версією ДКП «ДІЯ» представлений на Рис. 2.1 [24].

№	Розробник	Назва та версія платформи	Інтеграційна взаємодія з СЕВ ОВВ	НПА
1	ТОВ «Софтлайн-ІТ»	Мегаполіс v.2.57	+	-
2	ТОВ «Софтлайн-ІТ»	«Megapolis. DocNet» v.1.x	+	-
3	ТОВ «Інтекресі Бейз»	«Megapolis. DocNet» v.1.x	+	+
4	ТОВ «Айкюжн ІТ»	«Megapolis. DocNet» v.1.x	+	-
5	АТ «ІнфоПлюс»	АСКОД II v 10.3.8.141	+	-
6	АТ «ІнфоПлюс»	АСКОД Корпоративний v.10	+	+
7	ТОВ «Транс Лінк Консалтинг»	ДОК ПРОФ™ СТЕП 2.0	+	-
8	ТОВ «Транс Лінк Консалтинг»	«Автоматизована система управління документами «ДОК ПРОФ 3»	+	+
9	ТОВ «Інтерактивні системи»	InterDoc v 4.2	+	-
10	ТОВ НВП «Інформаційні технології»	«IT-Enterprise»(IT Підприємство)	+	+

Рис. 2.1. Протестовані системи ЕДО за версією ДКП «ДІЯ»

Функції, які СЕДО надає своїм користувачам, мають широкий спектр. Їх можна умовно класифікувати на кілька категорій:

- зберігання та пошук документів;
- підтримка роботи канцелярії;
- маршрутизація та контроль за виконанням документів;
- аналітичні звіти;
- забезпечення інформаційної безпеки;
- додаткові (специфічні) функції.

Розглянемо найпопулярніші функції з наведених категорій.

1. Зберігання та пошук документів. Централізоване зберігання документів є ключовим аргументом для впровадження ЕДО. У цьому контексті важливо звернути увагу на постачальника системи зберігання даних, яка використовується в конкретній системі ЕДО.

Серед функцій, що використовуються для пошуку документів, можна виділити:

- пошук за атрибутами (полями) документів;
- пошук за файлами, що містяться в документах (повнотекстовий пошук);
- розширений пошук (з використанням логічних операторів);
- адаптивна система управління правами доступу.

2. Підтримка роботи канцелярії. Підтримка функціонування канцелярії є одним із ключових елементів СЕДО. Основні функції, пов’язані з канцелярською діяльністю, включають:

- презентація документа у формі електронної картки, що є аналогом реєстраційної картки документа;
- можливість введення документів у систему за допомогою сканера;
- створення документів в електронному форматі безпосередньо в системі;
- реєстрація документів, включаючи ті, що надійшли електронною поштою;
- ведення номенклатури справ;
- повний цикл обробки вхідних та вихідних документів;

- підтримка службових записок;
- обробка звернень громадян;
- робота з заявками;
- ведення журналів реєстрації та обліку паперових оригіналів документів;
- підтримка допоміжних процесів документообігу (контрольне вичитування, додаткове узгодження);
- підтримка ієрархічних довідників.

3. Маршрутизація та контроль за виконанням документів. Функції цієї категорії забезпечують управління документопотоками в організації та контроль за виконанням робіт з документами. Основні функції цієї категорії включають:

- проектування маршрутів документів з можливістю їх послідовно-паралельного виконання;
- підтримка різних дій з документами під час маршруту: візування, узгодження, накладення резолюцій, підписання тощо;
- відправка документів за вже визначеними типовими маршрутами, а також новими, які користувач може встановити під час виконання завдання;
- інформування працівників про надходження нових документів для виконання.
- повідомлення про закінчення етапів маршрутів;
- підтримка версій документів (проектів документів);
- автоматичний моніторинг термінів виконання документів.

4. Аналітичні звіти. До загальновизнаних звітів належать:

- звіт про актуальну зайнятість працівників;
- звіт про виконання робіт з документами (ретроспективний);
- звіт про невиконані доручення.

5. Забезпечення інформаційної безпеки. Функції цієї категорії забезпечують інформаційну безпеку СЕДО за допомогою таких засобів:

- аутентифікація користувачів системи;

- розподіл прав доступу для працівників, які користуються СЕДО;
- підтримка ЕЦП документів;
- шифрування листів і документів;
- ведення історії та статистики роботи з документами;
- аудит діяльності користувачів у системі.

6. Додаткові (специфічні) функції. Деякі розробники СЕДО пропонують унікальні функції, які характерні лише для їхніх конкретних рішень. Наприклад, СЕДО ОПУ розроблена на базі платформи SharePoint, забезпечує безперешкодну інтеграцію з усіма програмами Microsoft Office (Outlook, Word, Excel, PowerPoint, OneNote) та має мобільний інтерфейс для операційних систем Windows і iOS [7, с. 22].

Багато СЕДО пропонують власні API-інтерфейси для розробки нових функцій на замовлення. При виборі СЕДО для державних установ важливою проблемою є відповідність системи чинному законодавству та нормативним актам. Наприклад, постачальники ЕЦП, що використовується в СЕДО, повинні мати сертифікацію від відповідних державних органів. Для українських державних установ критично важливою є повна україномовна локалізація як користувацьких інтерфейсів, так і документації, а також наявність технічної підтримки українською мовою.

ЕА – це організоване сховище незмінних оригіналів ЕД (електронних копій паперових документів), яке створюється відповідно до законодавства та норм архівного зберігання в певній місцевості (в конкретній країні). Документи, що формують основу ЕА, зазвичай пов’язані з діловими процесами організації. Структурування документів здійснюється шляхом об’єднання їх у більш великі одиниці зберігання, які називаються справами [37].

ЕА є інформаційною системою, що забезпечує одночасний доступ до ЕД. Її основні функції включають:

- створення каталогу документів з визначеною ієрархією;
- автоматизована систематизація та класифікація документів (документи автоматично відносяться до відповідних категорій);

- зручне збереження документів (документ має завантажуватися в систему всього за два-три кліки миші);
- гарантування повного збереження інформації, незважаючи на фізичні впливи, технологічні зміни, зміни форматів даних тощо;
- надання користувачам доступу до документів;
- перегляд і робота з електронними копіями;
- пошук документа як за каталогом, так і за наявними параметрами;
- резервне копіювання документа;
- друк документів;
- адміністрування системи (реєстрація нових користувачів, контроль за роботою, надання прав доступу тощо) [7, с. 23].

СЕДО та ЕА мають кілька спільних характеристик. По-перше, в обох типах систем основною одиницею обробки є ЕД. По-друге, ці системи створені для виконання подібних завдань, таких як структурування та систематизація документів, що циркулюють в організації. По-третє, інтерфейси систем обох типів є приблизно однаковими.

Варто зазначити, що ЕА і ЕДО не є взаємозамінними термінами; скоріше, вони доповнюють один одного. Функції, які виконують ці системи, можна порівняти з функціями традиційного паперового архіву та документообігу. Основна відмінність між ними полягає в тому, що архів призначений для зберігання та пошуку інформації, яку не потрібно змінювати [7, с. 24].

Таким чином, на нашу думку, можна виділити кілька ключових відмінностей у збереженні інформації в ЕА та документообігу:

- у СЕДО фіксується вся актуальна документація організації, а ЕА створені для зберігання важливих документів. Визначення значимості документів не може бути виконане автоматично і є виключно людським завданням;
- СЕДО призначені для щоденної роботи з документами, включаючи внесення змін, затвердження та розсилку різним працівникам організації. Хоча системи ЕА можуть мати інструменти для підтримки

щоденної роботи, їх основною метою є надійне (включаючи захист від змін) зберігання важливих документів;

- СЕДО призначені для роботи з невеликими обсягами інформації, тоді як системи ЕА спочатку створювалися для обробки великих масивів документів;
- СЕДО орієнтовані на структурування потоку документів, з якими організація працює в даний момент, у той час як системи ЕА призначені для систематизації та структурування документів минулого. Крім того, вони надають можливість встановлювати структуру для організації та збереження документів у майбутньому;
- СЕДО забезпечує лише тимчасове зберігання документів, тоді як система ЕА гарантує тривале (фактично довічне) збереження;
- у системах ЕА доступні розширені функції для пошуку документів;
- у СЕДО зазвичай працює велика кількість користувачів з високим навантаженням, тоді як ЕА використовують обмежена кількість осіб час від часу.

Описані вище відмінності відображені і в стандарті MoReq2, що представлений у Таблиці 2.

Таблиця 2

Відмінності між СЕДО та ЕА [7, с. 25]

№	СЕДО	Системи ЕА
1.	Призначені, в першу чергу, для роботи з актуальною документацією.	Можуть містити інструменти для щоденної діяльності, проте головна увага приділяється збереженню важливих документів.
2.	Включають набір інструментів для роботи з різними версіями документа.	Передбачається зберігати лише остаточну версію документа, яка більше не підлягає редагуванню.
3.	Існує можливість видалити документи.	Видалення документів заборонено, за винятком обмеженої кількості строго контрольованих ситуацій і процесів. Після закінчення терміну зберігання в архіві документи повинні бути знищені відповідно до вимог законодавства.

Основними перевагами ЕА є:

- швидкий та зручний доступ до інформації;
- спільний доступ до матеріалів без необхідності вилучення оригіналів;
- надійне та організоване зберігання;
- звільнення площ в організації;
- обмеження несанкціонованого доступу;
- надійний захист оригіналів документів від пошкоджень або безповоротної втрати інформації за умови належного планування та реалізації рішення [7, с. 25-26].

Отже, ЕА та СЕДО в ідеалі взаємодоповнюють одна одну, зберігаючи, систематизуючи та забезпечуючи доступ до всієї інформації органу публічного управління. СЕДО дозволяє працювати з актуальними документами, тоді як ЕА надає доступ до архівних даних. Завдяки впровадженню цих двох систем, робота з інформацією стає максимально зручною, безпечною та ефективною. Планування, виконання завдань, звітність та оцінка результатів діяльності проходять прозоро. Інформація в організації перетворюється на саморегульований інструмент управління та контролю.

ЕА органу публічного управління може функціонувати як самостійне рішення або бути інтегрованим у СЕДО. Він може бути створений як природне сховище документів не лише для СЕДО, а й для інших інформаційних систем, що застосовуються в органі публічного управління.

СЕДО, що застосовуються в Україні, мають подібні функціональні можливості. Так, наприклад, СЕДО ОПУ була створена його працівниками на основі платформи Microsoft SharePoint у 2014 році та запроваджена в дослідну експлуатацію 1 лютого 2015 року.

Проектування СЕДО в ОПУ відбувалося паралельно з реорганізацією цієї установи та вдосконаленням її адміністративних процесів. Внаслідок виконаних заходів була оптимізована організаційна структура ОПУ, що призвело до скорочення чисельності персоналу приблизно на 25%, а також до

значного підвищення ефективності обробки документів, зокрема, спрощеного розгляду 87% вхідних документів [7, с. 26].

Протягом першого року роботи в СЕДО ОПУ було зареєстровано понад 100 тисяч вхідних документів. Кількість користувачів, серед яких працівники Офісу, інтерни та стажери, перевищила 450 осіб. У цей період було проведено чотири повних цикли навчання персоналу, що сприяло значному покращенню знань працівників у галузі роботи з персональним кабінетом, інформаційної безпеки та ЕДО [7, с. 27].

Основне вікно програми (модуль «Персональний кабінет») представлено на Рис. 2.2.

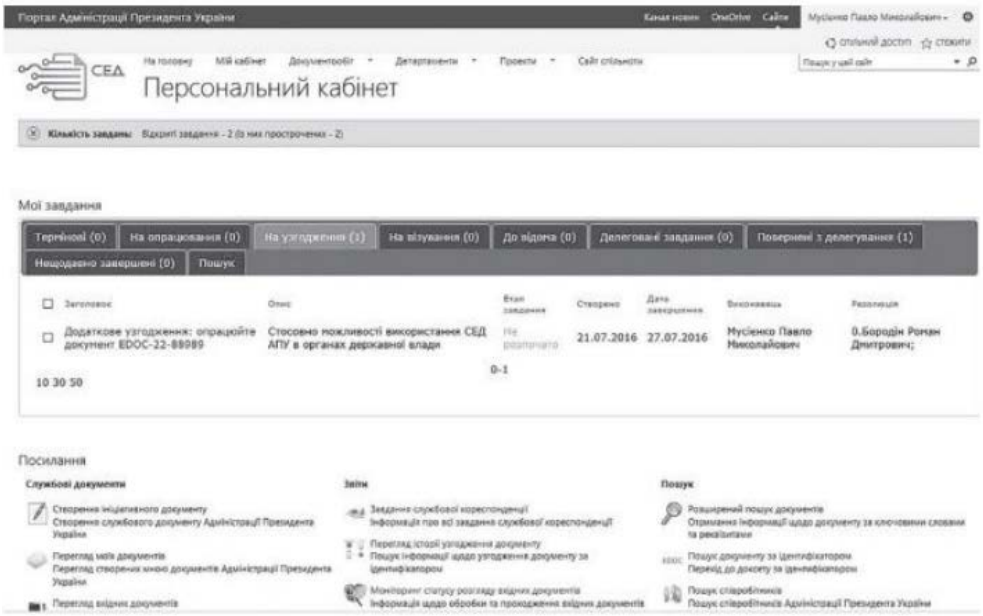

Рис. 2.2. Модуль СЕДО ОПУ «Персональний кабінет»

СЕДО ОПУ реалізує автоматизацію основних і додаткових процесів документообігу, включаючи обробку вхідної, внутрішньої та вихідної документації з використанням ЕЦП, обробку звернень громадян, петицій, пошук документів, контрольне вичитування, додаткове узгодження, а також звітність і аналітику.

Процес обробки вхідної кореспонденції включає створення реєстраційної картки для вхідного документа, переведення документа в

електронний формат (сканування), формування резолюції та передачу завдання на обробку вхідного документа виконавцям.

З метою оптимізації процедури підготовки резолюцій на вхідні документи в СЕДО ОПУ було запроваджено принцип роботи з єдиним проектом резолюції. Це дозволяє уникнути маніпуляцій на етапі підписання резолюції та надає керівництву установи можливість самостійно вносити зміни в резолюції перед їх підписанням без залучення діловодів.

В ОПУ було успішно реалізовано експеримент з автоматизації процесу підписання резолюцій. Якщо протягом доби керівником не буде не внесено правки до резолюції, вона автоматично отримує статус погодженої, і вхідний документ надсилається виконавцям, зазначеним у ній. При цьому керівник має можливість відкликати резолюцію, яка була погоджена автоматично. Завдяки цьому ефективність обробки вхідних документів зросла на 60% [16, с. 24].

Процес підготовки внутрішньої та вихідної кореспонденції в системі СЕДО ОПУ виконується за практично однаковою процедурою, з тією лише різницею, що для обробки вихідних документів передбачені додаткові етапи – контрольне вичитування та оформлення на бланку.

У рамках процесу обробки внутрішньої та вихідної документації в СЕДО ОПУ забезпечується встановлення взаємозв’язку між вхідними та вихідними документами. У системі реалізовано можливість створення ЕД (включаючи ті, що базуються на заданих шаблонах) безпосередньо в самій системі.

Оскільки в СЕД ОПУ ведеться протоколювання всіх змін, які вносять користувачі, а також забезпечується автоматичне збереження всіх версій документа під час спільної роботи над ним (з можливістю порівняння версій і відновлення будь-якої збереженої раніше версії), ризик втрати інформації, спотворення змісту документа та інших маніпуляцій повністю усувається. Крім того, СЕД ОПУ дозволяє багатьом виконавцям працювати спільно в одному файлі завдяки інтеграції з програмами Microsoft Office. Після того, як виконавці затверджують фінальну версію документа, СЕД ОПУ забезпечує збереження незмінної версії документа у форматі PDF, що дозволяє надалі

накладати ЕЦП відповідно до законодавства України [7, с. 29].

Допоміжним етапом у СЕДО ОПУ є контрольне вичитування документів. У рамках цього процесу до редагування фінальної версії документа залучаються виконавці, які мають спеціалізовані знання. Контрольне вичитування проводиться в режимі рецензування, що дозволяє автору документа контролювати зміни, які вносять співвиконавці. Для залучення інших фахівців у СЕДО ОПУ реалізовано процес додаткового узгодження, який надає можливість призначати завдання на опрацювання документа будь-якому виконавцеві, незалежно від організаційної ієрархії.

СЕДО ОПУ включає налаштовуваний модуль «Персональний кабінет», який дозволяє виконавцям різних рівнів відстежувати свої завдання щодо обробки документів. Завдання в персональному кабінеті організовані за критеріями терміновості та типу документів. Виконавці мають можливість швидко ознайомитися з документами, вносити зміни, делегувати завдання іншим співробітникам, а також погоджувати або відхиляти документи. Додатково, у персональному кабінеті доступні посилання для швидкого створення та перегляду раніше створених документів, звіти та аналітичні дані, а також можливість пошуку за різними параметрами. Однією з ключових особливостей модуля «Персональний кабінет», як і всієї СЕДО ОПУ, є можливість гнучкого налаштування інтерфейсу та функціоналу відповідно до специфічних потреб кожної організації.

Інтеграція СЕДО ОПУ з внутрішнім поштовим клієнтом забезпечує оперативне сповіщення виконавців про призначення завдань та інші важливі події в процесах документообігу [7, с. 29].

Для підвищення ефективності роботи керівників державних установ у СЕДО ОПУ було створено мобільний інтерфейс (для операційних систем Windows та iOS), який у режимі офлайн дозволяє ознайомлюватися з документами, редагувати та підписувати резолюції, а також приймати управлінські рішення (погоджувати або відхиляти документи з використанням ЕЦП). Клієнт заздалегідь завантажує завдання, що дозволяє миттєво

переходити між документами та завданнями без необхідності чекати на завантаження наступного файлу.

Окремими підсистемами СЕДО ОПУ є функції обробки звернень громадян та електронних петицій до Президента України. Процес обробки електронних петицій повністю реалізовано у безпаперовому форматі: від моменту реєстрації нової петиції до передачі опрацьованої петиції та супровідних матеріалів на підпис Президентові України все виконується виключно в електронному вигляді.

СЕДО ОПУ може бути інтегрована з внутрішнім порталом організації, що суттєво розширює можливості співпраці працівників поза межами СЕД. Портал дозволяє налаштовувати різноманітні бібліотеки як сховища робочих файлів з гнучкими правами доступу, замінюючи мережеві диски, календарі, стрічки новин організації, довідники, кадрову документацію та інші ресурси [7, с. 29].

Після розробки та впровадження СЕДО ОПУ у березні 2016 року було ухвалено рішення про безкоштовну передачу функціоналу всім зацікавленим державним установам. Процес передачі функціоналу здійснюється на основі заявок від державних органів, які бажають отримати код системи та супутню документацію.

СЕДО «АСКОД» є основним продуктом у функціональному ряді сімейства АСКОД. Головне вікно програми представлено на Рис. 2.3. Крім СЕДО, до складу продуктів сімейства АСКОД входять такі незалежні компоненти, як АСКОД-Архів (який забезпечує процеси доархівного та архівного зберігання) та АСКОД-Адміністратор (який підтримує налаштування системи та розвиток її базового функціоналу за допомогою Framework-конструктора) [14, с. 44].

Серед супутніх застосувань СЕДО, поряд з уже згаданими, можна виділити такі підсистеми АСКОД: «Послуги» (надання адміністративних послуг та реалізація дозвільних процедур через ЦНАП за принципом «єдиного вікна»), «Електронна черга» (оптимізація доступу відвідувачів до посадових

осіб ЦНАП та консультантів з боку постачальників послуг), «Портал» (створення Інтернет-вітрини та формування єдиного інформаційно-комунікаційного середовища як внутрішнього, так і зовнішнього), «Органайзер» (планувальник), «Месенджер» (обмін повідомленнями), «Скан-клієнт» (взаємодія веб-застосувань з планшетним сканером) та ін. [16, с. 27].

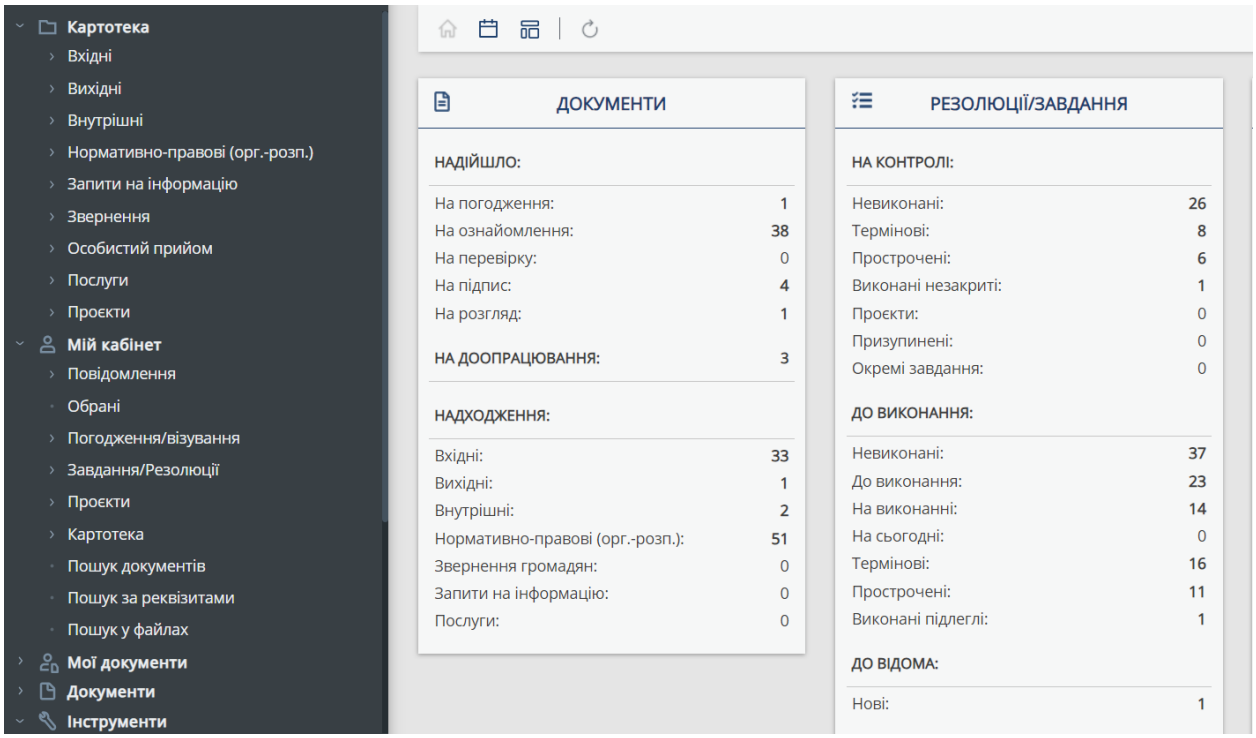

Рис. 2.3. Головне вікно СЕДО АСКОД

Головною метою СЕДО АСКОД та супутніх продуктів є автоматизація процесів організаційно-розпорядчого документообігу на всіх етапах життєвого циклу документа, а також підтримка процедур діловодства і документоведення для таких категорій кореспонденції, як: вхідна, вихідна, внутрішня, нормативно-правова, звернення фізичних і юридичних осіб, а також запити на інформацію [1].

Для системи АСКОД характерний наступний набір операцій обробки інформаційних об’єктів (документів, резолюцій, завдань, запитів та відгуків на узгодження/візування, повідомлень):

- отримання та обробка надходжень інформаційних об’єктів, їх приймання, відхилення та повернення;

- реєстрація, накопичення та надійне зберігання інформаційних об’єктів;
- первинний аналіз документів, визначення маршрутів (технологічних карт) їх обробки;
- формування рішень (у вигляді резолюцій, завдань, доручень) стосовно прийнятих документів, встановлення термінів і видів контролю, призначення виконавців та контролерів (в результаті – організація комунікаційної вертикалі між посадовими особами або підрозділами, що взаємодіють);
- здійснення контролю за виконанням дисципліни;
- спільна розробка проектів відповідей на вхідні документи або ініціативно створюваних вихідних документів, а також забезпечення версійності проектів документів;
- використання механізму узгодження та візування інформаційних об’єктів, зокрема під час колективної роботи над проектами документів, що сприяє організації горизонтальної комунікації між посадовими особами або підрозділами;
- оповіщення про наближення термінів та попередження про перевищення контрольних строків;
- використання наглядного набору індикаторів для візуального контролю стану інформаційних об’єктів, представленого у вигляді панелі кольорових кульок, де кожен колір відповідає певному стану;
- впровадження персоналізованих функціональних середовищ для певних ролей користувачів у вигляді компонента «Мій кабінет»;
- забезпечення ефективної роле-орієнтованої видимості інформаційних об’єктів, що потребують опрацювання, за допомогою функціоналу «Мої документи» (замість того, щоб усі ролі бачили абсолютний стан об’єкта однаково, тут використовується відносне значення стану, яке сприймається по-різному в залежності від виконаних дій над об’єктом);
- формування та передача звіту про виконання резолюції/завдання,

отримання та аналіз звіту, затвердження його результатів або відправка на доопрацювання;

- застосування функціонально розвиненого механізму обміну даними в режимах «АСКОД-АСКОД», «E-mail», «точкаточка» (P2P) та «зірка» (СЕВ ОВВ) для організації внутрішньої комунікації між структурними підрозділами однієї установи, а також для інформаційної інтеграції територіально-розподілених установ або їх підрозділів. При цьому використовуються відповідні сценарії обміну та певні формати надання даних (XML, JSON);
- своєчасне та дострокове завершення обробки документів і резолюцій з подальшим їх закриттям;
- передача закритих документів на оперативне (доархівне) зберігання;
- забезпечення швидкого доступу до оперативних та архівних документів;
- створення розвинутої статистичної та аналітичної звітності (як регламентованої, так і управлінської);
- використання індикаційного табло ключових показників для інформування користувачів з певними ролями (керівників, виконавців, контролерів, діловодів) про поточну ситуацію;
- гарантування конфіденційності інформації завдяки розширеному набору прав доступу для користувачів (переліку дозволів і обмежень);
- використання ЕЦП для гарантування цілісності, встановлення авторства, підтвердження підпису інформаційних об’єктів та надання їм юридичної значущості [9].

СЕДО АСКОД розроблена на основі трирівневої архітектури «клієнт-сервер», орієнтована на застосування системи управління базами даних ORACLE та включає різноманітні клієнтські програми:

- «АСКОД Корпоративний»;
- «АСКОД Мобільний» (АРМ Керівника, що функціонує на планшетах та смартфонах з операційними системами Windows, Android, iOS);

- «АСКОД WEB».

Вибір конкретного варіанту Системи визначається обсягами документообігу, числом користувачів СЕД та особливостями діяльності фахівців.

Основним функціональним елементом системи АСКОД є електронна реєстраційно-контрольна картка документа. Вона дозволяє записувати в численних полях різноманітні дані, що відповідають різним етапам життєвого циклу документа. Окрім великої кількості інформаційних полів та вказаних карток, АСКОД також пропонує широкий спектр різних сервісних функцій. Доповненням до електронних реєстраційно-контрольних карток документу є функціональний об'єкт СЕД, відомий як журнал реєстраційно-контрольних карток. Для зручного управління списком карток цей журнал включає механізм пошуку та широкий набір фільтрів для вибору даних [11].

На базі системи АСКОД автоматизується діяльність ЦНАП-ів. Крім того, СЕД АСКОД використовується у Київській міській державній адміністрації, Національному банку України, Міністерстві оборони України, Генеральному штабі Збройних Сил України, а також в органах місцевої влади та самоврядування Київської, Волинської, Одеської, Миколаївської та Херсонської областей, а також у багатьох інших установах і підприємствах.

СЕДО АСКОД забезпечує інтеграцію з офісними пакетами MS Office, Open Office та LibreOffice на рівні обміну файлами. Щодо інформаційних потоків, СЕД АСКОД здатна інтегруватися з будь-якими інформаційно-комунікаційними системами за допомогою API [7, с. 33].

Отже, сьогодні на українському ринку програмного забезпечення активно представлені системи, що автоматизують діловодство, документообіг та інші адміністративні процеси в органах публічної влади. Функції сучасних СЕДО здатні суттєво підвищити ефективність управлінської діяльності.

ЕА є інформаційною системою, яка забезпечує: створення каталогу документів з визначеною ієрархією; автоматизовану систематизацію та класифікацію документів; зручне збереження документів; повне збереження

інформації, незважаючи на фізичні впливи, технологічні зміни чи зміни форматів даних; доступ користувачів до документів; можливість перегляду та роботи з електронними копіями; пошук документів; резервне копіювання; друк документів; а також адміністрування системи.

СЕДО виконують кілька ключових функцій, серед яких: зберігання та пошук документів, підтримка роботи канцелярії, маршрутизація та контроль за виконанням документів, підготовка аналітичних звітів, забезпечення інформаційної безпеки, а також ряд інших додаткових (специфічних) функцій.

2.2. Загрози та захист інформації в системах електронного урядування як важлива складова безпеки держави в умовах воєнного стану

Практика впровадження систем електронного урядування в різних країнах світу налічує понад два десятиліття. За цей час було накопичено значний досвід, як позитивний, так і негативний. Правильне використання узагальнених результатів таких впроваджень дозволяє економити фінансові та людські ресурси, зменшувати кількість помилок, а також вирішувати проблеми стандартизації, уніфікації та взаємодії національних систем електронного урядування з міжнародними [2, с. 53].

При розробці сучасних систем електронного урядування важливо враховувати досвід різних країн у впровадженні таких систем, зокрема в аспектах основних принципів, підходів та методів створення корпоративних інформаційних структур.

Серед загальних викликів, з якими стикнулися країни під час реалізації електронного урядування, були різні стратегії для подолання труднощів. Наприклад, для більшості держав однією з ключових проблем стало забезпе-

чення сумісності різноманітних інформаційних систем, які розроблялися в різні роки, за різними принципами та на різних технологічних платформах.

Системи електронного урядування функціонують на основі інформаційних систем, які розгорнуті на корпоративних комп'ютерних мережах. Внаслідок цього, на їхнє функціонування впливають також проблеми, притаманні корпоративним структурам. З такими викликами стикаються як фахівці з технічного обслуговування, так і служби інформаційної безпеки в сфері публічного управління. Основними причинами, які спричиняють виникнення подібних проблем, є наступні:

1. Складність і різноманітність програмного та апаратного забезпечення, яке застосовується в системах електронного уряду. У процесі створення систем електронного урядування для виконання важливих завдань застосовуються різні операційні системи. Робочі місця державних службовців зазвичай обладнані операційною системою Windows, тоді як обробка інформації в СЕДО та зберігання важливих інформаційних ресурсів здійснюється в базах даних, що працюють на ОС Linux, FreeBSD або Solaris. Все частіше державні службовці користуються портативними мобільними пристроями (планшетами, смартфонами), що працюють на операційній системі Android. У цьому контексті виникає проблема технічного обслуговування, яка включає управління конфігураціями та оновленнями програмного забезпечення, а також виконання стандартних базових заходів у сфері інформаційної безпеки.

2. Велику кількість вузлів у системах електронного урядування. Велика кількість вузлів корпоративної мережі в системах електронного урядування, їх територіальна розподіленість та брак часу для контролю конфігураційних параметрів основних програмних засобів становлять серйозну проблему. Часто вузли, що обробляють важливу інформацію в рамках корпоративної мережі системи електронного урядування, розташовані не лише в межах одного міста, а й у різних регіонах або навіть країнах. Ця характеристика, а також брак часу для перевірки необхідних налаштувань програмного забезпе-

чення, ускладнює технічному персоналу своєчасний моніторинг діяльності і безпеки користувачів у розподілених системах електронного урядування.

3. Наявність зовнішнього доступу до системи електронного урядування. Однією з ключових проблем, що виникають внаслідок функціонування системи електронного урядування, є забезпечення підключення зовнішніх користувачів (підприємств, організацій, окремих громадян) до відкритих сервісів. Це також включає надання прав персоналу органу публічного управління для віддаленої роботи з внутрішніми інформаційними ресурсами. З одного боку, це відкриває нові можливості, а з іншого — призводить до збільшення загальної кількості вразливостей, які постійно виникають у корпоративній мережі. Вразливості, які присутні в програмному забезпеченні систем електронного урядування, можуть призвести до несанкціонованого доступу до інформаційних ресурсів. Тому для їх усунення та забезпечення належного рівня захисту інформації в системах електронного урядування використовуються різноманітні механізми та засоби безпеки. Налаштування цих засобів залежить від технології обробки інформації, що застосовується в системах публічного адміністрування. Комплекс таких правил, законів і практичних рекомендацій викладено в політиці безпеки, яка враховує різні аспекти процесу обробки інформації. До інструментів, що забезпечують реалізацію політики безпеки та, відповідно, ефективний захист технологій обробки інформації, належать: міжмережеві екрани, системи виявлення атак, системи шифрування трафіку, системи контролю «мобільного коду» (Java, ActiveX) та інші засоби.

4. Робота груп технічного обслуговування та інформаційної безпеки. У системах електронного урядування група технічного обслуговування переважно відповідає за вирішення завдань, пов’язаних із системним і мережевим адмініструванням. Група інформаційної безпеки займається питаннями, що стосуються процесів у сфері інформаційної безпеки на адміністративному, організаційному, технічному та інших рівнях. У цьому контексті виникає проблема чіткого розмежування функціональних обов’язків

персоналу цих груп, які відповідають за технічний рівень. Наприклад, це включає обслуговування віддаленого доступу користувачів до інформаційних ресурсів системи електронного урядування, а також роботу з основними службами та сервісами корпоративної мережі, такими як DNS і електронна пошта, а також прикладними системами, такими як ЕД [8, с. 19].

Отже, при розробці та експлуатації системи електронного урядування необхідно вирішити ключові питання, пов'язані як з її технічним обслуговуванням, так і з інформаційною безпекою.

У Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 № 447/2021, зазначено, що загрози для кібербезпеки виникають внаслідок впливу ряду чинників, зокрема:

- невідповідність інфраструктури електронних комунікацій держави її рівню розвитку та сучасним вимогам захищеності;
- недостатня захищеність критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, захист якої передбачений законодавством, від кіберзагроз;
- відсутність системного підходу до заходів кіберзахисту критичної інформаційної інфраструктури;
- невисокий рівень розвитку організаційно-технічної інфраструктури для забезпечення кібербезпеки та захисту критичної інформаційної інфраструктури, а також державних електронних інформаційних ресурсів;
- низька ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам, що виникають внаслідок військових, кримінальних, терористичних та інших дій;
- недостатня координація, взаємодія та обмін інформацією між суб'єктами, що займаються забезпеченням кібербезпеки [43].

У вказаній Стратегії зазначено, що інформаційній безпеці загрожують ведення інформаційної війни проти України, відсутність єдиної комунікативної політики з боку держави та низький рівень медіа-культури в суспільстві.

Загрози інформаційній безпеці охоплюють комплекс умов і факторів, які становлять небезпеку для життєво важливих інтересів суспільства, держави та особи. В цілому, під загрозою інформаційній безпеці розуміють потенційно можливу подію, дію, процес або явище, що можуть завдати шкоди системі [23, с. 28]. Згідно з більш детальним визначенням, загроза інформаційній безпеці системи полягає в можливості впливу на інформацію, що може призвести до порушення конфіденційності, цілісності або доступності даних. Крім того, це також включає можливість впливу на компоненти системи, що може викликати втрату або знищення інформації, а також збої у роботі інформаційної системи [3, с. 117].

Класифікацію загроз інформаційній безпеці можна проводити за різними критеріями. Розглянемо найбільш поширені з них, що представлені на Рис. 2.4.

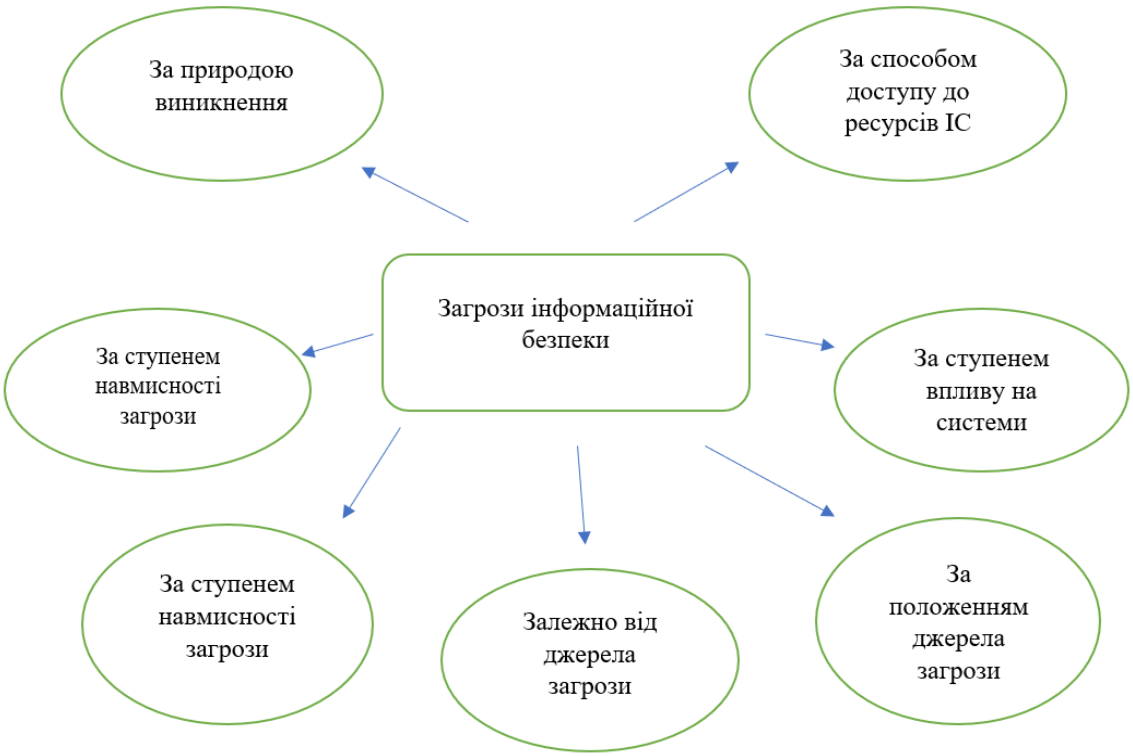

Рис. 2.4 Класифікація загроз інформаційній

1. За природою виникнення:

- природні – загрози, що виникають внаслідок впливу об’єктивних фізичних процесів або стихійних природних явищ, які не підлягають контролю

людини (до природних загроз відносяться пожежі, повені, цунамі, землетруси, техногенні аварії). Неприємною рисою таких загроз є їхня надзвичайна складність або навіть неможливість прогнозування;

- штучні загрози – це загрози, які виникають внаслідок діяльності людини.

2. За ступенем навмисності загрози:

- випадкові – виникають через недбалість або ненавмисні помилки співробітників. Прикладами випадкових загроз можуть бути ненавмисне введення неправильних даних або випадкове пошкодження обладнання;
- навмисні – зазвичай є наслідком цілеспрямованих дій зловмисників. Наприклад, навмисна загроза може проявитися під час роботи з веб-інтерфейсом інформаційної системи, коли на базу даних здійснюється атака за допомогою SQL-ін’єкцій з метою зміни або видалення важливих даних.

3. Залежно від джерела загрози:

- загрози, що виникають з природного середовища. Прикладами таких загроз є різке підвищення або зниження температури повітря, геомагнітні аномалії, повені, буревії та інші стихійні лиха;
- загрози, що походять від людської діяльності. Прикладом такої загрози може бути призначення недержавною організацією своїх довірених осіб на посади, які відповідають за обслуговування державних інформаційних систем;
- загрози, що виникають внаслідок використання санкціонованих програмно-апаратних засобів. Прикладом такої загрози є некомпетентне застосування системних утиліт;
- загрози, пов’язані з несанкціонованими програмно-апаратними засобами. До таких загроз можна віднести, наприклад, встановлення кейлогерів у систему. Використання особистих носіїв (флешок, MP3-плеєрів, мобільних телефонів) може призвести до зараження шкідливим програмним забезпеченням.

4. За положенням джерела загрози:

- загрози, джерело яких знаходиться за межами контрольованої зони. До таких загроз можна віднести перехоплення побічних електромагнітних випромінювань або даних, що передаються через канали зв'язку; дистанційне фото- та відеоспостереження; перехоплення акустичної інформації за допомогою направлених мікрофонів;

- загрози, джерело яких розташоване в межах контрольованої зони. Прикладами таких загроз можуть бути використання пристроїв для підслуховування або крадіжка носіїв, що містять конфіденційну інформацію.

5. За ступенем впливу на системи:

- пасивні загрози – це такі загрози, які не викликають жодних змін у складі та структурі інформаційної системи під час їх реалізації. Прикладом пасивної загрози може слугувати несанкціоноване копіювання файлів, що містять дані;

- активні загрози. Реалізація активних загроз призводить до порушення структури інформаційної системи. Наприклад, це може бути вторгнення зловмисника в інформаційні ресурси системи електронного урядування з метою моніторингу та перегляду вмісту мережевого трафіку для перехоплення паролів або інших важливих даних.

6. За способом доступу до ресурсів ІС:

- загрози, що реалізуються через стандартний доступ. Прикладом такої загрози є несанкціоноване отримання пароля шляхом підкупу, шантажу, неналежного зберігання або фізичного насильства щодо законного власника;

- загрози, що виникають через нестандартні методи доступу. Прикладом такої загрози є використання незадекларованих функцій засобів захисту. Класифікацію загроз можна продовжувати, проте на практиці найчастіше застосовується класифікація, що базується на трьох основних властивостях інформації, яка підлягає захисту (див. Рис. 2.5) [8, с. 22].

Рис. 2.5. Класифікація загроз, що ґрунтується на базових властивостях інформації

Слід зазначити, що реальні загрози інформаційній безпеці не завжди можна однозначно віднести до жодної з наведених вище категорій. Наприклад, загрози викрадення носіїв інформації за певних умов може бути віднесена до всіх трьох категорій [8, с. 23].

Важливо додати, що питання глобальної інформаційної безпеки посідає особливе місце в міжнародній інформаційній політиці та знаходять своє відображення у звітах авторитетних організацій (наприклад: ООН, ОБСЄ, ЄС).

Відоме Європейське агентство з мережевої безпеки (European Network and Information Security – ENISA) було створено на початку 2004 року для вирішення питань, пов'язаних з вирішенням критичних проблем у сфері інформаційної безпеки.

Основними завданнями агентства є підвищення здатності європейських електронних мереж протистояти зовнішнім впливам і атакам, збір та аналіз даних для комп'ютерні зломи в Європі, а також розробка методів оцінки та управління ризиками для поліпшення здатності ЄС реагувати на загрози інформаційній безпеці [59].

Стандарти інформаційної безпеки, відомі як «Європейські критерії», які були розроблені в країнах Європи (зокрема у Франції, Німеччині, Нідерландах та Великобританії), охоплюють такі завдання в сфері інформаційної безпеки:

1) захист інформації від несанкціонованого доступу для гарантування конфіденційності;

2) забезпечення цілісності даних шляхом захисту від

несанкціонованих змін або знищення;

3) підтримка працездатності систем шляхом протидії загрозам відмови в обслуговуванні [17, с. 55].

Для вирішення проблеми запобігання загрозам інформаційних систем було введено поняття гарантій засобів захисту. Ці гарантії включають два аспекти:

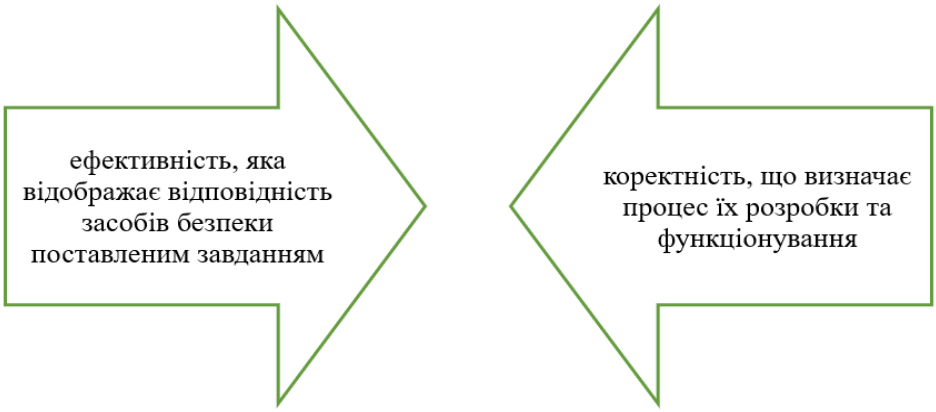

Рис. 2.6. Двоаспектність гарантій засобів захисту інформаційних систем

У «Європейських критеріях» визначено сім рівнів гарантій: від Е0 до Е6, які розташовані в порядку зменшення ймовірності виникнення загрози. Рівень Е0 відповідає мінімальним гарантіям, що є аналогом рівня D з «Жовтогарячої книги». Під час перевірки гарантій здійснюється аналіз життєвого циклу інформаційної системи, починаючи з початкової фази проектування і закінчуючи експлуатацією та супроводом.

Рівні гарантій від Е1 до Е6 характеризуються поступовим ускладненням вимог до ретельності та контролю. Наприклад, на рівні Е1 проводиться лише загальний аналіз архітектури інформаційної системи, а підтвердження гарантій засобів захисту здійснюється через функціональне тестування.

На етапі Е3 до аналізу підключаються вихідні тексти програм та схеми апаратного забезпечення. На етапі Е6 необхідно мати формальний опис функцій безпеки, загальної архітектури та політики безпеки, які забезпечують мінімізацію ризиків від загроз [8, с. 23-24].

Отже, у «Європейських критеріях» виділено три рівні інформаційної

безпеки: базовий, середній та високий. Базовий рівень інформаційної безпеки характеризується здатністю засобів захисту протистояти окремим випадковим атакам. Середній рівень вважається таким, коли засоби захисту можуть протистояти зловмисникам з обмеженими ресурсами та можливостями. Інформаційну безпеку можна вважати надійною, якщо існує впевненість, що засоби захисту можуть бути подолані лише зловмисниками з високим рівнем кваліфікації, які мають значні можливості та ресурси.

Історично потреба в захисті інформації від внутрішніх загроз завжди була важливою на всіх етапах розвитку засобів інформаційної безпеки. З часом увага до внутрішніх загроз, таких як витік інформації, зросла.

Основою витоку інформації є процес перенесення або передачі енергії чи речовини, які виконують роль носіїв інформації.

З точки зору фізичної природи, існують такі способи передачі інформації: світлові промені, звукові хвилі, електромагнітні хвилі, а також матеріали і речовини.

Будь-який сигнал, що передається, може бути перенесений або енергією, або матерією. Це може бути акустична хвиля (звук), електромагнітне випромінювання (світло, радіохвилі) або ж лист паперу (або інший носій написаного тексту).

Застосовуючи різні фізичні поля, людина формує певну систему для передачі інформації між собою. Такі системи зазвичай називають системами зв’язку. Кожна система зв’язку включає джерело інформації, передавач, канал передачі та приймач (одержувача інформації). Ці системи активно використовуються відповідно до їх призначення і слугують засобами для передачі інформації [8, с. 24].

Процес передачі інформації загалом відбувається наступним чином (див. Рис. 2.7). Джерело інформації представляє собою суб’єкт, який створює певне повідомлення, звукові коливання, текст тощо. У джерелі сигналу (або перетворювачі) ці повідомлення перетворюються на сигнали: електричні, звукові, світлові тощо. Такі сигнали набувають форми, що підходить для їх

передачі через канали зв’язку. Канал зв’язку переносить сигнали з одного місця в інше до отримувача інформації [8, с. 26].

Рис. 2.7. Загальна схема передачі інформації

Витік інформації у контексті обговорюваного процесу передачі даних розглядається як несанкціоноване розповсюдження відомостей за межі системи передачі інформації. Також витік може відбуватися через певну групу осіб, яким були довірені деякі дані.

Витік інформації, по своїй суті, означає незаконне (усвідомлене або випадкове, таємне або явне) отримання інформації, яка не повинна бути розповсюджена, незалежно від способу її здобуття.

Несанкціоноване отримання інформації з технічних каналів є поширеним явищем. Такі канали витоку складаються з небезпечних фізичних сигналів, середовищ їх розповсюдження та зберігання, об’єктів технічної розвідки, а також різних методів і засобів технічної розвідки. На основі аналізу наукових досліджень була розроблена узагальнена схема можливих каналів витоку та несанкціонованого доступу до інформації, що обробляється в типовому одноповерховому офісі.

Класифікація каналів витоку інформації може бути розділена на:

- акустичні канали витоку інформації, які включають також канали з акустично-електричними перетвореннями;
- радіотехнічні канали витоку інформації, що охоплюють відкриті канали радіозв’язку, а також канали, які виникають внаслідок паразитних випромінювань і наведення;

- оптичні канали витоку інформації;
- речові канали витоку інформації, що залежать від людського фактору [50, с. 22].

Отже, коректне визначення каналів витоку інформації та загроз безпеці в системах електронного урядування дозволяє розробити ефективні методи протидії цим загрозам.

Відповідно, по-перше, при розробці сучасних систем електронного урядування важливо враховувати досвід різних країн світу у впровадженні подібних систем, зокрема в аспектах основних принципів, підходів та методів створення корпоративних інформаційних структур. Основними причинами, які можуть спричинити проблеми з безпечним функціонуванням систем електронного урядування, є: складність і різноманітність програмного та апаратного забезпечення, що використовується в цих системах; велика кількість вузлів у системах електронного урядування; наявність зовнішнього доступу до системи; а також діяльність груп, відповідальних за технічне обслуговування та інформаційну безпеку.

По-друге, загрози інформаційній безпеці охоплюють сукупність умов і факторів, які можуть загрожувати життєво важливим інтересам суспільства, держави та особи. Загроза інформаційній безпеці системи визначається як ймовірність впливу на інформацію, що може призвести до порушення конфіденційності, цілісності або доступності даних. Також це включає можливість впливу на елементи системи, що може викликати втрату або знищення інформації, а також збої в роботі інформаційної системи.

По-третє, загрози інформаційній безпеці можна класифікувати за різними критеріями, що дає змогу обирати та використовувати ефективні методи і засоби захисту інформації в системах електронного урядування.

По-четверте, застосування стандартів інформаційної безпеки «Європейські критерії», розроблених у провідних країнах Європи (Франція, Німеччина, Нідерланди та Великобританія), передбачає виконання таких основних завдань: захист інформації від несанкціонованого доступу для

забезпечення конфіденційності; гарантування цілісності інформації шляхом захисту від несанкціонованої модифікації або знищення; забезпечення функціонування систем шляхом протидії загрозам відмови в обслуговуванні.

По-п’яте, витік інформації визначається як неправомірне (усвідомлене чи випадкове) отримання інформації, яка не повинна бути розповсюджена, незалежно від способу її отримання. Коректне визначення каналів витоку інформації та загроз безпеці в системах електронного урядування дозволяє розробити ефективні методи для протидії цим загрозам [25, с. 164].

Отже, проблема інформаційної безпеки та культури в умовах війни є критично важливою для виживання як окремої особи, так і суспільства і держави, в цілому. Основними її складовими є цілісність даних, доступність інформації, конфіденційність та надійність її зберігання.

Сучасні загрози інформаційній безпеці становлять виклик, який виходить за межі нашої країни і впливає не лише на національний простір, але й має серйозні глобальні наслідки. У зв’язку з цим, для запобігання та протидії цим загрозам необхідно не лише розробити нормативно-правову базу, а й забезпечити ефективне функціонування інституційного механізму інформаційної безпеки, включаючи освітній аспект. Йдеться про послідовну та системну діяльність державних і правових інституцій, які повинні ефективно реалізовувати національні інтереси в інформаційній сфері. Вони мають бути здатні не лише оперативно реагувати на поширення інформаційних фейків та неправдивих відомостей, а й запобігати інформаційним конфліктам та формувати загальну інформаційну культуру суспільства. Крім того, з огляду на існуючі глобальні загрози та виклики, ефективно протидіяти інформаційній агресії, залучаючи до цього процесу міжнародні організації, інституції та міжнародну спільноту. Окрім того, важливо, при розробці сучасних систем електронного урядування враховувати досвід різних країн у впровадженні подібних систем, зокрема в аспектах основних принципів, підходів та методів створення корпоративних інформаційних структур.

Висновки до Розділу 2

Сьогодні на українському ринку програмного забезпечення активно представлені системи, що автоматизують діловодство, документообіг та інші адміністративні процеси в органах публічної влади. Функції, які пропонують сучасні СЕДО, здатні суттєво підвищити ефективність управлінської діяльності. Це такі функції як: зберігання та пошук документів, підтримка канцелярської роботи, маршрутизація та контроль за виконанням документів, підготовка аналітичних звітів, забезпечення інформаційної безпеки, а також ряд інших додаткових (специфічних) функцій.

Основними причинами, які можуть спричинити проблеми з безпечним функціонуванням систем електронного урядування, є: складність і різноманітність програмного та апаратного забезпечення, що використовується в цих системах; велика кількість вузлів у системах електронного урядування; наявність зовнішнього доступу до системи; а також діяльність груп, що займаються технічним обслуговуванням і інформаційною безпекою.

Інформаційна безпека має надзвичайно важливе значення, особливо в умовах війни. Дезінформація може спричинити паніку серед населення, негативно вплинути на розвиток подій, прискорити внутрішню міграцію, що, в свою чергу, може погіршити боєздатність Збройних Сил України, а також вплинути на фізичний і психічний стан громадян. Зважаючи на це, ефективна протидія інформаційній агресії можлива за рахунок залучення міжнародних організацій, інституцій та світової спільноти в цілому. Практика демонструє, що для ведення інформаційної війни не існує кордонів. Тому важливо захищати відкритий інформаційний простір країни від ворожих впливів і маніпуляцій.

РОЗДІЛ 3
ПОСИЛЕННЯ БЕЗПЕКИ ФУНКЦІОНУВАННЯ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В СФЕРІ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ВОЄННОГО СТАНУ

3.1. Проблеми розвитку системи електронного документообігу в сфері публічного управління та способи їх вирішення

Сьогодні важливою проблемою розвитку українського державотворення є створення інформаційного суспільства, в якому значну роль відіграє взаємодія не лише між органами публічної влади, такими як органи державної влади (глава держави – Президент України; законодавча влада – Верховна Рада України; виконавча влада – Кабінет Міністрів України, міністерства, відомства, центральні органи виконавчої влади зі спеціальним статусом, місцеві державні адміністрації з підзвітними підприємствами, установами та організаціями державної форми власності; судова влада – Верховний Суд України, вищі спеціалізовані, апеляційні та місцеві суди; силові органи – Національна поліція України, Служба безпеки України, Генеральна прокуратура України, Збройні Сили України тощо) та органами місцевого самоврядування (місцеві ради, органи самоорганізації населення), а також з приватним сектором, до якого входять юридичні особи (підприємства, установи та організації).

Розв’язання цієї проблеми можливе за умови вдосконалення системи електронного урядування, яка в Україні почала впроваджуватися на основі Концепції розвитку електронного урядування, затвердженої розпорядженням Кабінету Міністрів України від 20 вересня 2017 року № 649-р.

Ця концепція має на меті підвищення якості обслуговування фізичних та юридичних осіб шляхом прискорення обміну інформацією між органами

публічної влади та приватним сектором [45].

Однак основною проблемою в органах публічної влади України є, насамперед, відсутність відповідного програмного забезпечення, яке б забезпечувало працівникам можливість швидкої передачі та отримання інформації під час виконання їхніх обов'язків у різних сферах діяльності (консультації, стратегічне планування, тестування; збір, обробка та зберігання даних; ремонтні роботи, навчання персоналу тощо).

Згідно зі ст. 8 Угоди про Асоціацію між Україною та Європейським Союзом, Європейським співтовариством з атомної енергії та їхніми державами-членами, угоди щодо комп'ютерних послуг передбачають можливість надання як електронних послуг (без необхідності фізичної присутності клієнта в установі), так і неелектронних (за умови відвідування установи для отримання послуг), що стосуються роботи з комп'ютерними програмами [52].

У таких умовах органам публічної влади необхідно пройти процедуру укладення договорів на основі публічно-приватного партнерства. Це дозволить забезпечити постійну взаємодію з виробниками комплексного програмного забезпечення, закупівля якого сприятиме, по-перше, активнішій співпраці між органами влади, а по-друге, досягненню високих результатів (збільшення рейтингу публічних установ) та ефекту (підвищення рівня довіри до влади з боку приватного сектору) у наданні послуг.

Ще однією проблемою, яка особливо гостро проявляється в органах публічної влади України, є низький рівень обізнаності працівників щодо використання ІКТ у процесі виконання їх службових обов'язків. Багато співробітників, особливо старшого віку, сприймають ІКТ як джерело незручностей та витрат часу на освоєння роботи з різними електронними системами у відповідних структурних підрозділах. Це часто призводить до непорозумінь між керівництвом і підлеглими, а також між колегами, які надають перевагу безпосередньому спілкуванню з людьми, а не роботі через електронні засоби. Для вирішення цієї проблеми необхідно впровадити в

органах публічної влади спеціальний план-графік короткострокових семінарів, тренінгів, навчальних програм та курсів підвищення кваліфікації, спрямованих на освоєння роботи з ІКТ [46, с. 346].

Отже, основною проблемою розвитку електронного урядування в Україні, пов'язаною з вищезгаданими труднощами, є відсутність стратегічного підходу з боку керівництва органів публічної влади щодо виділення фінансування на загальні потреби держави та громадян. Це особливо актуально у випадках, коли громадянам необхідно отримати корисну інформацію про певні послуги, консультації щодо їх надання та ухвалення рішень про отримання або відмову від цих послуг. Тому збільшення обсягу державних інвестицій у приватні компанії, які займаються виробництвом технічних і програмних продуктів, а також приділення більшої уваги фінансуванню закупівлі цих продуктів і навчання кваліфікованого персоналу органів публічної влади, значно прискорить реалізацію Концепції розвитку електронного урядування в Україні. Це може стати суттєвим кроком вперед у розвитку інноваційної інфраструктури та значно поліпшити інвестиційний клімат в країні.

На сьогодні розвиток інформаційного суспільства в Україні викликає чимало спірних питань, пов'язаних із становленням громадянського суспільства. Це створює можливості для певних груп населення об'єднуватися в неприбуткові організації та встановлювати співпрацю з органами публічної влади. Як зазначає дослідниця М.В. Скиба у своїй праці, громадянське суспільство є інститутом, що об'єднує людей на основі спільних цінностей, культурно-моральних та політичних інтересів, забезпечуючи права і свободи громадян у вільному виборі своїх позицій в економічному та соціальному середовищі. Оскільки економічні та соціальні потреби населення змінюються з часом, зростає потреба у тісній співпраці між державою та суспільством. Така співпраця можлива лише за умови дотримання обома сторонами європейських принципів інформаційної взаємодії, зокрема: участі, довіри, підзвітності, прозорості та незалежності [49].

Проте дотримання зазначених вище принципів усіма учасниками інформаційних відносин вимагає наявності підтвердженої інформації як про постачальників, так і про отримувачів відповідних послуг. Особливо цю думку підтримують деякі закордонні науковці.

Наприклад, Дж. Р. Гіл-Гарсія у своїй роботі підкреслив, що ключовим фактором успіху співпраці між громадськими організаціями та органами державної влади є належне налаштування веб-сайтів останніх, які повинні відображати рівень ефективності роботи уряду в контексті виконання службових обов'язків працівниками урядових установ та підзвітних організацій щодо обслуговування фізичних і юридичних осіб [47, с. 100].

Однак така процедура вимагає, по-перше, наявності комп'ютерної техніки, по-друге, високошвидкісного Інтернету, а по-третє, кваліфікації працівників у використанні відповідних веб-ресурсів на робочому місці. Сукупність цих чинників формує електронний уряд, тобто урядову систему, що базується на застосуванні ІКТ суб'єктами інформаційних відносин для швидкого обміну необхідною інформацією, яка буде використана в подальшій діяльності [56, с. 142].

Е. Тротта пропонує використовувати термін «електронне урядування» для позначення системи електронної взаємодії між учасниками електронного уряду. Водночас «електронний уряд» він трактує як частину електронного урядування, що включає органи виконавчої влади, які мають повноваження співпрацювати з прибутковими та неприбутковими організаціями, а також з громадянами, які звертаються до них з проханнями задовольнити свої потреби, використовуючи ІКТ [60, с. 47].

Отже, враховуючи затверджену розпорядженням Кабінету Міністрів України Концепцію розвитку електронного урядування в Україні, яка визначає електронне урядування як форму організації державного управління, що ґрунтується на принципах ефективності, відкритості та прозорості діяльності органів державної влади та місцевого самоврядування з використанням ІКТ, орієнтовану на задоволення потреб громадян [45] (див. Рис. 3.1).

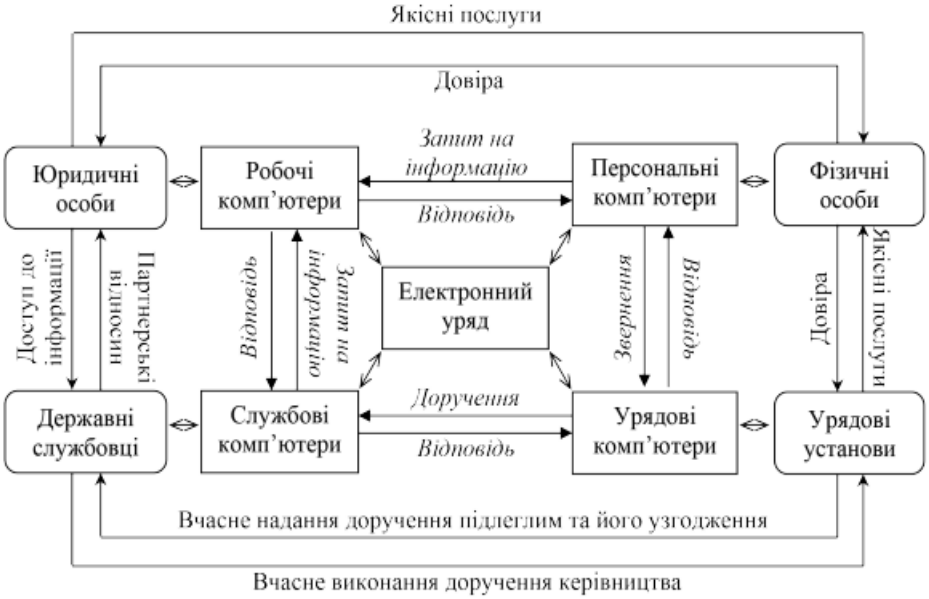

Рис 3.1. Електронне урядування як система електронної взаємодії суб'єктів електронного уряду

Як видно, учасниками електронного уряду є суб'єкти інформаційних відносин, які під час звернення за інформацією, а також її надання та отримання взаємодіють один з одним за допомогою комп'ютерної техніки, використовуючи різні електронні системи. Це, завдяки мережі Інтернет, дозволяє обмінюватися інформацією у формі службових документів.

Урядові установи, зокрема органи виконавчої влади, надсилають доручення іншим органам виконавчої влади. Це доручення може бути підготовлене на основі: постанови або розпорядження Кабінету Міністрів України, наказу міністерства, відомства чи центрального органу виконавчої влади зі спеціальним статусом, які були розроблені та затверджені відповідно до певного закону або указу Президента України; депутатського звернення; розпорядження місцевої державної адміністрації, що розроблене та затверджене на основі рішення місцевої ради та інших документів. Всі ці дії здійснюються через електронну систему урядових комп'ютерів, розташованих у відповідних канцеляріях.

Доручення надходить до представника керівництва органу (керівника, першого заступника або заступника керівника) через канцелярію, де він накладає резолюцію та направляє його до підпорядкованих структурних

підрозділів. Отримавши це доручення на своїх службових комп'ютерах, керівники зазначених підрозділів також накладають резолюцію і пересилають його на виконання своїм підлеглим, які виконують повноваження в межах компетенції структурного підрозділу, що відповідає за управління певною галуззю діяльності.

З метою виконання контрольного доручення, працівники відокремлених галузевих структурних підрозділів органів виконавчої влади, як правило, надсилають запити на інформацію до відповідних юридичних осіб – представників приватного сектору. Ці особи можуть надати інформацію у повному обсязі через встановлену електронну систему на своїх робочих комп'ютерах, але лише за умови налагодження партнерських відносин. Зазвичай, такі відносини пов'язані з державно-приватним партнерством, яке оформлюється укладеними договорами між органами виконавчої влади та приватними підприємствами. Ці угоди також фіксуються в електронному вигляді під час реєстрації підприємств у електронних базах даних. Таким чином, ефективна інформаційна взаємодія між державним і приватним секторами створює можливості для державних службовців встановлювати зв'язки з громадянами України під час обробки їхніх звернень. Працівники, які мають доступ до інформації, завжди можуть надати рекомендації щодо підприємств, установ або організацій, до яких слід звернутися для отримання якісних послуг, а також допомогти у вирішенні галузевих питань [54, с. 169].

Отже, інформаційна взаємодія між урядовими організаціями та державними службовцями сприяє своєчасному наданню доручень підлеглим та їх узгодженню через накладення електронної резолюції з боку керівництва, а також своєчасному виконанню цих доручень підлеглими. Це, в свою чергу, дозволяє встановити партнерські відносини між державним і приватним секторами шляхом укладення електронних договорів з накладенням ЕЦП обома сторонами. Таким чином, галузеві структурні підрозділи органів виконавчої влади отримують всю необхідну інформацію для надсилання адресатові – ініціатору доручення. За таких умов державні службовці, які

працюють у відповідних підрозділах, завдяки постійній інформаційній взаємодії з приватним сектором, що займається певним видом діяльності, завжди матимуть можливість надавати конструктивні відповіді громадянам на їх звернення, надіслані через електронну систему на їхні персональні комп'ютери.

Зважаючи на викладене можна говорити про те, що електронне урядування сприяє підвищенню рівня довіри населення як до підприємств, установ та організацій приватного сектору через встановлення партнерських відносин з органами виконавчої влади, так і до держави в цілому завдяки зростанню кількості задоволених громадян, які отримують електронні державні послуги. Це, в свою чергу, призводить до об'єднання певної групи громадян у громадські організації для забезпечення постійної інформаційної взаємодії з органами публічної влади за допомогою інструментів електронної участі, таких як електронні звернення, електронні петиції, відкритий бюджет та громадський бюджет. У таких умовах громадяни мають більше можливостей для участі в електронних нарадах, форумах, конференціях та інших заходах, присвячених обговоренню різних питань. Це стає можливим завдяки процедурі реєстрації на веб-сайті органу публічної влади або його структурного підрозділу, що сприяє розвитку електронної демократії в суспільстві [55, с. 43].

Отже, як свідчить міжнародний досвід, електронне урядування сприяє покращенню якості життя населення країни завдяки швидкому доступу фізичних та юридичних осіб до якісних послуг. Використання електронних систем дозволяє представникам органів публічної влади економити час на обробку питань, зазначених у документах, отриманих через електронну систему, а також на вжиття необхідних заходів для їх вирішення. Водночас, наявність лише паперової інформаційної системи лише подовжує час очікування отримання офіційно підтвердженої інформації у вигляді документів від представників органів публічної влади, що ускладнює виконання завдань для громадськості через бюрократичні процедури збору

мокрих підписів та печаток.

Одним із ключових показників ефективності реалізації інноваційної політики держави є її позиція в глобальних рейтингах. Україна представлена в численних міжнародних рейтингах, які оцінюють її інноваційний потенціал, здатність до інновацій та результати інноваційної політики. Всебічну характеристику цих аспектів надають, зокрема, такі рейтинги: Глобальний індекс інновацій ГІІ (The Global Innovation Index) , Глобальний індекс стійкої конкурентоспроможності ГІСК (The Global Sustainable Competitiveness Index), Глобальний індекс конкурентоспроможності талантів ГІКТ (The Global Talent Competitiveness Index), Зведений інноваційний індекс ЗІІ (Summary Innovation Index – SII) та Індекс людського розвитку ІЛР (Human Development Index).

Динаміка рейтингів України за чотирма основними підходами до оцінки інноваційної спроможності в період з 2015 року до 2022 року – Глобальний інноваційний індекс (ГІІ), Глобальний індекс стартапів і підприємництва (ГІСК), Глобальний індекс ІКТ та Звіт про інновації (ЗІІ) – свідчить про те, що наша країна займає досить скромні позиції. Проте в останні роки спостерігається позитивна тенденція до покращення деяких показників. Наприклад, у міжнародному рейтингу ГІСК у 2022 році Україна потрапила до топ-50 серед 180 країн світу (див. Рис. 3.2) [19, с. 18-19].

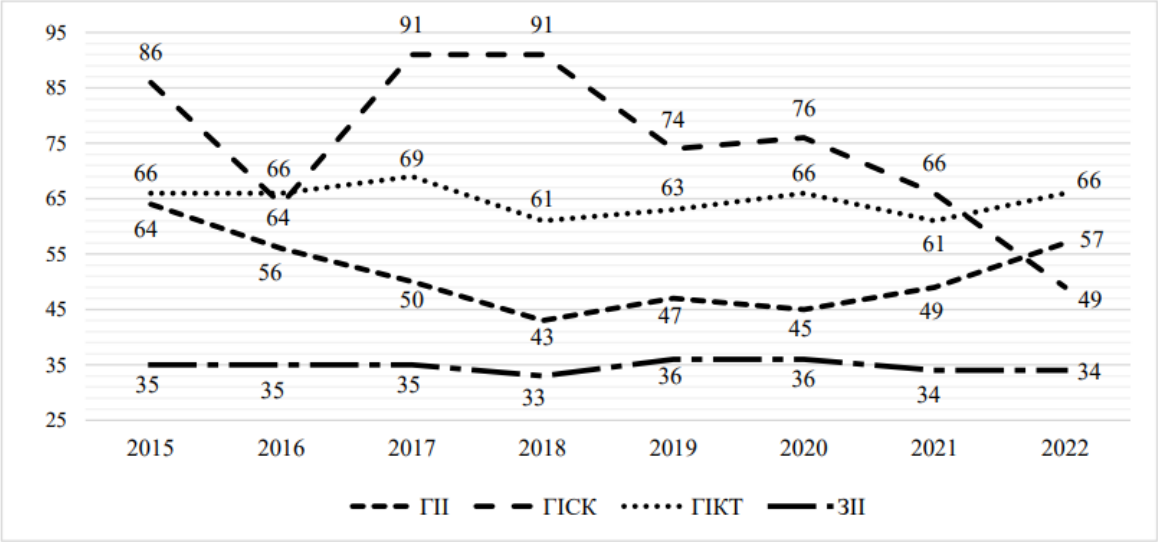

Рис. 3.2. Рейтинги України за індексами інноваційної спроможності

Позиції України в міжнародних рейтингах інноваційного розвитку свідчать про високий рівень науково-освітнього потенціалу, який є основою конкурентоспроможності української науково-інноваційної сфери, а також підґрунтям для наукових розробок, інновацій, нових технологій тощо. Проте, з іншого боку, результати оцінювання науково-інноваційної спроможності України вказують на наявність ряду проблем:

- відсутність ефективного та потужного механізму впровадження інновацій у сферу економічної діяльності та їх подальшої комерціалізації;
- недостатня державна підтримка інноваційних проєктів та їх фінансування, як з державного бюджету, так і з боку приватних інвесторів;
- не використання всіх можливостей, передбачених Угодою про асоціацію між Україною та ЄС, зокрема в аспектах науково-технологічного співробітництва, розвитку підприємництва та промислової політики;
- низький рівень співпраці між інноваційними підприємствами та науково-дослідними установами [48, с. 111].

Отже, ми пропонуємо можливі шляхи покращення виконання Урядом плану дій щодо реалізації Концепції розвитку електронного урядування в Україні, спираючись на наукові дослідження окремих українських та іноземних вчених.

Як зазначено у Додатку А, кожен пункт плану заходів щодо реалізації Концепції розвитку електронного урядування в Україні повинен бути виконаний Урядом з дотриманням принципів прозорості (запобігання корупції), верховенства права (гарантування інформаційної безпеки), взаємодії (довіра до приватного сектору), державної підтримки (інвестиційна підтримка як прибуткових, так і неприбуткових організацій) та професіоналізму (підвищення кваліфікації кадрів в органах публічної влади).

Система надання електронних послуг державою повинна функціонувати в рамках єдиної системи електронного сервісу (е-сервісу). У цій системі через промислову платформу постійно проводитиметься автоматизована перевірка стандартів і ліцензій, які підтверджують законність діяльності державних

установ, що надають різні послуги юридичним та фізичним особам. Додатково, за допомогою промислової платформи, державна установа зможе зв’язуватися з прибутковими організаціями, де встановлені ціни та терміни обслуговування, для оцінки надійності приватних підприємств. У разі потреби, громадянам буде надана інформація про ці організації у відповідь на їх запити. Проте, для досягнення цієї мети органи публічної влади повинні, по-перше, забезпечити інвестиційну підтримку промисловим підприємствам, що виробляють ці платформи з метою їх подальшого придбання; по-друге, розробити програми підвищення кваліфікації, які формують у публічних службовців відповідальність за результати надання різних видів послуг із використанням промислової платформи [51, с. 152-153].

Система відкритих даних повинна бути реалізована шляхом накладення електронного коду (е-коду) на інформацію, що надсилається до спеціалізованих структурних підрозділів органів публічної влади. Використання спеціального програмного забезпечення дозволяє працівникам автоматизувати обробку документів у СЕДО, на які накладено ЕЦП, а також обробляти фотографії подій, зафіксованих у певний момент часу, для підтвердження достовірності надісланої інформації, яка буде розміщена на сайті відповідного органу публічної влади [53, с. 33].

Додатково, під час отримання статистичних даних від приватних підприємств, які мають бути оприлюднені на сайті (наприклад, річний обсяг реалізованої продукції), процес зчитування даних дозволяє оцінити потужність підприємства та проаналізувати можливі похибки в надісланій інформації.

Однак, впровадження такої системи вимагає від держави, по-перше, інвестиційної підтримки виробників відповідних програмних продуктів; по-друге, розробки програм підвищення кваліфікації для працівників органів публічної влади, що дозволить їм здобути необхідні навички для прийняття рішень щодо розміщення інформації на сайті органу публічної влади на основі автоматизованої обробки даних.

Розвиток електронних інструментів для залучення фізичних та юридичних осіб (інструментів електронної участі) вимагає створення єдиної системи електронного офісу (е-офісу). Це дозволить працівникам органів публічної влади здійснювати моніторинг учасників електронних обговорень в Інтернеті шляхом ідентифікації IP-адрес їх автоматизованих робочих місць. Таким чином, можна буде налагодити контакт з представниками як прибуткових організацій (приватних підприємств), отримуючи від них необхідну інформацію про спектр послуг, так і з неприбутковими організаціями (громадськими об'єднаннями), які мають повноваження здійснювати громадський контроль за діяльністю органів публічної влади щодо регулювання роботи відповідних підприємств, що надають різні види послуг. У такому випадку державі слід забезпечити максимальну інвестиційну підтримку розвитку громадських організацій, а також розробити програми підвищення кваліфікації. Це дозволить публічним службовцям здобути навички, необхідні для їх самореалізації як осіб, які в першу чергу відповідають за рівень життя суспільства, а не за рейтинг самих установ.

Розвиток електронної ідентифікації та довірчих послуг повинен включати впровадження системи, відомої як «електронна особа» (е-особа). Ця система міститиме інформацію про особу (товар або послугу, яку вона пропонує), на основі якої під час реєстрації особи (товару або послуги) буде проводитися перехресна перевірка документів, зафіксованих у базах даних різних підприємств, установ та організацій, де відповідна особа їх отримувала. Ця перевірка засвідчує (аутентифікує) право особи на ведення діяльності, що стосується продажу товарів або надання послуг в електронному форматі, при цьому товар або послуга ідентифікується сертифікатом якості, який підтверджує право інтелектуальної власності [51, с. 153].

Важливим аспектом є рівень зносу основних засобів приватних підприємств, особливо тих, що займаються інноваційною діяльністю, оскільки ефективність проведення відповідних перевірок залежить від якості комп'ютерного обладнання. Таким чином, державна інвестиційна підтримка

інноваційно активних установ є надзвичайно важливою. Крім того, розробка спеціальних програм підвищення кваліфікації дозволить компетентним публічним службовцям оволодіти технологіями ідентифікації, автентифікації та реєстрації фізичних і/або юридичних осіб, а також товарів і/або послуг, які вони пропонують.

Коли мова йде про розвиток електронної взаємодії, важливо насамперед звернути увагу на електронний портал (е-портал) установи. Він може бути представленим як Інтернет-портал, що надає інформацію у відкритому доступі, або як Інтранет-портал, доступ до якого можливий лише через вхід у особистий кабінет, що вимагає накладення ЕЦП на фізичну чи юридичну особу під час реєстрації.

Крім того, портал органу публічної влади може одночасно містити відкриті дані та особистий кабінет. У такому випадку проводиться системний аналіз IP-адрес користувачів, які найчастіше звертаються до публічної інформації, розміщеної на сайті органу. Також аналізуються дані зареєстрованих осіб, які користуються особистим кабінетом на відповідному сайті, де важливу роль відіграє дизайн сайтів приватних підприємств. Це може слугувати доказом наявності або відсутності у підприємства певної інформації, зокрема щодо мети його діяльності [51, с. 153].

Іншими словами, це підтверджує, наскільки можна довіряти інформації, розміщеній на сайті підприємства, яке можна ідентифікувати за IP-адресою, а також інформації, яку воно запитує через електронний кабінет. У цьому контексті державна інвестиційна підтримка розробників інформаційних мереж створює основу для електронної взаємодії. Водночас розробка програм підвищення кваліфікації, які навчають публічних службовців проявляти ініціативу в командній роботі, є важливим чинником для підтримки процесу електронної взаємодії між учасниками електронного уряду.

Уявити ефективний розвиток СЕДО без ЕА в органах публічної влади неможливо. Саме в ЕА зберігаються всі документи в електронному форматі. Кожен документ, який пройшов етапи отримання, обробки, виконання та

пересилання адресатові, може бути необхідний працівнику органу публічної влади для подальшої діяльності, і він захищений ЕЦП. Цей підпис накладається канцелярією органу на основі зв'язку з Акредитованим центром сертифікації ключів (АЦСК), який гарантує захист інформаційної цілісності документа та безпеку передачі службової інформації іншим учасникам електронного уряду через СЕДО. У цьому контексті для встановлення партнерських відносин важливим є такий вид співпраці з приватним сектором. Завдяки СЕДО органи публічної влади зможуть отримувати від приватних підприємств необхідну інформацію в документах, яка буде офіційно підтверджена за допомогою ЕЦП. Однак, для отримання доступу до цієї системи підприємство повинно бути зареєстроване в Єдиному державному реєстрі підприємств та організацій України, що дозволяє підтвердити його статус юридичної особи за відповідним номером. Це, у свою чергу, сприяє розвитку приватного сектору, де державна інвестиційна підтримка, пов'язана з фінансуванням будівництва та реконструкції приватних підприємств, відіграє значну роль. Окрім того, розробка програм підвищення кваліфікації, які надають публічним службовцям знання про спеціальні закони, що стосуються реєстрації фізичних та юридичних осіб, сприятиме більш ефективному регулюванню державою будь-якої сфери діяльності, в якій залучений приватний сектор [51, с. 154].

Врешті-решт, для успішної роботи галузевих структурних підрозділів органів публічної влади необхідна співпраця з приватним сектором, представники якого виробляють продукцію, що потрібна державному сектору. Система електронного партнерства (е-партнер) надає можливість аналізувати кількість робочих місць, на кожному з яких повинна бути встановлена персоніфікована система даних про працівника органу публічної влади. Ця система розпізнає працівника під час його роботи в інформаційно-телекомунікаційній системі на робочому місці. Завдяки цьому керівництво органу може робити висновки щодо своєчасності початку та завершення роботи, а також оцінювати якість виконання завдань працівником. Усе це

формує єдину інформаційно-телекомунікаційну інфраструктуру, яка об’єднує телекомунікаційні мережі, загальні та спеціалізовані електронні системи, а також різноманітне програмне забезпечення, що дозволяє суб’єктам електронного уряду підтримувати постійний зв’язок між собою.

Однак, для створення необхідних технічних можливостей потрібно, по-перше, мати кваліфікований персонал у виробничих компаніях, де важливу роль відіграє державна інвестиційна підтримка; по-друге, регулярно проводити публічні закупівлі через систему електронних тендерів, де здійснюється факторний аналіз цін та функціональних можливостей технічних засобів або їх комплектуючих, запропонованих виробниками. Ці фактори в значній мірі залежать від кількості основних засобів, які завдяки державній інвестиційній підтримці надають відповідним компаніям можливість проводити якісні науково-дослідні та дослідно-конструкторські роботи для подальшого обслуговування інших учасників електронного уряду. У такому випадку виникає система електронного уряду (е-уряду), яка надає можливість кожній групі суб’єктів аналізувати якість роботи структурних підрозділів органів публічної влади. Це, в свою чергу, значною мірою впливає на обсяг прибутку, отриманого приватним сектором від інвестиційної діяльності, який може бути використаний для розвитку пріоритетних галузей економіки, залежно від обсягу інвестицій, здійснених державою.

У такому випадку розробка спеціальних програм підвищення кваліфікації, які дозволять публічним службовцям здобути знання з державного управління, зокрема в аспекті взаємодії між працівниками апарату та відокремленими структурними підрозділами органів публічної влади, стане поштовхом для створення програм, що, по-перше, нададуть публічним службовцям компетенції у використанні загальних та спеціалізованих електронних систем; по-друге, забезпечать їх знаннями з економіки для проведення якісного аналізу роботи структурних підрозділів, відповідальних за різні сфери економічної діяльності. Це дозволить публічним службовцям виявляти найменш ефективні галузі, розробляти прогнозні показники та

розраховувати обсяги бюджетних коштів, необхідних для інвестування в найбільш затребувані суспільством інноваційні проекти [51, с. 154].

Підсумовуючи, варто зазначити, що затверджена урядом Концепція розвитку електронного урядування має на меті реформувати публічну службу шляхом створення повноцінної системи електронного уряду. Ця система забезпечить суб'єктам інформаційної взаємодії, зокрема громадянам, більше можливостей для участі в обговоренні питань, що стосуються економічного та соціального розвитку їхніх регіонів, а також здійснення громадського контролю за діяльністю Уряду. Це, у свою чергу, сприятиме переходу країни до децентралізованої системи управління, що забезпечить тісну взаємодію між органами державної влади та місцевого самоврядування. Концепція також має на меті відновлення довіри суспільства до уряду, для чого Кабінет Міністрів України затвердив план заходів щодо її реалізації, що передбачає поступове вдосконалення роботи органів публічної влади через впровадження ІКТ. Проте для цього уряд повинен змінити своє ставлення до реалізації кожного пункту плану, орієнтуючись на сталий розвиток суспільства, а не на показову діяльність, що має на меті штучно підвищити довіру з боку громадськості.

Отже, для вирішення зазначеного питання урядові варто поступово вдосконалювати виконання плану заходів, пов'язаних із запобіганням корупції в органах публічної влади, забезпеченням інформаційної безпеки держави, підвищенням довіри до приватних підприємств, збільшенням обсягу бюджетних інвестицій у розвиток прибуткових і неприбуткових організацій, а також підвищенням кваліфікації персоналу в органах публічної влади.

3.2. Недоліки й прогалини у безпечному функціонуванні систем електронного урядування та шляхи їх усунення

Незважаючи на значний прогрес у формуванні нормативно-правової бази для електронного урядування в Україні, існує безліч проблемних аспектів, які потребують вирішення.

Система державної влади в нашій країні не відповідає потребам України, яка прагне до комплексного реформування в різних сферах державної політики, а також європейським стандартам управління. Україна займає низькі позиції у світових рейтингах конкурентоспроможності, пов’язаних із державним управлінням.

У сучасному світовому суспільстві можна виділити спільні проблеми, які стосуються багатьох країн, серед яких є брак довіри громадян до влади і навпаки. Електронне урядування покликане вирішити цю проблему, і його впровадження в Україні останнім часом набирає швидких обертів. Довіра зміцнює владу, надаючи їй легітимність, а також покращує бізнесові перспективи на державному рівні та залучає більше іноземних інвесторів.

Це пояснюється тим, що глобальна мережа електронного управління державою відкриває реальні можливості для стабільної інтерактивної взаємодії між усіма гілками державної влади та населенням. Громадяни не лише отримують доступ до публічної інформації про діяльність уряду, його проєкти та результати, але й уряд має додатковий інформаційний канал, через який громадяни добровільно надають дані для покращення державного управління.

Суть електронного урядування полягає не лише в модернізації системи державного управління та її адаптації до вимог інформаційного суспільства, а, насамперед, у забезпеченні взаємодії громадян з владою за допомогою сучасних ІКТ. Таким чином, ключовим елементом електронного урядування є електронна демократія, основною метою якої є задоволення потреб громадян

та підвищення рівня суспільних цінностей. Це має бути досягнуто шляхом використання переваг інформаційного суспільства, а також шляхом боротьби з негативними явищами, такими як корупція та бюрократія. Крім того, важливо формалізувати сучасний управлінський процес і надавати послуги громадянам відповідно до їхніх потреб [18, с. 97].

Організація економічного співробітництва та розвитку окреслила ключові критерії для створення електронного урядування, які залишаються актуальними в Україні й сьогодні: значення законодавства; прозорість, відповідальність та доброчесність; ефективність; узгодженість; адаптивність; легітимність; партнерство та консультації.

В Україні наразі триває активний етап розвитку електронного урядування. Це, в першу чергу, стосується електронного уряду: впроваджуються більш досконалі СЕДО з використанням ЕЦП в усіх сферах суспільного життя. Послуги надаються фізичним та юридичним особам через ЦНАП, системи «єдиного вікна» та інші. Адміністративна реформа, що була реалізована в Україні, сприяла активізації та оновленню цих процесів. Електронне урядування швидко розвивається в різних сферах, зокрема в електронній медицині (важливою складовою якої є телемедицина), електронній освіті (передусім дистанційній освіті), електронній комерції, електронному банкінгу, транспортній сфері, податковій службі, судах, митниці, правоохоронних органах тощо [18, с. 97].

Однак, з прискоренням розвитку електронного урядування та розширенням його застосування, зростає й обговорення відповідальності, яка лягає на кожного, хто залучений до цих процесів.

Не було проведено всебічної та глибокої оцінки стану системи державного управління в Україні. Серед численних проблемних аспектів цієї системи слід виділити такі:

- незадовільна якість електронних послуг, що надаються громадянам та юридичним особам;
- низький рівень ефективності базових електронних реєстрів;

- відсутність адекватних технічних рішень для забезпечення функціональної сумісності різних систем органів державної влади.

На нашу думку, усі проблеми електронного урядування доцільно систематизувати за основними тематичними блоками:

Блок 1. Фахове забезпечення. В Україні існує потреба в спеціалізованих фахівцях, які займаються реформуванням різних галузей і сфер. Зокрема, необхідні кваліфіковані лідери в системі державної служби, здатні здійснити національні реформи та забезпечити потрібні зміни. Для підвищення ефективності роботи державних органів важливо залучити велику кількість експертів з питань реформ, які можуть впроваджувати нові підходи в діяльності цих органів.

Основним завданням реформування є формування в кожному органі виконавчої влади, міністерствах та центральних органах виконавчої влади спеціалізованих груп, які займатимуться питаннями реформ. Ці групи повинні регулярно забезпечувати ефективну та послідовну реалізацію змін. До складу таких груп мають входити керівники всіх рівнів, фахівці та менеджери різних категорій, які володіють практичним досвідом впровадження новітніх реформ.

Потрібні висококваліфіковані та компетентні фахівці з питань реформ, які здатні забезпечити реалізацію пріоритетних напрямків реформування та підготувати процес формування, аналізуючи політику ключових галузей. Такі посади фахівців з питань реформ будуть включені до складу реформованої структури центральних органів виконавчої влади відповідно до нових завдань і функцій, що виникнуть внаслідок реорганізації. Для спеціалістів у сфері реформування мають бути визначені спеціальні посади з нормативно закріпленими посадовими окладами та особливими умовами праці.

Блок 2. Сумісність. Електронне урядування в різних сферах суспільного життя впроваджувалося в різні періоди, що призвело до використання різноманітних інформаційних технологій, які часто виявляються несумісними. Як наслідок, існує відсутність єдиної інформаційної системи та узгодженої бази даних. Технології електронного урядування, які використовують органи

державної влади та місцевого самоврядування, повинні бути, якщо не ідентичними, то принаймні однотипними. Це забезпечить ефективну комунікацію між різними органами державної влади. На сьогоднішній день, у Європейському Союзі вирішення цієї проблеми є пріоритетним завданням.

Блок 3. Національна безпека та національна самобутність. Прозорість та відкритість діяльності органів державної влади та місцевого самоврядування впливають на рівень захищеності держави від зовнішніх і внутрішніх загроз у інформаційній сфері. Використання СЕДО та їх інтеграція з іншими системами значно підвищують ризики зловживання цією інформацією, що може зашкодити суверенітету та незалежності нашої країни. Правоохоронні органи звертають увагу на різні форми кіберзлочинності, зокрема, на хакерські атаки на сайти державних установ і органів місцевого самоврядування, шпигунські віруси, які здатні зчитувати та передавати інформацію зацікавленим особам з інших країн, а також на ведення інформаційних війн за допомогою сучасних ІКТ [18, с. 97-98].

Проблема національної самобутності полягає в спробі створити технічну основу для впровадження системи електронного урядування, використовуючи розробки іноземних фахівців. При цьому ці розробки спрощуються, не враховуючи специфічні напрямки діяльності органів державної влади в Україні, що може призвести до негативних наслідків, зокрема до втрати національної самобутності.

Блок 4. Економічна безпека. Захист приватної інформації та електронних звітів українських компаній (підприємств, установ, організацій) залишається на досить низькому рівні в умовах загрози з боку недобросовісних конкурентів.

Блок 5. Політика конфіденційності (приватності). Особливу увагу під час дослідження слід звернути на політику конфіденційності. Формування державних баз даних без чіткого визначення умов доступу до цієї інформації може призвести до втрати даних або їх неправомірного розголошення, що, у свою чергу, може викликати зниження довіри з боку громадян.

Законодавець у Законі України «Про захист персональних даних» визначив, що регулюються правові відносини, пов’язані із захистом та обробкою персональних даних. Цей закон спрямований на забезпечення основоположних прав і свобод людини та громадянина, зокрема права на недоторканність особистого життя в контексті обробки персональних даних. Крім того, дія Закону поширюється на обробку персональних даних, яка виконується повністю або частково за допомогою автоматизованих засобів, а також на обробку персональних даних, що містяться в картотеці або призначені для внесення до картотеки, із використанням неавтоматизованих засобів [41].

Блок 6. Відповідальність. Проблема різних видів юридичної відповідальності стає дедалі актуальнішою в умовах сучасного державотворення. Багато працівників органів державної влади, місцевого самоврядування та сфери обслуговування не несуть відповідальності за надання доступу зацікавленим особам до інформації про персональні дані інших громадян. Яскравим прикладом цього є фальсифікації, що відбуваються під час виборів або рекламних кампаній різних установ і компаній.

Блок 7. Непередбачувані обставини. Зберігання всіх документів в електронному вигляді без резервних копій, а також перехід на дистанційне навчання з використанням сучасних ІКТ у різних сферах знань під час виникнення непередбачуваних обставин може призвести до їх втрати. Якщо розглядати цю ситуацію в межах країни, це може призвести до повного колапсу.

На сьогоднішній день, коли система надання державних послуг лише частково функціонує в електронному форматі, технічні збої, такі як відключення електрики, «зависання» СЕДО, електронної черги, е-реєстрації тощо, можуть призвести до паралічу роботи цих органів. Тому, при переході на 100% електронний режим надання найважливіших послуг для громадян, захист національної безпеки та безпеки життєдіяльності має бути забезпечений на найвищому рівні. Деякі науковці вважають, що оптимальним

співвідношенням має бути 70-80% електронного режиму, залежно від важливості послуг, а решта – в традиційному форматі [18, с. 98].

Підсумовуючи викладене, можна зазначити, що в Україні останнім часом активно реалізується система електронного урядування, яка має на меті підвищення прозорості державних інститутів і, відповідно, зміцнення довіри населення до всіх гілок влади. Для досягнення максимальної ефективності від впровадження електронного урядування важливо врахувати та мінімізувати ризики, пов'язані з цим процесом. З цією метою вважаємо за необхідне встановити активний діалог між владою та громадянами, що сприятиме подальшому розвитку електронної демократії, а також координації зусиль державних органів і місцевого самоврядування для вироблення механізмів вирішення виявлених проблем і запобігання їх виникненню в майбутньому.

З огляду на надану вище інформацію про впровадження системи електронного урядування в Україні, слід зазначити, що існує безліч недоліків, які потребують термінового усунення.

Однак сама система має величезний потенціал і може принести багато позитивних результатів після її належного впровадження та забезпечення всім необхідним для ефективного функціонування.

Безсумнівно, для ефективного впровадження електронного урядування потрібно пройти складний шлях адаптації системи державного управління до європейських стандартів, зберігаючи при цьому українську самобутність та враховуючи особливості діяльності і менталітет українського народу. Тому спробуємо виділити основні перспективні напрямки розвитку системи електронного урядування в Україні.

Напрям 1. Розробити та впровадити найкращі стандарти електронного урядування та інноваційних практик, що сприятимуть підвищенню якості послуг і доступу громадян до публічної інформації про діяльність органів державної влади та місцевого самоврядування. Стандарти електронного урядування мають бути підтримані створенням технічної інфраструктури та її регулярним оновленням відповідно до потреб електронного урядування.

Впровадження державних програм для розвитку ІКТ у державній службі та навчальних курсів з електронного урядування, а також популяризація нових комунікаційних каналів між представниками органів державної влади та громадянами.

Напрям 2. Важливо забезпечити підтримку інклюзивного діалогу для розробки політики електронного урядування та електронної демократії, що враховує інтереси та потреби регіонів України.

Напрям 3. Активне підвищення прозорості та підзвітності державних органів шляхом впровадження сучасних ІКТ.

Напрям 4. Постійне вдосконалення механізмів електронного урядування та електронної демократії з урахуванням потреб центральних органів державної влади та регіонів України. Впровадження ЕДО в органах державної влади та місцевого самоврядування, а також розширення практики використання ЕЦП. При цьому необхідно забезпечити інформаційну безпеку під час роботи з ЕД.

Напрям 5. Посилення ролі громадянського суспільства у захисті прав і свобод громадян, активізація та розвиток електронної демократії з метою забезпечення більшої участі громадян у процесах прийняття рішень на місцевому та регіональному рівнях. Також передбачено регулярне інформування громадян про стан справ у державі через електронні комунікаційні канали. Громадяни України повинні мати вільний доступ до відкритої державної інформації про діяльність органів державної влади та місцевого самоврядування.

Напрям 6. Зменшення рівня корупційних ризиків в Україні та підвищення довіри громадян до інститутів публічної влади.

У світовій спільноті електронне урядування стало постійним явищем, до якого європейці звикли і в ефективності якого переконалися. Щоб українські громадяни почали довіряти електронному урядуванню, необхідно продемонструвати його ефективність та повну відсутність корупції. Це можна досягти, дотримуючись принципів прозорості і відкритості в електронному

урядуванні.

Напрям 7. Збільшення активності громадян у законодавчій та правотворчій ініціативі. Ці поняття вже мають досвід у світовій практиці, і їх різноманітні моделі реалізовані в таких провідних країнах, як Австрія, Данія, Італія, Сполучені Штати Америки, Швеція, Швейцарія та інших.

Громадяни повинні мати можливість брати участь у розробці законодавчих актів та підзаконних нормативно-правових документів під час громадських обговорень законопроєктів, проєктів рішень і постанов, що стосуються нормативно-правових актів міністерств та органів місцевого самоврядування. Вони можуть долучатися до громадських слухань, що стосуються прийняття та внесення змін до проєктів містобудівної документації, а також через місцеві ініціативи, в рамках яких може бути ухвалено рішення, запропоноване ініціативною групою тощо.

Отже, можна зробити висновок, що для досягнення максимальної ефективності від впровадження електронного урядування необхідно мінімізувати ризики, пов’язані з його реалізацією. Для цього важливо встановити активний діалог між владою та громадянами, що сприятиме подальшому розвитку електронної демократії, а також координувати зусилля органів державної влади та місцевого самоврядування для розробки механізмів вирішення існуючих проблем і запобігання їх виникненню в майбутньому.

Висновки до Розділу 3

Наша країна ще не змогла повністю впровадити національну систему ЕДО та електронного діловодства через відсутність стандартів і нормативних актів, організаційні труднощі, а також проблеми з безпекою та захистом інформації.

Покращення якості публічного управління здійснюється, з одного боку, через впровадження нових ІКТ, які сприяють виконанню функцій органів публічної влади, а з іншого боку, через трансформацію та оптимізацію самих функцій, а також розвиток нових можливостей для більш ефективного задоволення потреб споживачів державних послуг. Технологічні та функціональні аспекти підвищення якості публічного управління підтримуються державою, яка сприяє розвитку зовнішнього середовища для органів публічної влади, зокрема інформаційного суспільства та нової економіки.

ВИСНОВКИ

У кваліфікаційній роботі досліджено безпекові питання функціонування системи електронного документообігу в сфері публічного управління в умовах воєнного стану. Отриманні результати у процесі дослідження дають змогу сформулювати такі висновки і пропозиції:

1. ЕДО є комплекс процесів, що охоплює створення, обробку, відправлення, передачу, отримання, зберігання, використання та знищення електронних документів.

Наразі можна з упевненістю говорити про широке впровадження технології ЕДО, яка об’єднує користувачів у єдиній мережі та забезпечує швидкий і зручний обмін документами відповідно до єдиних оптимальних правил і регламентів. Що стосується України, то більшість документообігу в публічно-владних установах все ще відбувається в паперовому форматі. Однак, сучасний стан автоматизованого діловодства та документообігу в органах влади створює сприятливі технологічні умови для подальшого розвитку ЕДО та наближення його до стандартів країн ЄС.

В нашій державі нормативне забезпечення функціонування СЕДО в сфері публічного управління представлене значною кількістю законодавчих та підзаконних актів. Проте воно має ряд недоліків, таких як неповнота, декларативність, відсутність системності, нечіткість, недостатня узгодженість документів та невідповідність міжнародним стандартам, зокрема, європейським. Крім того, існує проблема втрати актуальності, що суттєво стримує розвиток цієї сфери і є однією з основних причин, чому Україна втрачає свої позиції в міжнародних рейтингах розвитку інформаційного суспільства та електронного урядування.

2. Сьогодні на українському ринку програмного забезпечення активно представлені системи, що автоматизують діловодство, документообіг та інші адміністративні процеси в органах публічної влади. Всі їх умовно

можна поділити на внутрішні та зовнішні. Перші, котрі іноді називають корпоративними, охоплюють процес обігу документів всередині організації між різними підрозділами і працівниками. Натомість, інші – являють собою процес переміщення документів поза межами організації, що включає обмін документами з різними суб'єктами публічно-правових відносин. Зазвичай зовнішній документообіг охоплює узгодження рахунків, актів виконаних робіт, звітів, накладних тощо. Використання такого ЕДО дозволяє миттєво передавати документи контрагентам, заощаджуючи час і кошти на друк та доставку. Крім того, ЕДО підвищує рівень захисту документів.

Функції, які пропонують сучасні СЕДО, здатні суттєво підвищити ефективність управлінської діяльності. Це такі функції як: зберігання та пошук документів, підтримка канцелярської роботи, маршрутизація та контроль за виконанням документів, підготовка аналітичних звітів, забезпечення інформаційної безпеки, а також ряд інших додаткових (специфічних) функцій.

3. Загрози інформаційній безпеці становлять виклики, що виходять за межі нашої країни і впливають не лише на національний простір, але й мають серйозні глобальні наслідки. Для запобігання та протидії цим загрозам необхідно: розробити надійну нормативно-правову базу, забезпечити ефективне функціонування інститутів публічного управління в сфері захисту національних інтересів інформаційної сфери, а також активно протидіяти інформаційній агресії, використовуючи досвід міжнародних країн й організацій у впровадженні подібних систем, зокрема в аспектах основних принципів, підходів та методів створення корпоративних інформаційних структур. Адже, як показує сучасна реальність, у війні в інформаційному просторі немає кордонів.

4. Більшість проблем розвитку СЕДО в сфері публічного управління можна вирішити в органах публічного управління шляхом ефективного впровадження та використання ЕДО. Це передбачає навчання посадових осіб, застосування більш потужного обладнання, вдосконаленого програмного і технічного забезпечення, запобігання корупції в органах влади тощо. Однак,

питання юридичного підтвердження електронних облікових документів може бути вирішене лише за умови наявності відповідної законодавчої бази.

5. Україна ще не повністю реалізувала свою національну систему ЕДО та електронного діловодства через брак стандартів і нормативних актів, організаційні труднощі, а також проблеми з безпекою і захистом інформації. Однак, для подальшого розвитку електронного діловодства в нашій державі варто звернути увагу на такі напрямки, як: створення правової основи та національної СЕДО, розвиток електронної ідентифікації, забезпечення криптографічного захисту даних та інших технологій, що гарантують безпеку ЕД. На нашу думку, з активним розвитком інноваційних технологій середовище кіберпростору стає все більш вразливим до потенційних загроз. Тому методи боротьби та засоби захисту від кіберзлочинів потребують постійного удосконалення. Крім того, важливо організувати надійне зберігання та архівування ЕД, а також навчити публічних службовців і громадян користуватися ЕДО та електронними сервісами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Автоматизована система контролю і організації діловодства «АСКОД» [Електронний ресурс]. Режим доступу: http://www.scritub.com/limba/ucraineana/72294.php.

2. Бабаєв В.М., Новікова М.М., Гайдученко С.О. Текст лекцій з дисципліни «Електронне урядування» (для студентів 5 курсу спеціальності 8.03060101 «Менеджмент організацій і адміністрування» денної форми навчання). Х.: ХНУМГ, 2014. 127 с.

3. Бурячок В.Л., Киричок Р.В., Складанний П.М. Основи інформаційної та кібернетичної безпеки: Навч. посіб. К., 2018. 320 с.

4. Всесвітній саміт з питань інформаційного суспільства (Женева 2003 – Туніс 2005): підсумкові документи [Електронний ресурс]. Режим доступу: https://old.apitu.org.ua/wsis/dp#2.

5. Деякі питання документування управлінської діяльності: Постанова Кабінету Міністрів України від 17 січня 2018 р. № 55 [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/55-2018-%D0%BF#Text.

6. Директива 1999/93/ЕС Європейського Парламенту та Ради від 13 грудня 1999 року «Про систему електронних підписів, що застосовується в межах Співтовариства» від 13 грудня 199 р. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/994_240#Text.

7. Електронне урядування та електронна демократія: Навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. К., 2017. Частина 9: Електронний документообіг. Реінжиніринг адміністративних процесів в органах публічної влади / С.П. Кандзюба, Р.М. Матвійчук, Я.М. Сидорович, П.М. Мусієнко. К.: ФОП Москаленко О. М., 2017. 64 с.

8. Електронне урядування та електронна демократія: Навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. К., 2017. Частина 13: Захист

інформації в системах електронного урядування / за ред. О.М. Хошаба. К.: ФОП Москаленко О. М., 2017. 72 с.

9. Електронний документообіг (загальне діловодство) [Електронний ресурс]. Режим доступу: https://www.viaduk.com/viaduk/web5ua.nsf/0/ACC6E5C6C0A30BD9C225726F0051E265?OpenDocument&Highlight=0,%D0%B7%D0%B0%D0%B3%D0%B0%D0%BB%D1%8C%D0%BD%D0%B5.

10. Електронний документообіг та захист інформації: Навч. посіб. / за заг. ред. д. держ. упр., професора Н.В. Грицяка. К.: НАДУ, 2015. 84 с.

11. Інструкція АСКОД [Електронний ресурс]. Режим доступу: https://askod.online/instructions/index.html.

12. Клюцевський В.І. Використання сучасних цифрових технологій при наданні адміністративних послуг на регіональному рівні. Актуальні проблеми державного управління. 2018. Вип. 4(76). С. 47-51.

13. Коновал В.О. Рекомендації органам публічної влади місцевого рівня щодо розроблення і застосування організаційно-правових механізмів державного управління електронним урядуванням. Молодий вчений. 2018. № 10(50). С. 765-774.

14. Куспляк І.С., Серенок А.О. Сто міст – крок вперед. Моніторинг впровадження інструментів електронного урядування, як основи надання адміністративних послуг в електронному вигляді / за заг. ред. І.С. Куспляка. Вінниця: ГО «Подільська агенція регіонального розвитку», 2014. 86 с.

15. Лагутін В.Д., Ільїна А.О. Вплив держави на розвиток інноваційно-інвестиційних процесів в Україні. Формування ринкових відносин в Україні. 2013. № 3(142). С. 58-66.

16. Линьов К.О. Інформаційне забезпечення державного управління та державної служби: Навч. посіб. К., 2016. 42 с.

17. Ляшенко І.О. Європейські критерії безпеки інформаційних технологій. Сучасні інформаційні технології у сфері безпеки та оборони. 2012. № 1(13). С. 84-86.

18. Ніколіна І.І., Януш М.П. Особливості впровадження та

перспективи Mobile ID в Україні. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2019. № 34. С. 95-106.

19. Ніщименко О.А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17-23.

20. Новікова Н.Л., Науменко Р.А., Ільїна А.О. Маркери професійної компетентності державних службовців. Економіка України. 2018. № 9(682). С. 88-94.

21. Окінавська хартія глобального інформаційного суспільства від 22 липня 2000 р. [Електронний ресурс]. Режим доступу: https://ips.ligazakon.net/document/MU00269.

22. Орлова Н.С., Яровой Т.С. Сучасні принципи та методи державної політики у сфері інформаційної безпеки. Менеджер: Вісник Донецького державного університету управління. 2019. № 3 (84). С. 17-26.

23. Остапов С.Е., С.П. Євсеєв, Король О.Г. Технології захисту інформації: Навч. посіб. Х.: Вид. ХНЕУ, 2013. 476 с.

24. Перелік протестованих систем електронного документообігу [Електронний ресурс]. Режим доступу: https://se.diia.gov.ua/sedlist.

25. Прилипко Н.О. Вдосконалення системи електронного документообігу в органах державної влади. Збір. наукових праць Донецького державного університету управління. 2014. Т. 15. Вип. 286. С. 164-165.

26. Про електронний цифровий підпис: Закон України від 22 травня 2003 р. № 852-IV. Відомості Верховної Ради України. 2003. № 36. Ст. 276 (втратив чинність 5 жовтня 2017 р.).

27. Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 р. № 851-IV. Відомості Верховної Ради України. 2003. № 36. Ст. 275.

28. Про затвердження Державної стратегії регіонального розвитку на період до 2020 року: Постанова Кабінету Міністрів України від 6 серпня 2014 р. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/695-2020-%D0%BF#Text.

29. Про затвердження плану заходів з реалізації Концепції розвитку електронного урядування в Україні: Розпорядження Кабінету Міністрів України від 22 серпня 2018 р. № 617-р [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/617-2018-%D1%80#Text.

30. Про затвердження Положення про центральний засвідчувальний орган: Постанова Кабінету Міністрів України від 28 жовтня 2004 р. № 1451 [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1451-2004-%D0%BF#Text (втратила чинність 10 травня 2018 р.).

31. Про затвердження Порядку акредитації центру сертифікації ключів: Постанова Кабінету Міністрів України від 13 липня 2004 р. № 903 [Електронний ресурс]. Режим доступу: https://www.kmu.gov.ua/npas/7401792.

32. Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу: Постанова Кабінету Міністрів України від 26 травня 2004 р. № 680 [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/680-2004-%D0%BF#Text (втратила чинність 7 листопада 2018 р.).

33. Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності: Постанова Кабінету Міністрів України від 28 жовтня 2004 р. № 1452 [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1452-2004-%D0%BF#Text (втратила чинність 19 вересня 2018 р.).

34. Про затвердження Порядку зберігання електронних документів в архівних установах: Наказ Державного комітету архівів України від 25 квітня 2005 р. №49 [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/z0627-05#Text (втратив чинність 11 листопада 2014 р.).

35. Про затвердження Порядку обов’язкової передачі документованої інформації: Постанова Кабінету Міністрів України від 28 жовтня 2004 р. № 1454 [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/

show/1454-2004-%D0%BF#Text (втратила чинність 10 жовтня 2018 р.).

36. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text.

37. Про затвердження Правил організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях: наказ Міністерства юстиції України від 18 червня 2015 р. № 1000/5 [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/z0736-15#Text.

38. Про затвердження Примірної інструкції з діловодства у міністерствах, інших центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органів виконавчої влади: Постанова Кабінету Міністрів України від 17 жовтня 1997 р. № 1153 [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1173-2003-%D0%BF#Text (втратила чинність 30 листопада 2011 р.).

39. Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади: Постанова Кабінету Міністрів України від 28 жовтня 2004 р. № 1453 [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1453-2004-%D0%BF#Text (втратила чинність 17 січня 2018 р.).

40. Про захист інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 р. №80/94-ВР. Відомості Верховної Ради України. 1994. № 31. Ст. 286.

41. Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297-VI. Відомості Верховної Ради України. 2010. № 34. Ст. 481.

42. Про інформацію: Закону України від 2 жовтня 1992 р. № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Ст. 650.

43. Про рішення Ради національної безпеки і оборони України від

14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 № 447/2021 [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

44. Про Стратегію сталого розвитку «Україна–2020»: Указ Президента України від 12 січня 2015 р. № 5/2015 [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/5/2015#Text.

45. Про схвалення Концепції розвитку електронного урядування в Україні: Розпорядження Кабінету Міністрів України від 20 вересня 2017 р. № 649-р [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80.

46. Проноза І.І. Інформаційна безпека держави: сутність та основні визначення. Гілея: науковий вісник. 2017. Вип. 127. С. 345-348.

47. Риженко О.В. Стратегічні пріоритети сучасного розвитку електронного урядування в Україні. Ефективність державного управління. 2017. № 43. С. 99-103.

48. Семенченко А.І. Механізми державного управління у сфері електронного урядування. Студії з архівної справи та документознавства. 2017. Т. 20. С. 109-113.

49. Скиба М.В., Шелудько В.Я. Теоретичні аспекти дослідження розвитку громадянського суспільства. Державне управління: удосконалення та розвиток. 2019. № 2 [Електронний ресурс]. Режим доступу: http://www.dy.nayka.com.ua/pdf/2_2019/24.pdf.

50. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: Навч. посіб. / С.О. Іванченко, О.В. Гавриленко, О.А. Липський, А.С. Шевцов. К.: ІСЗЗІ НТУУ «КПІ», 2016. 104 с.

51. Торяник В.М. Інформаційна безпека як складова національної безпеки держави. роль ЗМІ в забезпеченні інформаційного суверенітету України. Право і суспільство. 2016. № 2. С. 151-156.

52. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і

їхніми державами-членами, з іншої сторони від 27 червня 2014 р. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/984_011#Text.

53. Чирський Ю.В. Електронний цифровий підпис: правові аспекти застосування. Довідник секретаря та офіс-менеджера. 2007. № 1. С. 31-38.

54. Шеверда В.А. Електронне урядування як спосіб підвищення ефективності системи державного управління. Менеджмент за умов трансформаційних інновацій: виклики, реформи, досягнення: матеріали міжнар. наук. конф. (м. Суми, 10-12 травня) 2017. Ч-2. С. 168-170.

55. Юлдашев О.В. Електронне урядування: проблеми та перспективи. Персонал. 2017. № 10. С. 42-46.

56. Gil-Garcia J.R. Enacting Electronic Government Success: An Integrative Study of Government-wide Websites, Organizational Capabilities, and Institutions. Springer, 2012. 251 p.

57. Panchenko V. Ilyina A., Mihus I., Vavrin M., Karpenko Yu. The role of investment strategy in the strategic management system of service companies. Academy of Strategic Management Journal. 2019. Volume 18. Special Issue 1. С. 3-7.

58. Suri P.K. Strategic Planning and Implementation of E-Governance. Springer, 2017. 292 p.

59. The European Network and Information Security Agency [Електронний ресурс]. Режим доступу: http://www.enisa.europa.eu/.

60. Trotta A. Advances of E-Governance: Theory and Application of Technological Initiatives. New York: Routledge, 2017. 206 p.

61. UN E-Government Knowledgebase. Ukraine [Електронний ресурс]. Режим доступу: https://publicadministration.un.org/egovkb/en-us/Data/CountryInformation/id/180-Ukraine.

62. United Nations. E-government. Survey 2024: accelerating digital transformation for sustainable development [Електронний ресурс]. Режим доступу:https://desapublications.un.org/sites/202024%201392024.pdf.

Додаток А

Шляхи покращення виконання плану дій щодо реалізації Концепції розвитку електронного урядування в Україні

№	Способи втілення плану дій щодо розвитку [29]	Шляхи покращення				
		Електронні системи протидії корупції в органах влади [58, с. 142].	Методи забезпечення інформаційної безпеки держави [22, с. 19]	Фактори, що впливають на рівень довіри держави до приватних підприємств [57, с. 4]	Державна інвестиційна підтримка через інвестиції [15, с. 62]	Результат підвищення кваліфікації працівників органів влади [20, с. 89].
1.	Електронні послуги	Е-сервіс	Перевірка стандарту / ліцензії	Час / ціна обслуговування	Промислові платформи	Відчуття відповідальності
2.	Відкриті дані	Е-код	Обробка документів	Потужність	Програмні продукти	Вибір рішення
3.	Інструменти е-участі	Е-офіс	Мережевий нагляд	Спектр послуг	Громадські об’єднання	Самореалізація
4.	Електронні ідентифікації	Е-особа	Перевірка свідоцтва / сертифіката	Знос основних засобів	Інноваційно-активні установи	Знання ІТ-програм
5.	Електронна взаємодія	Е-портал	Системний аналіз	Дизайн сайтів	Мережу Інтернет	Робота в команді
6.	Електронний документообіг	Е-архів	Накладення ЕЦП	ЄДРПОУ	Приватний сектор	Знання законів
7.	Галузевих структурних підрозділів	Е-бізнес	Кількісний аналіз	Кваліфікований персонал	Фірми-виробники	Знання з державного управління
8.	ІТІ	Е-тендер	Факторний аналіз	Основні засоби	НДДКР	Знання ІТ-систем
9.	Електронне урядування	Е-уряд	Якісний аналіз	Інвестиційний прибуток	Пріоритетні галузі	Знання з економіки