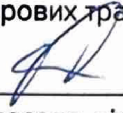


(гриф обмеження доступу
за наявності)

ЗАТВЕРДЖУЮ
Власник Підсистеми

Заступник Голови ДСА України
з питань цифрового розвитку,
цифрових трансформацій і цифровізації

 Леонід САПЕЛЬНИКОВ
(посада, підпис, ім'я, ПРІЗВИЩЕ)
«06» 08 2026 року

ТЕХНІЧНІ ВИМОГИ

НА СТВОРЕННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ – ЄДИНОГО ДЕРЖАВНОГО РЕЄСТРУ
ВИКОНАВЧИХ ДОКУМЕНТІВ ЄДИНОЇ СУДОВОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ
СИСТЕМИ

(вибрати мету, зазначити повну назву ІКС)

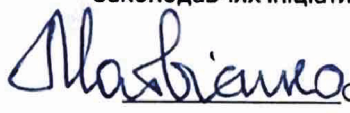
Шифр роботи: ЄСІКС – ЄДРВД
(шифр ІКС)

На 75 аркушах

ПОГОДЖЕНО

Розробник технічних вимог

Виконавча директорка ГО «Лабораторія
законодавчих ініціатив»

 Світлана МАТВІЄНКО
(посада, підпис, ім'я, ПРІЗВИЩЕ)
«06» серпня 2026 року

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ	5
1.1 Підстава для розроблення технічних вимог	5
1.2 Найменування засобу інформатизації	6
1.3 Мета створення засобу інформатизації	6
1.4 Терміни, що використовуються	6
1.5 Нормативно-правові документи	10
2. ПРИЗНАЧЕННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ	12
2.1 Основні завдання та функції засобу інформатизації	12
2.2 Очікувані результати від впровадження засобу інформатизації	12
2.3 Порядок розвитку засобу інформатизації	13
3. ХАРАКТЕРИСТИКИ ОБ'ЄКТА ІНФОРМАТИЗАЦІЇ	14
4. ВИМОГИ ДО ЗАСОБУ ІНФОРМАТИЗАЦІЇ	16
4.1 Вимоги до структури та функціонування засобу інформатизації	16
4.2 Вимоги до функцій, що виконуються засобом інформатизації	17
4.3 Основні бізнес-процеси	17
4.4 Опис користувачів Підсистеми та доступів	19
4.4.1 Ролі та права доступу	21
5. ФУНКЦІОНАЛЬНІ ВИМОГИ	25
5.1 Виконавчий документ	25
5.1.1 Створення виконавчого документа користувачем у вебінтерфейсі	27
5.1.2 Реєстрація виконавчого документа	27
5.1.3 Перегляд реєстраційної картки виконавчого документа	29
5.1.4 Перегляд виконавчих документів	29
5.1.5 Зміна процесуального статусу виконання виконавчого документа	29
5.1.6 Архівування виконавчого документа	31
5.1.7 Знищення виконавчого документа	32
5.1.8 Пошук виконавчого документа	32
5.2 Визнання виконавчого документа таким, що не підлягає виконанню	32
5.2.1 Реєстрація ухвали або рішення про визнання виконавчого документа таким, що не підлягає виконанню	32
5.2.2 Перегляд ухвали або рішення про визнання виконавчого документа таким, що не підлягає виконанню	33
5.3 Виправлення помилки у виконавчому документі	33
5.3.1 Реєстрація документа про виправлення помилки у виконавчому документі	33
5.3.2 Перегляд документа про виправлення помилки у виконавчому документі	34
5.4 Пред'явлення виконавчого документа до виконання	34
5.4.1 Створення заяви про виконання рішення	34
5.4.4 Перегляд заяви про виконання рішення, заяви про повернення виконавчого документа та заяви про поновлення виконавчого провадження	35
5.4.5 Зміна статусу заяви на виконання рішення	36
5.5 Інтеграції	36
5.5.1 Внутрішні інтеграції	36

5.5.1.1 Керування доступом (Управління ідентифікацією та доступом (IAM))	37
5.5.1.2 Єдиний персональний простір користувача	38
5.5.1.3 Функціональні компоненти для роботи з документами (Документ-сервіс)	39
5.5.1.4 Підсистеми електронного документообігу суду	40
5.5.1.5 Довідники і класифікатори	41
5.5.1.6 Майстер-реєстри	41
5.5.1.7 Оркестрація (BPMS)	42
5.5.1.8 Нотифікації користувачів	43
5.5.1.9 Підписання документів (Крипто-сервіс)	44
5.5.1.10 Довідка та рекомендації. База знань	44
5.5.1.11 Аналіз та звітність	45
5.5.1.12 Платежі	46
5.5.1.13 Пошук і фільтри	46
5.5.1.14 Логування	47
5.5.1.15 Моніторинг	48
5.5.1.16 Архів документів	48
5.5.1.17 Конструктор відкритих даних	49
5.5.1.18 Виявлення сутностей та тегування	49
5.5.1.19 Сервіс-деск	50
5.5.1.20 Календарі та завдання	50
5.5.1.21 Електронна взаємодія	51
5.5.2 Зовнішні інтеграції	51
6. НЕФУНКЦІОНАЛЬНІ ВИМОГИ	52
6.1 Вимоги до чисельності та кваліфікації персоналу, залученого до експлуатації та супроводу Підсистеми	52
6.2 Вимоги до безпеки	53
6.3 Вимоги до ергономіки та технічної естетики	54
6.4 Вимоги до захисту інформації	55
6.5 Вимоги до уніфікації	56
6.6 Вимоги до надійності засобу інформатизації та збереженості інформації	56
6.7 Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації	58
6.8 Вимоги до режимів функціонування засобу інформатизації	58
6.9 Вимоги щодо придатності системи до розвитку та модернізації	58
6.10 Вимоги до лінгвістичного забезпечення	59
6.11 Вимоги до потужності Підсистеми	59
6.12 Вимоги до умов ліцензування та використання стороннього ПЗ	60
6.13 Вимоги до розробки	61
6.14 Вимоги до міграції даних	62
7. ТЕХНОЛОГІЧНИЙ СТЕК	63
7.1 Мови програмування, Фреймворки та бібліотеки	63
7.2 Бази даних	64
7.3 Інструменти інтеграції та API	64

7.4. Контейнеризація та оркестрація	64
7.4.1 Загальний опис	64
7.4.2 Основні функціональні вимоги	65
7.5 Вебсервер та реверс-проксі	65
7.6 Вхідний мережевий шлюз	65
7.6.1 Загальний опис	65
7.6.2 Основні функціональні вимоги	66
7.6.3 Вимоги до інтеграції та використання	67
7.7 Кешування даних	67
7.7.1 Загальний опис	67
7.7.2 Основні функціональні вимоги	67
7.8 Брокер повідомлень	68
7.8.1 Загальний опис	68
7.8.2 Основні функціональні вимоги	68
7.8.3 Вимоги до надійності та продуктивності	68
7.8.4 Вимоги до інтеграції та безпеки	68
7.9 Індикатор	69
7.9.1 Загальний опис	69
7.9.2 Основні функціональні вимоги	69
7.9.3 Вимоги до інтеграції та використання	69
8. ВИМОГИ ДО СУПРОВОДУ ТА ОБСЛУГОВУВАННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ	71
8.1 Вимоги до гарантійної підтримки	71
8.2 Вимоги до навчання користувачів	71
8.3 Вимоги до документації	72
9. ВИМОГИ ДО ПРИЙМАННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ	73
9.1 Вимоги до проведення випробувань	74
9.1.1 Функціональне тестування	74
9.1.2 Інтеграційне тестування	74
9.1.3 Тестування на проникнення	74
9.1.4 Тестування під навантаженням	75
9.2 Вимоги до передачі результатів виконаних робіт	75
9.3 Вимоги до патентної чистоти	76
9.3.1 Вимоги до програмного забезпечення, яке розробляється Виконавцем	76

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1 Підстава для розроблення технічних вимог

Підставою для розроблення технічних вимог є необхідність створення Єдиного державного реєстру виконавчих документів як єдиного державного інформаційного ресурсу для централізованого обліку та доступу до виконавчих документів незалежно від органу, що їх видав, з метою забезпечення реалізації положень Закону України «Про виконавче провадження» від 02.06.2016 № 1404-VIII та з урахуванням змін, внесених Законом України «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів» від 03.10.2017 № 2147-VIII.

Стадія виконання рішень є завершальною та обов'язковою частиною реалізації судових та інших рішень уповноважених органів. Водночас на сьогодні процеси створення, обліку, передачі та використання виконавчих документів у межах цієї стадії здійснюються із застосуванням різних інформаційних систем, паперових носіїв та організаційних процедур. Така фрагментація призводить до розривів між судами, іншими державними органами та органами примусового виконання рішень, ускладнює контроль за рухом виконавчих документів, перевірку їх актуального процесуального стану та дотримання строків пред'явлення до виконання.

Відсутність єдиного державного електронного реєстру виконавчих документів унеможливорює формування повного та актуального масиву даних про виконавчі документи у масштабах держави, що негативно впливає на ефективність організації виконавчого провадження, створює додаткове навантаження на працівників судів, інших державних органів і органів виконання рішень, а також підвищує ризики помилок, пов'язаних із людським фактором.

Зазначені проблеми мають не лише внутрішньодержавний, а й міжнародний вимір. Практика Європейського суду з прав людини, зокрема у справах «Юрій Миколайович Іванов проти України» від 15 жовтня 2009 року, «Бурмич та інші проти України», підтверджує наявність системної проблеми невиконання або тривалого невиконання судових рішень в Україні.

У межах процесу підготовки України до повноправного членства в Європейському Союзі держава взяла на себе зобов'язання щодо реалізації реформ у сфері верховенства права, зокрема підвищення ефективності судової системи та забезпечення реального виконання рішень. Відповідні завдання визначені у Дорожній карті з питань верховенства права, схваленої розпорядженням Кабінету Міністрів України від 14 травня 2025 р. № 475-р, яка є складовою переговорної рамки України з ЄС у межах Кластера 1 «Основи процесу вступу до ЄС» та передбачає впровадження сучасних, прозорих і контрольованих механізмів реалізації рішень відповідно до стандартів Європейського Союзу.

У цьому контексті створення Єдиного державного реєстру виконавчих документів є необхідною системною відповіддю держави на наявні виклики та міжнародні зобов'язання. Реалізація Єдиного державного реєстру виконавчих документів відповідає положенням Концепції Єдиної судової інформаційно-комунікаційної системи та забезпечує формування архітектурно узгодженого рішення для централізованого обліку виконавчих документів і автоматизації процесів їх проходження на стадії виконання рішень.

Розроблення технічних вимог до створення Єдиного державного реєстру виконавчих документів як підсистеми Єдиної судової інформаційно-комунікаційної системи

є необхідною передумовою для впровадження уніфікованого, прозорого та контрольованого підходу до роботи з виконавчими документами.

1.2 Найменування засобу інформатизації

Повне найменування підсистеми: Єдиний державний реєстр виконавчих документів

Скорочена назва: ЄДРВД

Вживання термінів «Підсистема» та ЄДРВД є тотожними.

1.3 Мета створення засобу інформатизації

Метою створення ЄДРВД як засобу інформатизації є забезпечення функціонування автоматизованої системи, що у складі Єдиної судової інформаційно-комунікаційної системи забезпечує створення, внесення, збирання, зберігання, захист, облік, пошук та перегляд електронних виконавчих документів, а також надання інформації щодо стану їх виконання відповідно до вимог законодавства.

Створення ЄДРВД спрямоване на формування єдиного інформаційного середовища обігу виконавчих документів, забезпечення їх простежуваності від моменту створення до завершення виконання або припинення відповідних процедур, а також на підтримку інформаційної взаємодії з іншими підсистемами ЄСІКС та зовнішніми інформаційно-комунікаційними системами.

Реалізація засобу інформатизації має забезпечити підвищення прозорості обігу виконавчих документів, своєчасність їх пред'явлення до виконання, зменшення ризиків втрати або дублювання інформації, а також створення передумов для формування достовірної аналітичної та статистичної інформації у межах Єдиної судової інформаційно-комунікаційної системи.

1.4 Терміни, що використовуються

Терміни та скорочення, що використовуються в документі:

Термін	Значення
Автентифікація	Електронна процедура, яка дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-комунікаційної системи та/або походження та цілісність електронних даних
Авторизація	Частина процедури визначення та надання прав доступу до функцій та/або інформаційних ресурсів для роботи в інформаційній системі, після автентифікації
Адміністратор Підсистеми	Юридична особа публічного права, що забезпечує функціонування та здійснює адміністрування публічного електронного реєстру, визначена законом або іншим нормативно-правовим актом, згідно з яким створено публічний електронний реєстр
АСВП	Автоматизована система виконавчого провадження
Бізнес–процес	Сукупність взаємопов'язаних дій або операцій, спрямованих на досягнення визначеного результату

Валідація	Встановлення об'єктивних і задокументованих доказів того, що вимоги для конкретного передбаченого застосування або використання виконані
Виконавчий документ, ВД	Електронний документ, що відповідає вимогам до виконавчого документа, визначеним Законом України «Про виконавче провадження», на який накладається кваліфікований електронний підпис особи, яка має повноваження відповідно до закону на його видання, та є оригіналом виконавчого документа
Верифікація	Комплекс заходів з порівняння, встановлення відповідності та підтвердження відомостей, що містяться в інформаційних системах, з відомостями, що містяться в тих самих або інших системах або інших державних інформаційних ресурсах, а також відомостями, одержаними, зокрема шляхом електронної взаємодії, від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, які є володільцями та/або розпорядниками таких відомостей
Власник Підсистеми	Державна судова адміністрація України, яка є також держателем Підсистеми у розумінні Закону України «Про публічні електронні реєстри»
ДСА	Державна судова адміністрація України
Електронний кабінет (ЕК)	Персональна сторінка Користувача в Єдиній судовій інформаційно-комунікаційній системі, що має статус офіційного процесуального інструменту. Використовується для ідентифікації особи та реалізації її прав і обов'язків, визначених процесуальним законодавством (подання позовів, отримання повісток, участь у відеоконференціях). Сфера застосування: Зовнішні комунікації (суд — учасник справи) та офіційні дії посадових осіб, що мають процесуальні наслідки. Юридичне підґрунтя: Закон України «Про судоустрій і статус суддів», Господарський процесуальний кодекс України, Цивільний процесуальний кодекс України, Кримінальний процесуальний кодекс України, Кодекс адміністративного судочинства України
ЄДРВД, Реєстр	Автоматизована система, що забезпечує створення, внесення, збирання, зберігання, захист, облік, надсилання, пошук та перегляд електронних виконавчих документів, а також надання інформації з них. Реєстр функціонує у складі Єдиної судової інформаційно-комунікаційної системи
Єдиний персональний простір користувача (ЄППК)	Технологічна оболонка та архітектурне рішення фронтенд-частини Системи, що реалізує концепцію «єдиного вікна» для доступу до всіх складових ЄСІКС. ЄППК забезпечує уніфікований користувацький досвід (UX), візуальну цілісність інтерфейсу (UI) та спільну навігацію, виступаючи середовищем для динамічного завантаження функціональних модулів різних складових ЄСІКС без втручання в їхню внутрішню бізнес-логіку. Виступає технологічною платформою для реалізації функціональних можливостей Електронного кабінету та/або Кабінету користувача, яка забезпечує інтеграцію інтерфейсів складових ЄСІКС у єдине робоче середовище.
ЄСІКС, Система	Єдина судова інформаційно-комунікаційна система
ЄСПЛ	Європейський суд з прав людини
Заява на примусове виконання рішення	Електронний документ про примусове виконання рішення (заяви стягувача про виконання рішення), заяви прокурора у разі представництва ним інтересів громадянина або держави в суді, супровідного листа (повідомлення, розпорядження) суду, Національного агентства України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів
ІКС	Інформаційно-комунікаційна система

Інформаційні ресурси	Сукупність електронних документів, що містяться в Реєстрі, а також їх реквізити та відомості
Кабінет користувача (КК)	Узагальнений функціональний інтерфейс («цифрове робоче місце») будь-якої особи, зареєстрованої в Системі (працівника суду, Вищої ради правосуддя, Вищої кваліфікаційної комісії суддів, ДСА або зовнішнього користувача). Кабінет користувача є персоналізованим відображенням доступних користувачеві підсистем, модулів та даних відповідно до його ролей та юридичних статусів. Сфера застосування: внутрішня робота (адміністрування, кадри, бухгалтерія), робота з документами, аналітика, а також доступ до функцій Електронного кабінету. Концептуальна роль: Для громадянина або адвоката його «Кабінет користувача» за набором функцій дорівнює «Електронному кабінету». Для працівника суду «Кабінет користувача» включає як функції Електронного кабінету, так і внутрішні робочі інструменти (підсистема документообігу суду, підсистема кадрового обліку тощо)
КЕП, УЕП	Кваліфікований електронний підпис, Удосконалений електронний підпис
КМУ	Кабінет Міністрів України
Користувач	Особа, яка має активний доступ до функціональності Підсистеми відповідно до налаштованих ролей
Підсистема	Засіб інформатизації, щодо якого створені ці технічні вимоги
Підсистема електронного документообігу суду	Програмний компонент, призначений для автоматизації процесів документообігу судів. Для цілей цих Технічних вимог до введення в експлуатацію підсистеми ЄСІКС «Електронний документообіг суду» таким компонентом вважаються Комп'ютерна програма «Д-3» та Комп'ютерна програма «Діловодство спеціалізованого суду». Після введення в експлуатацію підсистеми ЄСІКС «Електронний документообіг суду» вона замінює зазначені системи та забезпечує виконання їх функцій у складі ЄСІКС
Процесуальний статус користувача	Сукупність визначених прав та повноважень користувача системи у межах конкретного виконавчого документа або відповідного бізнес-процесу, що визначає його права доступу та перелік допустимих дій.
Реєстратор	Суддя, уповноважена особа органу, інша(і) посадова(і) особа(и), які відповідно до закону видають виконавчі документи та/або уповноважені на внесення виконавчих документів до Реєстру.
ТВ	Технічні вимоги. Документ, що визначає планові потреби Власника Підсистеми та загальні умови створення (модернізації, модифікації, розвитку), адміністрування та забезпечення функціонування засобу інформатизації та містить набір критеріїв, які описують засіб інформатизації
ТЗ	Технічне завдання. Документ, розроблений відповідно до технічних вимог, що визначає призначення, показники якості, техніко-економічні, технічні та спеціальні характеристики засобу інформатизації і включає опис робочих процесів (бізнес-процесів) та умови використання засобу інформатизації
Юридичний статус користувача ЄСІКС (юрстатус)	Спеціалізований блок інформації, в якому зазначається, від імені кого користувач входить в систему і має намір здійснювати дії. Різні юридичні статуси передбачають різний набір ролей, який користувач може отримати під час авторизації. Якщо Система не може однозначно визначити за наявними засобами ідентифікації юрстатус користувача, вона це має явно уточнити у користувача під час автентифікації. Одна і та сама ФО (користувач) може мати одночасно декілька юридичних статусів (наприклад, розлучатися через суд як фізична особа і бути

	помічником судді на посаді в суді). Але в Системі такий користувач може працювати тільки під одним конкретно обраним юридичним статусом Розрізняють наступні різновиди юрстатусів: ● Фізична особа — користувач має намір виконувати дії в Системі як пересічний громадянин і представляти сам себе, відповідно такий користувач має право працювати з інформацією та виконувати дії, які стосується виключно його самого як фізичної особи; такі користувачі ідентифікуються за РНОКПП в КЕП ● Посадова особа — користувач, який має намір виконувати дії в Системі як уповноважена особа органу державної влади, органу місцевого самоврядування, суду або іншої організації відповідно до наданих повноважень. Користувач з таким юридичним статусом має отримати ролі та права, що відповідають його посадовим обов'язкам в цій організації на цій посаді. Відповідно, такий користувач має право працювати з інформацією та виконувати дії, які стосуються виключно його посадових обов'язків; такі користувачі ідентифікуються за РНОКПП в КЕП та додатково за ЄДРПОУ організації в КЕП. У разі, якщо користувач одночасно «обіймає» декілька посад (у тому числі виконує обов'язки тимчасово відсутнього працівника), Система під час авторизації повинна забезпечити можливість вибору посади, від імені якої користувач здійснює дії, з урахуванням відповідного набору ролей і прав доступу; ● Представник — користувач має намір виконувати дії в Системі та переглядати інформацію від імені та за дорученням певної юридичної особи або ФОП або від імені іншої фізичної особи. Система має забезпечувати двосторонні механізми призначення представників з забезпеченням всіх юридичних вимог до цієї процедури. Користувач в цьому юридичному статусі має право працювати з інформацією та виконувати дії, які стосуються тільки тієї юридичної особи, ФОП або ФО, яку він представляє. Такі користувачі ідентифікуються за РНОКПП в КЕП та додатково встановленими ознаками, що фіксуються під час призначення представника. З метою зниження технічних помилок, одночасно в рамках поточної сесії роботи в Системі користувач може «представляти» тільки одну конкретну юридичну особу/ФОП або одну конкретну ФО
API (АПІ)	Автоматизовані програмні інтеграції, відомі також як «прикладний інтерфейс програмування – application programming interface»
IAM	Identity Access Management – модуль управління ідентифікацією та доступом

1.5 Нормативно-правові документи

Усі вимоги, визначені цим документом, повинні відповідати нормативно-правовим актам та стандартам, наведеним у цьому розділі:

1. Конституція України
2. Господарський процесуальний кодекс України від 06.11.1991 № 1798-XII
3. Цивільний процесуальний кодекс України від 18.03.2004 № 1618-IV
4. Кодекс адміністративного судочинства України від 06.07.2005 № 2747-IV
5. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI
6. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X
7. Кодекс законів про працю України від 10.12.1971 № 322-VIII
8. Закон України від 23.02.2006 № 3477-IV «Про виконання рішень та застосування практики Європейського суду з прав людини»
9. Закон України від 02.06.2016 № 1404-VIII «Про виконавче провадження»
10. Закон України від 07.04.2026 № 4833-IX «Про внесення змін до деяких законодавчих актів України щодо удосконалення порядку виконання судових рішень, рішень інших органів та цифровізації окремих етапів виконавчого провадження»
11. Закон України від 03.10.2017 № 2147-VIII «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів»
12. Закон України від 29.06.2023 № 3200-IX «Про внесення змін до деяких законодавчих актів України щодо обов'язкової реєстрації та використання електронних кабінетів в Єдиній судовій інформаційно-телекомунікаційній системі або її окремій підсистемі (модулі), що забезпечує обмін документами»
13. Закон України від 02.10.1992 № 2657-XII «Про інформацію»
14. Закон України від 13.01.2011 № 2939-VI «Про доступ до публічної інформації»
15. Закон України від 18.11.2021 № 1907-IX «Про публічні електронні реєстри»
16. Закон України від 01.06.2010 № 2297-VI «Про захист персональних даних»
17. Закон України від 22.05.2003 № 851-IV «Про електронні документи та електронний документообіг»
18. Закон України від 5 жовтня 2017 року № 2155-VIII «Про електронну ідентифікацію та електронні довірчі послуги»
19. Закон України від 05.07.1994 № 80/94-ВР «Про захист інформації в інформаційно-комунікаційних системах»
20. Закон України від 05.10.2017 № 2163-VIII «Про основні засади забезпечення кібербезпеки України»
21. Закон України від 11.05.2004 № 1701-IV «Про третейські суди»
22. Закон України від 02.09.1993 № 3425-XII «Про нотаріат»
23. Закон України від 11.01.2001 № 2210-III «Про захист економічної конкуренції»
24. Закон України від 30.10.1996 № 448/96-ВР «Про державне регулювання ринків капіталу та організованих товарних ринків»
25. Закон України від 07.12.2000 № 2121-III «Про банки і банківську діяльність»
26. Закон України від 06.12.2019 № 361-IX «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення»
27. Закон України від 21.12.2017 № 2258-VIII «Про аудит фінансової звітності та аудиторську діяльність»
28. Закон України від 13.12.2022 № 2849-IX «Про медіа»
29. Постанова Кабінету Міністрів України від 21.10.2015 № 835 «Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних»
30. Постанова Кабінету Міністрів України від 28.06.2024 № 764 «Деякі питання електронної ідентифікації та електронних довірчих послуг»

31. Постанова Кабінету Міністрів України від 21.02.2025 № 205 «Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації»
32. Постанова Кабінету Міністрів України від 03.08.2011 № 845 «Про затвердження Порядку виконання рішень про стягнення коштів державного та місцевих бюджетів або боржників»
33. Рішення Вищої ради правосуддя від 17.08.2021 № 1845/0/15-21 «Про затвердження Положення про порядок функціонування окремих підсистем Єдиної судової інформаційно-телекомунікаційної системи»
34. Наказ Міністерства юстиції України від 05.08.2016 № 2432/5 «Про затвердження Положення про автоматизовану систему виконавчого провадження»
35. Спільний наказ Державної судової адміністрації України та Міністерства юстиції України від 14.06.2022 № 177/2370/5 «Про затвердження Положення про Єдиний державний реєстр виконавчих документів»
36. Рішення Ради суддів України від 11.11.2024 № 39 «Про затвердження Положення про автоматизовану систему документообігу суду»
37. ISO/IEC 19510 — Інформаційні технології — Нотація моделювання бізнес-процесів BPMN версії 2.0
38. ДСТУ ISO/IEC/IEEE 12207:2018 «Процеси життєвого циклу програмних засобів»
39. IETF BCP 47 — стандарт позначення мовних тегів в поєднанні з кодами країн
40. ДСТУ 3973-2000 — Система технічної документації на АСУ. Правила виконання технічного завдання
41. ДСТУ 3974-2000 — Система технічної документації на АСУ. Правила виконання технічного завдання на створення (розвиток або модернізацію) системи
42. ДСТУ 42010:2025 — Програмні засоби, системи та підприємство. Опис архітектури
43. ДСТУ ISO/IEC/IEEE 29148:2025 Інженерія систем і програмних засобів. Процеси життєвого циклу. Інженерія вимог (ISO/IEC/IEEE 29148:2018, IDT)

2. ПРИЗНАЧЕННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ

2.1 Основні завдання та функції засобу інформатизації

Єдиний державний реєстр виконавчих документів є Підсистемою Єдиної судової інформаційно-комунікаційної системи та призначений для організації централізованого обліку виконавчих документів та пов'язаних з ними даних.

У частині роботи з виконавчими документами ЄДРВД забезпечує повний життєвий цикл виконавчого документа – від його створення, внесення або надходження шляхом інформаційної взаємодії до пред'явлення до виконання, зміни процесуального статусу виконання, архівування або знищення у встановленому законодавством порядку. Формування документів, їх підписання, перевірка кваліфікованих електронних підписів, генерація документів у форматі PDF, а також ведення історії змін і журналювання дій користувачів здійснюються із застосуванням функціональних компонентів ЄСІКС.

Функціонування ЄДРВД здійснюється в межах уніфікованої інфраструктури ЄСІКС із використанням централізованих механізмів автентифікації та авторизації, функції пошуку, нотифікацій, інформаційної взаємодії та зберігання даних, що забезпечує цілісність даних, масштабованість, інформаційну безпеку та інтегрованість з іншими підсистемами ЄСІКС і зовнішніми інформаційно-комунікаційними системами.

Межі Підсистеми визначаються як сукупність функціональних можливостей, що забезпечують облік, зберігання, обробку та доступ до виконавчих документів. Функції автентифікації та авторизації користувачів, управління електронними документами, накладення та перевірки електронних підписів, а також функціональні компоненти (зокрема ІАМ, Документ-сервіс, сервіси зберігання та журналювання) не входять до складу ЄДРВД та використовуються як зовнішні централізовані функціональні компоненти ЄСІКС.

2.2 Очікувані результати від впровадження засобу інформатизації

Впровадження ЄДРВД у складі ЄСІКС, відповідно до вимог нормативно-правових актів, дозволить досягти наступних результатів:

- реалізація визначених законодавством функцій щодо створення, внесення, обліку, зберігання, пошуку, надсилання та отримання виконавчих документів в електронній формі;
- забезпечення функціонування ЄДРВД як централізованого єдиного джерела достовірної інформації про облік виконавчих документів та процесуальний стан їх виконання;
- забезпечення доступу виконавців та інших суб'єктів виконання рішень до електронних виконавчих документів з накладеним кваліфікованим електронним підписом;
- забезпечення інформаційної взаємодії між ІКС суб'єктів виконавчого провадження та державними інформаційними системами;
- підвищення прозорості та простежуваності обігу виконавчих документів і моніторингу інформації про стан виконання;
- забезпечення своєчасного інформування користувачів про події, пов'язані з виконавчими документами;
- створення умов для формування статистичної та аналітичної інформації щодо виконання рішень, у тому числі щодо виконавчих документів, виданих на підставі рішень національних судів про стягнення коштів, де боржником є держава,

державний орган, державна установа, державна організація або державне підприємство;

- зменшення фрагментарності даних та дублювання інформації в різних системах;
- зниження операційного навантаження та мінімізація впливу людського фактора;
- забезпечення передумов для подальшого розвитку ЄДРВД та розширення його функціональних можливостей відповідно до законодавства.

2.3 Порядок розвитку засобу інформатизації

Створення ЄДРВД здійснюється в межах реалізації проєкту зі створення Підсистеми як складової ЄСІКС та передбачає доведення її функціональних можливостей до рівня, необхідного для введення в промислову експлуатацію із забезпеченням повноцінного виконання визначених функцій.

На етапі реалізації проєкту забезпечується створення та впровадження функціональності ЄДРВД, необхідної для введення Підсистеми в промислову експлуатацію, включаючи забезпечення повного життєвого циклу виконавчого документа в межах ЄДРВД:

- внесення виконавчого документа;
- реєстрацію та облік;
- зберігання і ведення реквізитів виконавчого документа;
- перегляд та доступ до інформації про виконавчий документ відповідно до повноважень користувачів;
- ініціювання, облік та відображення інформації про платежі, пов'язані з виконанням виконавчих документів;
- пред'явлення виконавчого документа до виконання відповідно до вимог законодавства;
- отримання та фіксацію інформації про статуси виконання;
- завершення життєвого циклу виконавчого документа після присвоєння відповідних процесуальних статусів, визначених законодавством;
- архівування та подальше знищення виконавчого документа, додатків та метаданих після закінчення встановленого строку зберігання.

Зазначені етапи життєвого циклу виконавчого документа забезпечуються шляхом інтеграції ЄДРВД з іншими підсистемами ЄСІКС, функціональними компонентами ЄСІКС, а також з іншими державними інформаційно-комунікаційними системами, у тому числі, але не виключно з АСВП та інформаційними системами Державної казначейської служби України.

З урахуванням кількості зовнішніх ІКС, а також зважаючи на їх розрізненість та різний рівень технічної готовності, окремі інтеграції можуть потребувати додаткового часу та узгодження технічних та організаційних рішень, що необхідно враховувати під час планування строків виконання робіт.

Розвиток ЄДРВД повинен бути здійснений з урахуванням вимог Концепції ЄСІКС та передбачати перевикористання функціональних компонентів.

3. ХАРАКТЕРИСТИКИ ОБ'ЄКТА ІНФОРМАТИЗАЦІЇ

Об'єктом інформатизації є процеси, пов'язані зі створенням, обліком, зберіганням, передачею та подальшим виконанням виконавчих документів в електронній формі відповідно до вимог чинного законодавства.

Підсистема повинна забезпечувати формалізацію, уніфікацію та контроль виконання зазначених процесів, зокрема через фіксацію етапів їх виконання, контроль строків, відстеження змін та забезпечення прозорості відповідних процедур.

Засіб інформатизації повинен забезпечувати досягнення керованого, уніфікованого та контрольованого рівня виконання процесів, пов'язаних з обробкою виконавчих документів, зокрема шляхом:

- стандартизації процедур обробки виконавчих документів;
- автоматизації ключових етапів життєвого циклу виконавчого документа;
- забезпечення повноти та цілісності даних;
- контролю процесу виконання та станів обробки;
- фіксації подій та дій користувачів;
- забезпечення можливості аудиту та відстеження проходження виконавчих документів.

У межах зазначених процесів Підсистема оперує такими інформаційними об'єктами:

- виконавчі документи як електронні інформаційні об'єкти з визначеним набором реквізитів та пов'язаних документів;
- заяви користувачів, пов'язані з виконавчими документами (зокрема заяви про пред'явлення до виконання, відкликання та інші процесуальні звернення), включаючи їх реквізити, статуси та результати обробки;
- відомості про орган, що видав виконавчий документ та учасників виконавчого провадження;
- платежі, пов'язані з виконанням виконавчих документів, включаючи інформацію про їх статус, джерело походження та підтвердження;
- процесуальні статуси виконавчих документів і події, що впливають на їх зміну;
- строки пред'явлення до виконання, виконання та інші часові параметри;
- повідомлення та нотифікації, сформовані Підсистемою або отримані від інших інформаційних систем, включаючи їх зміст, статус доставлення та пов'язані події;
- результати дій користувачів та інформаційних систем, зафіксовані під час роботи з виконавчими документами.

На поточний момент обробка виконавчих документів здійснюється у розрізненому середовищі, яке включає:

- окремі інформаційні системи судів та інших державних органів;
- автоматизовану систему виконавчого провадження;
- локальні програмні засоби та паперові носії;
- організаційні та ручні процедури обміну інформацією.

Інформаційна взаємодія між суб'єктами, залученими до процесу виконання рішень, реалізується шляхом окремих інтеграцій або обміну документами поза автоматизованими каналами. Такі механізми не забезпечують автоматичної валідації даних, цілісності інформації та єдиного життєвого циклу виконавчих документів.

Поточний стан об'єкта інформатизації характеризується відсутністю:

- єдиного сховища виконавчих документів у електронній формі;
- централізованої моделі даних виконавчих документів;
- уніфікованих механізмів контролю статусів і строків;

- єдиних технічних правил інформаційної взаємодії між системами.

Зазначені характеристики визначають об'єкт інформатизації як такий, що характеризується фрагментарністю обліку виконавчих документів, відсутністю інтегрованого інформаційного середовища, що забезпечує узгодженість та синхронізацію даних про виконавчі документи між судами та органами виконання і обмеженими можливостями для наскрізного контролю їх проходження. Саме ці характеристики зумовлюють необхідність створення єдиного засобу інформатизації для впорядкування роботи з виконавчими документами у межах інформаційного супроводу виконавчих документів від моменту їх створення до завершення процедур виконання.

4. ВИМОГИ ДО ЗАСОБУ ІНФОРМАТИЗАЦІЇ

4.1 Вимоги до структури та функціонування засобу інформатизації

Програмне забезпечення ЄДРВД повинно створюватися з урахуванням вимог ДСТУ ISO/IEC/IEEE 12207:2018 «Процеси життєвого циклу програмних засобів» та загальних принципів побудови сучасних інформаційних систем.

ЄДРВД реалізується як підсистема ЄСІКС та функціонує з використанням функціональних компонентів ЄСІКС.

Архітектура ЄДРВД повинна визначатися з урахуванням Концепції ЄСІКС та визначених архітектурних рішень, а також бути орієнтованою на функціональні можливості підсистеми, а не на конкретні технологічні рішення. Підсистема повинна бути розроблена з урахуванням вимог до функціонування в режимі active-active у географічно розподілених центрах обробки даних відповідно до інфраструктурних вимог ЄСІКС.

ЄДРВД має забезпечувати:

- зрозумілий склад функціональних компонентів (модулів);
- чіткі межі відповідальності кожного компонента;
- можливість поетапного розвитку та розширення функціональності.

ЄДРВД повинен забезпечувати такі основні функціональні можливості:

- централізований облік, зберігання та управління виконавчими документами;
- автоматизацію процесів внесення, реєстрації, обліку, передачі та супроводу виконавчих документів в електронній формі;
- доступ користувачів до виконавчих документів і пов'язаної з ними інформації відповідно до визначених ролей, повноважень та прав щодо взаємодії з об'єктами;
- інтеграцію з іншими підсистемами ЄСІКС та зовнішніми державними реєстрами і системами;
- фіксацію статусів виконання виконавчих документів і подій, пов'язаних з їх проходженням;
- відстеження стану виконання (вчинення дій, зміни статусу об'єктів, обумовлених вимогами суду тощо);
- підтримку повідомлень про події та зміни стану виконавчих документів із використанням функціонального компонента «Нотифікації» ЄСІКС;
- забезпечення пошуку та перегляду виконавчих документів із використанням централізованої інфраструктури пошуку ЄСІКС;
- централізоване зберігання виконавчих документів та пов'язаних з ними метаданих;
- підтримку архівування виконавчих документів відповідно до встановлених строків зберігання;
- забезпечення захисту персональних даних та інформаційної безпеки з використанням централізованих механізмів ЄСІКС.

Функції ідентифікації, автентифікації, криптографічного захисту, інтеграції, пошуку, звітності, логування та моніторингу реалізуються з використанням відповідних функціональних компонентів ЄСІКС і не дублюються в ЄДРВД.

4.2 Вимоги до функцій, що виконуються засобом інформатизації

Функції ЄДРВД повинні реалізовуватися як взаємопов'язаний набір можливостей, узгоджених між собою за логікою роботи, структурою даних та правилами взаємодії. Реалізація зазначених функцій повинна забезпечувати єдині підходи до обробки, зберігання та використання даних Реєстру незалежно від способу доступу користувачів, способу створення виконавчих документів або етапів їх проходження.

Функції ЄДРВД повинні забезпечувати:

- коректну обробку даних та їх однозначність в процесі виконання кожної функціональної операції;
- узгодженість станів виконавчих документів між усіма функціональними компонентами системи;
- неможливість виконання дій, які суперечать чинним нормативно-правовим актам;
- фіксацію результатів виконання функцій з можливістю їх контролю та аналізу;
- обробку помилок у спосіб, який не порушує цілісність даних та стабільність роботи системи.

Функції повинні реалізовуватися з урахуванням можливості їх подальшого розвитку, розширення або уточнення без необхідності суттєвої зміни вже реалізованих механізмів та без негативного впливу на існуючі дані й процеси.

4.3 Основні бізнес-процеси

У межах функціонування Підсистеми ЄДРВД реалізуються бізнес-процеси, що охоплюють повний життєвий цикл виконавчого документа, процеси взаємодії із суб'єктами та інформаційними системами, а також підтримуючі процеси забезпечення функціонування Реєстру.

Окремі процеси, необхідні для забезпечення роботи Підсистеми, реалізуються з використанням інших підсистем та функціональних компонентів ЄСІКС. ЄДРВД здійснює ініціювання таких процесів, використовує їх результати та відображає їх у межах власного функціоналу без дублювання відповідної бізнес-логіки:

- Бізнес-процеси доступу та ідентифікації:
 - Автентифікація користувачів.
 - Реєстрація та авторизація користувачів за ролями.
 - Управління ролями та правами доступу до функціоналу Підсистеми.
 - Контроль подій безпеки, аудитних слідів та логування.
- Бізнес-процеси роботи з документами:
 - Створення, редагування та форматування документів;
 - Формування документів на основі шаблонів;
 - Формування візуального представлення документів у форматі PDF;
 - Генерування QR- та штрих-кодів для документів.
- Бізнес-процеси отримання та перегляду повідомлень і системних сповіщень (інформування користувачів про події).
- Бізнес-процеси аналізу та візуалізації аналітичних даних.

У межах цих технічних вимог передбачена реалізація наступних бізнес-процесів (наведений перелік не є вичерпним та може уточнюватися і доповнюватися на етапі розробки технічного завдання без зміни та розширення визначеного переліку функціональних можливостей Підсистеми):

- Внесення та реєстрація виконавчого документа:

- Завантаження з пристрою користувача та внесення обов'язкових реквізитів виконавчого документа.
- Введення даних через користувацький інтерфейс та реєстрація документа в Підсистемі.
- Підписання КЕП виконавчого документа.
- Автоматизована реєстрація документа на основі даних, отриманих через програмний інтерфейс з підсистем ЄСІКС та інших ІКС.
- Автоматична верифікація документа:
 - Перевірка наявності КЕП.
 - Перевірка наявності обов'язкових реквізитів.
- Бізнес-процеси управління життєвим циклом виконавчого документа:
 - Присвоєння процесуальних статусів виконавчому документу.
 - Автоматична зміна статусів відповідно до подій та результатів обробки.
 - Зміна статусів на підставі отриманих даних або дій користувачів у визначених випадках.
- Пред'явлення документа до виконання:
 - Створення заяв на виконання (заповнення шаблону, підписання КЕП)
 - Перевірка наявності передбачених нормативно-правовими актами підстав на виконання рішень.
 - Надсилання заяв до органів та осіб, які здійснюють виконання рішень.
 - Внесення або отримання від органів та осіб, які здійснюють виконання рішень (у т.ч. через програмний інтерфейс ІКС відповідного органу), процесуального статусу виконання та оновлення статусу виконавчого документа.
 - Надання через програмний інтерфейс Підсистемі електронного документообігу суду інформації про зміну статусу виконання судового виконавчого документа.
 - Відкликання надісланої раніше заяви на виконання рішення.
- Бізнес-процеси обробки процесуальних документів, що впливають на стан виконавчого документа (зокрема щодо виправлення помилок або визнання його таким, що не підлягає виконанню), з відповідною зміною його стану та життєвого циклу.
- Бізнес-процеси перегляду виконавчих документів:
 - Перегляд виконавчих документів (перегляд у вигляді списку, а також детальної інформації по документу).
 - Генерація та експорт виконавчого документа на основі шаблону.
 - Перегляд додаткових рішень по виконавчому документу.
- 1. Бізнес-процеси пошуку та фільтрації виконавчих документів:
 - Пошук виконавчих документів за реквізитами.
 - Застосування фільтрів та сортування.
 - Формування вибірок документів за визначеними критеріями.
- Бізнес-процеси управління доступом до виконавчих документів:
 - Забезпечення доступу до виконавчих документів відповідно до ролей, повноважень та процесуального статусу користувача.
 - Перевірка можливості виконання дій користувачем з урахуванням його участі у виконавчому документі та/або наявності повноважень діяти від імені інших суб'єктів.
- 1. Бізнес-процеси зберігання та архівування виконавчих документів:
 - Забезпечення зберігання виконавчих документів та пов'язаних даних.
 - Переведення документів у архівний стан відповідно до їх життєвого циклу, визначених правил та вимог законодавства.

- Обробка документів після завершення їх життєвого циклу відповідно до вимог законодавства.
- Бізнес-процеси моніторингу строків та подій.
- Бізнес-процеси доступу до обраних документів і матеріалів (використання механізмів швидкого доступу (обраного), експорту).

4.4 Опис користувачів Підсистеми та доступів

Підсистема повинна забезпечувати розмежування доступу користувачів до функціональних можливостей та інформаційних ресурсів на основі ролей відповідно до їх повноважень шляхом використання функціонального компонента Керування доступом (Управління ідентифікацією та доступом (IAM)) ЄСІКС.

Модель доступу повинна передбачати можливість визначення, налаштування та зміни ролей користувачів, а також пов'язаних з ними прав доступу, з урахуванням вимог законодавства та організаційної структури Адміністратора Підсистеми.

Підсистема повинна забезпечувати можливість здійснення користувачем дій як від власного імені, так і від імені інших осіб або організацій (зокрема юридичних осіб, органів державної влади, органів місцевого самоврядування) відповідно до його юридичного статусу та повноважень, визначених через IAM.

Розмежування прав доступу має здійснюватися з урахуванням ролі користувача, його юридичного статусу, атрибутів, належності до організації, а також контексту взаємодії з конкретним виконавчим документом або бізнес-процесом.

У Підсистемі повинні бути доступні наступні ролі користувачів:

Аліас	Група користувачів	Опис	Ролі
P1 edrvd_admin	Адміністратор	Користувачі, які здійснюють технічне адміністрування Підсистеми, включаючи налаштування параметрів функціонування та управління правами доступу. Доступ до інформаційних ресурсів надається виключно в межах виконання адміністративних функцій. Доступ до вмісту виконавчих документів та персональних даних не надається, за винятком випадків, передбачених законодавством. Дії користувача підлягають обов'язковому журналюванню.	

P2 edrvd_full_auth	Уповноважена особа з повним доступом	Користувачі, які є уповноваженими представниками органів державної влади та здійснюють функції нагляду, координації і контролю за функціонуванням Підсистеми. Доступ до інформаційних ресурсів надається в межах виконання визначених законодавством повноважень. Такі користувачі мають право перегляду виконавчих документів, пов'язаних даних, а також використання функціональних можливостей Підсистеми, необхідних для реалізації їх повноважень. Доступ до окремих категорій інформації, у тому числі персональних даних, здійснюється з урахуванням вимог законодавства щодо захисту інформації та розмежування прав доступу. Дії користувача підлягають обов'язковому журналюванню.	- посадові особи Державної судової адміністрації України; - посадові особи Міністерства юстиції України; - посадові особи органів державної влади відповідно до законодавства.
P3 edrvd_limit_auth	Уповноважена особа із загальним доступом (Реєстратор)	Користувачі, які є уповноваженими посадовими особами та здійснюють професійну діяльність, пов'язану зі створенням, внесенням та використанням виконавчих документів. Доступ до інформаційних ресурсів надається виключно в межах виконання їх повноважень та обмежується виконавчими документами і пов'язаною з ними інформацією, необхідною для здійснення відповідних функцій. Рівень доступу визначається відповідно до ролі користувача із дотриманням вимог законодавства щодо захисту інформації. Дії користувача підлягають обов'язковому журналюванню.	- судді місцевих та апеляційних судів, вищих спеціалізованих судів; - судді господарського суду; - судді адміністративного суду; - працівники секретаріату Урядового уповноваженого у справах ЄСПЛ; - нотаріуси; - голови або заступники або секретарі комісії по трудових спорах; - державні виконавці; - приватні виконавці; - уповноважені особи інших органів; - інші суб'єкти.
P4 edrvd_user	Користувач із загальним доступом	Користувачі, які зазначені у виконавчих документах сторонами або іншими учасниками, визначеними законодавством. Доступ до інформаційних ресурсів надається виключно щодо виконавчих документів, у яких такі	- стягувачі; - боржники; - уповноважені представники стягувачів; - уповноважені представники боржників; - арбітражні керуючі; - інші суб'єкти.

		користувачі зазначені як сторони, та обмежується інформацією, необхідною для реалізації їх прав та обов'язків. Такі користувачі мають можливість перегляду інформації про виконавчі документи та стан їх виконання, а також ініціювання передбачених законодавством та функціоналом Підсистеми дій у межах наданих повноважень. Доступ здійснюється з дотриманням вимог законодавства щодо захисту інформації. Дії користувача підлягають обов'язковому журналюванню.	
--	--	---	--

4.4.1 Ролі та права доступу

Управління ролями користувачів, створення облікових записів, надання прав доступу та налаштування політик, які регулюють дозволи на виконання дій, пов'язаних з виконавчими документами, здійснюється виключно з використанням функціонального компонента Керування доступом (Управління ідентифікацією та доступом (IAM)) ЄСІКС.

В межах ЄДРВД повинно бути використано зазначену рольову модель з метою контролю доступу користувачів до функціональності реєстру та даних. ЄДРВД не передбачає реалізацію власної функціональності управління ролями або правами користувачів. Перевірка прав доступу до функціональності реєстру та даних здійснюється на основі ролей, атрибутів, юридичного статусу користувача, а також його участі у виконавчому документі або відповідному бізнес-процесі відповідно до п. 5.5.1.1 цих Технічних вимог. Виконавець повинен спроекувати та зареєструвати в функціональному компоненті IAM ЄСІКС користувацькі ролі та політики доступу для ЄДРВД. Доступ надається за принципом найменших привілеїв.

Права доступу визначають можливість виконання користувачем певних дій у реєстрі, зокрема:

- ✓ – доступ дозволено;
- – доступу немає

Функціональний блок	Функція	P1	P2	P3	P4	Підсистема
Виконавчий документ	Створення виконавчого документа користувачем у вебінтерфейсі	–	–	✓	–	–
	Реєстрація виконавчого документа	–	–	✓	–	✓

	Перегляд реєстраційної картки виконавчого документа	–	✓	✓	✓	–
	Перегляд виконавчих документів	–	✓	✓	✓	–
	Зміна процесуального статусу виконання виконавчого документа	–	–	✓	–	✓
	Архівування виконавчого документа	–	–	–	–	✓
	Знищення виконавчого документа	–	–	–	–	✓
	Пошук виконавчого документа	–	✓	✓	✓	–
Надання доступу до виконавчого документа	Надання доступу до виконавчого документа іншому користувачу	–	–	–	✓	–
	Надання прав на здійснення процесуальних дій з виконавчим документом	–	–	–	✓	–
	Перегляд переліку користувачів, яким надано доступ до виконавчого документа	–	–	–	✓	–
	Відкликання доступу до виконавчого документа	–	–	–	✓	–
Визнання виконавчого документа таким, що не підлягає виконанню	Реєстрація ухвали або рішення суду про визнання виконавчого документа таким, що не підлягає виконанню	–	–	✓	–	✓
	Перегляд ухвали або рішення суду про визнання виконавчого документа таким, що не підлягає виконанню	–	✓	✓	✓	–
Виправлення помилки у виконавчому документі	Реєстрація документа про виправлення виконавчого документа	–	–	✓	–	✓

	Перегляд документа про виправлення помилки у виконавчому документі	–	✓	✓	✓	–
Пред’явлення виконавчого документа до виконання	Створення заяви про виконання рішення	–	–	✓	✓	–
	Перегляд заяви про виконання рішення	–	✓	✓	✓	–
	Зміна статусу заяви про виконання рішення	–	–	✓	✓	✓
Створення заяви про повернення виконавчого документа	Створення заяви про повернення виконавчого документа	–	–	–	✓	–
	Перегляд заяви про повернення виконавчого документа	–	✓	✓	✓	–
	Зміна статусу заяви про повернення виконавчого документа	–	–	✓	–	✓
Подання заяви про поновлення виконавчого провадження	Створення заяви про поновлення виконавчого провадження	–	–	✓	✓	–
	Перегляд заяви про поновлення виконавчого провадження	–	✓	✓	✓	–
	Зміна статусу заяви про поновлення виконавчого провадження	–	–	✓	✓	✓
Шаблони виконавчих документів	Створення шаблону документа	✓	–	–	–	–
	Оновлення реквізитів шаблону документа	✓	–	–	–	–

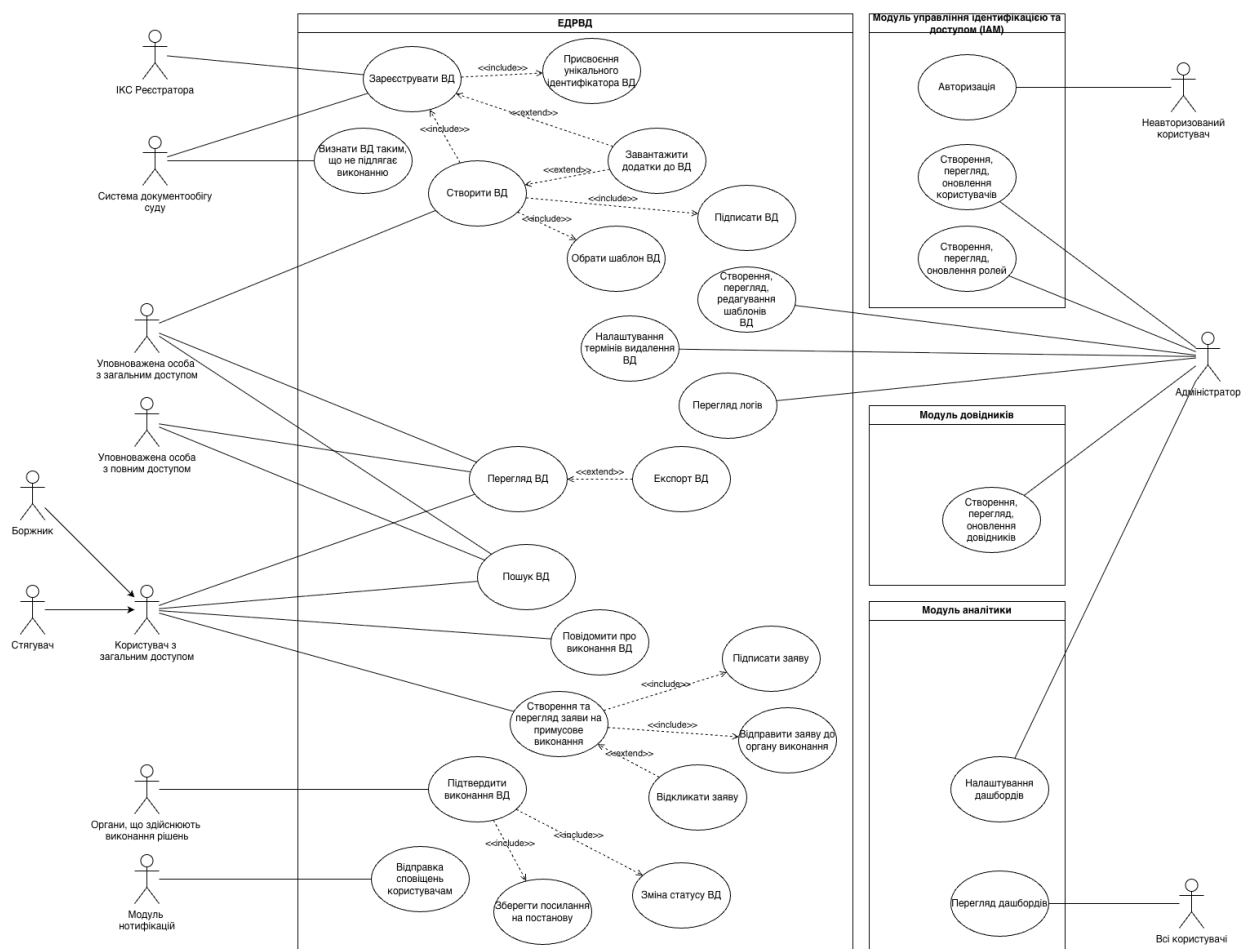
	Перегляд шаблонів виконавчих документів	✓	–	–	–	–
	Зміна статусу шаблону документа	✓	–	–	–	–
Нотифікації користувачів	Створення нотифікації	–	–	–	–	✓

Приведено узагальнену модель, яка повинна мати можливість гнучкого налаштування залежно від потреб користувачів та за погодженням з Адміністратором Підсистеми. Деталізація функціональних можливостей користувачів відповідно до визначених ролей та прав доступу уточнюється та погоджується між Виконавцем і Адміністратором Підсистеми на етапі розроблення технічного завдання.

5. ФУНКЦІОНАЛЬНІ ВИМОГИ

Відповідно до Концепції ЄСІКС, Підсистема призначена для автоматизації створення, внесення, обліку, пошуку, надання інформації щодо виконавчих документів та їх пред'явлення до виконання. Функціональні вимоги можуть уточнюватися, змінюватися, скорочуватися або доповнюватися в Технічному завданні за умови цілісності функціоналу.

Загальний перелік функціональності ЄДРВД зображений на діаграмі



Use case diagram ЄДРВД

5.1 Виконавчий документ

1. Підсистема повинна забезпечувати централізовану реєстрацію виконавчих документів в електронній формі.
2. Підсистема повинна забезпечувати облік виконавчих документів незалежно від способу їх створення або надходження до Підсистеми.
3. Підсистема повинна підтримувати такі способи внесення виконавчого документа:
 - завантаження з пристрою користувача та внесення обов'язкових реквізитів виконавчого документа;
 - створення виконавчого документа безпосередньо в Підсистемі з використанням затверджених шаблонів;
 - отримання виконавчих документів з інших інформаційних систем у межах інформаційної взаємодії (інтеграції API).

4. Виконавчі документи, які можуть бути внесені в Підсистему:

- виконавчі листи та накази, що видаються судами у передбачених законом випадках на підставі судових рішень, рішень третейського суду, рішень міжнародного комерційного арбітражу, рішень іноземних судів та на інших підставах, визначених законом або міжнародним договором України;
- судові накази;
- ухвали, постанови судів у цивільних, господарських, адміністративних справах, справах про адміністративні правопорушення, кримінальних провадженнях у випадках, передбачених законом;
- виконавчі написи нотаріусів;
- спеціальні виписки з Реєстру аграрних нот, що генерується за допомогою програмно-технічних засобів Реєстру аграрних нот виключно для звернення стягнення за аграрною нотою;
- посвідчення комісій по трудових спорах, що видаються на підставі відповідних рішень таких комісій;
- постанови державних виконавців про стягнення виконавчого збору, постанови державних виконавців чи приватних виконавців про стягнення витрат виконавчого провадження, про накладення штрафу, постанови приватних виконавців про стягнення основної винагороди;
- постанови органів (посадових осіб), уповноважених розглядати справи про адміністративні правопорушення у випадках, передбачених законом;
- рішення інших державних органів, рішення (акти) Національної комісії з цінних паперів та фондового ринку та рішення Національного банку України, які законом визнані виконавчими документами;
- рішення Європейського суду з прав людини з урахуванням особливостей, передбачених Законом України "Про виконання рішень та застосування практики Європейського суду з прав людини", а також рішення інших міжнародних юрисдикційних органів у випадках, передбачених міжнародним договором України;
- рішення (постанови) суб'єктів державного фінансового моніторингу (їх уповноважених посадових осіб), якщо їх виконання за законом покладено на органи та осіб, які здійснюють примусове виконання рішень;
- рішення Органу суспільного нагляду за аудиторською діяльністю або Аудиторської палати України, які законом визнані виконавчими документами;
- рішення Національної ради України з питань телебачення і радіомовлення про застосування заходів реагування у вигляді штрафу.

5. Користувачі можуть ініціювати наступні процеси, пов'язані з виконавчими документами, зокрема:

- створення Заяви на виконання рішення;
- створення Заяви про поновлення виконавчого провадження;
- створення Заяви про повернення виконавчого документа;
- повідомлення від Міністерства юстиції або Уповноваженого ЄСПЛ стягувачу;
- заяви про відшкодування за рішенням ЄСПЛ.

6. Зазначений перелік документів, які можуть бути внесені та зберігатися в ЄДРВД, має відповідати нормам статті 3 ЗУ «Про виконавче провадження» та може бути уточнений за погодженням із Власником Підсистеми на етапі підготовки технічного завдання.

5.1.1 Створення виконавчого документа користувачем у вебінтерфейсі

1. У Підсистемі повинна бути передбачена можливість створення виконавчого документа користувачем у вебінтерфейсі Підсистеми на основі наявних у системі типів виконавчих документів.
2. Для створення виконавчого документа у вебінтерфейсі, користувач повинен обрати тип виконавчого документа. Перелік доступних типів виконавчих документів може відрізнитись залежно від ролей, повноважень користувача та його належності до відповідної організації і обмежується типами виконавчих документів, які уповноважена формувати така організація.
3. Після обрання типу виконавчого документа, Підсистема повинна відображати користувачу реєстраційну картку для заповнення атрибутів виконавчого документа.
4. При внесенні даних в реєстраційну картку повинна здійснюватись валідація внесених даних. У разі некоректного введення даних, або незаповнення обов'язкових інформаційних полів в реєстраційній картці, має відображатись відповідне валідаційне повідомлення.
5. До реєстраційної картки виконавчого документа можуть додаватися інші документи — додатки до виконавчого документа.
6. Користувач повинен мати можливість зберегти внесені дані та підписати їх КЕП.
7. До підписання КЕП виконавчий документ може змінюватися або видалятися.
8. Після підписання КЕП виконавчий документ та пов'язані з ним дані не можуть бути змінені чи видалені.
9. Підписання виконавчого документа КЕП повинно ініціювати процес автоматичної реєстрації документа в Підсистемі.

5.1.2 Реєстрація виконавчого документа

1. Реєстрація виконавчого документа повинна відбуватись автоматично після наступних подій:
 - завантаження виконавчого документа з пристрою користувача, внесення обов'язкових реквізитів виконавчого документа та накладання КЕП;
 - створення та підписання КЕП виконавчого документа користувачем у вебінтерфейсі;
 - отримання засобами інформаційної взаємодії інформації про створення виконавчого документа в Підсистемі Електронний документообіг суду;
 - отримання засобами інформаційної взаємодії виконавчого документа, створеного в ІКС Реєстратора за межами ЄСІКС.
2. При реєстрації виконавчого документа в Реєстрі формується реєстраційна картка, в якій містяться такі реквізити та відомості:
 - назва виконавчого документа;
 - унікальний номер виконавчого документа, який генерується за єдиним шаблоном із трьох цифрових груп, розділених крапкою: код реєстратора (шість цифр, рік реєстрації виконавчого документа (чотири цифри), унікальний номер виконавчого документа за порядком у році його реєстрації (сім цифр);
 - унікальна вебадреса на виконавчий документ в централізованому сховищі ЄСІКС;
 - дата видачі виконавчого документа;
 - код та найменування органу, який видав виконавчий документ, згідно з довідником адміністратора, прізвище, ім'я, по батькові (за наявності) і посада реєстратора;
 - резолютивна частина рішення, на підставі якого видано виконавчий документ (резолютивна частина виконавчого документа);

- сума коштів, що підлягає стягненню за кожною вимогою (у разі виконання рішень про стягнення коштів);
 - відстрочка або розстрочка виконання рішення (за наявності);
 - граничний строк виконання рішення (за наявності);
 - вид боржника згідно з наявною інформацією в довідниках, включаючи можливість ідентифікації боржника як держави, державного органу, державної установи, державної організації, державного підприємства або іншого суб'єкта державного сектору;
 - унікальний номер запису в Єдиному державному демографічному реєстрі стягувача/боржника (за наявності);
 - ідентифікаційний код стягувача/боржника-юридичної особи в Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань;
 - ознака належності боржника-юридичної особи до державного сектору/державної форми власності згідно з відомостями відповідних довідників, класифікаторів або державних реєстрів;
 - реєстраційний номер облікової картки платника податків або серія та/або номер паспорта громадянина України (для фізичних осіб, які через свої релігійні переконання в установленому порядку відмовилися від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган і мають відмітку в паспорті громадянина України), у тому числі з імплантованим безконтактним електронним носієм, стягувача/боржника (для фізичних осіб – платників податків) (за наявності);
 - процесуальний статус виконавчого документа;
 - інші організаційно-технічні відомості, визначені на етапі розробки технічного завдання.
3. У реєстраційній картці до виконавчого документа, що внесений суддею, додатково до загальних реквізитів та відомостей зазначаються:
- форма судочинства;
 - форма рішення;
 - єдиний унікальний номер судової справи (кримінального провадження);
 - категорія справи;
 - склад суду із зазначенням судді (суддів);
 - дата ухвалення рішення;
 - дата набрання рішенням законної сили (крім рішень, що підлягають негайному виконанню);
 - заходи для забезпечення виконання рішення.
4. Під час внесення даних до реєстраційної картки Підсистема повинна використовувати дані локальних довідників Підсистеми, функціонального компонента «Довідники та класифікатори» та майстер-реєстрів.
5. Перед реєстрацією виконавчого документа Підсистема повинна перевірити коректність заповнення його реквізитів та КЕП.
6. Підсистема повинна мати можливість повідомляти інші підсистеми про реєстрацію виконавчого документа в ЄДРВД.
7. Після реєстрації виконавчого документа він повинен стати доступним для перегляду користувачам, які мають для цього відповідні права.
8. Сторонам, зазначеним у виконавчому документі повинні надсилатися повідомлення про реєстрацію нового виконавчого документа за допомогою функціонального компонента «Нотифікації».

5.1.3 Перегляд реєстраційної картки виконавчого документа

1. Користувач повинен мати можливість переглядати реєстраційну картку виконавчого документа відповідно до своїх прав та налаштованих політик.
2. В Підсистемі має бути реалізована можливість фільтрації та сортування доступних користувачу реєстраційних карток виконавчих документів.
3. При перегляді картки виконавчого документа, крім реквізитів та відомостей виконавчого документа, перелічених в розділі [5.1.2 Реєстрація виконавчого документа](#) повинні відображатись:
 - пов'язані з цим документом рішення про виправлення виконавчого документа (за наявності);
 - пов'язані з цим документом виконавчі провадження або процеси виконання та їх стани (за наявності).

5.1.4 Перегляд виконавчих документів

1. Користувач повинен мати можливість формувати представлення виконавчого документа у форматі PDF на основі актуальних структурованих даних виконавчого документа та затверджених шаблонів.
2. Шаблони виконавчих документів та правила їх заповнення формуються на підставі матеріалів, наданих уповноваженими на видання виконавчих документів органів державної влади, та погоджуються з Адміністратором Підсистеми.
3. Кожен тип виконавчого документа може мати декілька версій шаблонів, які містять визначені набори атрибутів, та мають визначений термін дії.
4. Сформований PDF-документ повинен містити реквізити виконавчого документа та інформацію про накладений кваліфікований електронний підпис, включаючи дані про підписувача, дату та час підписання.
5. У сформований PDF-документ повинні автоматично вбудовуватися QR-коди або штрих-коди, що містять унікальний ідентифікатор виконавчого документа або посилання на сервіс перевірки його автентичності в ЄДРВД.
6. Підсистема повинна забезпечувати можливість вивантаження PDF-документа.

5.1.5 Зміна процесуального статусу виконання виконавчого документа

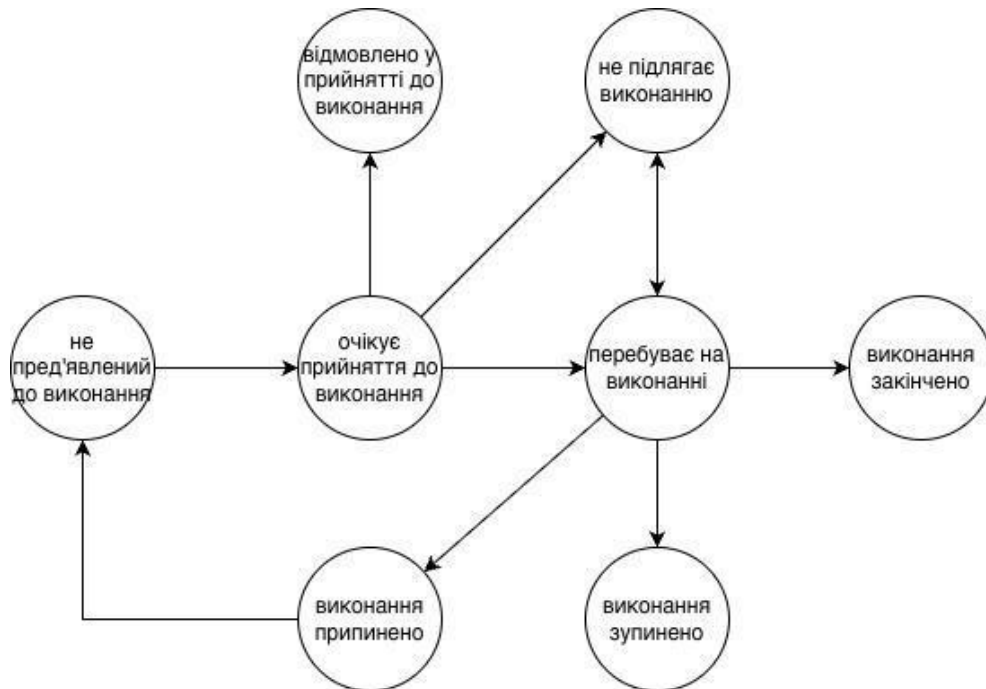
1. Підсистема повинна змінювати процесуальний статус виконання виконавчого документа у відповідь на дії користувача або інших систем.
2. Процесуальний статус виконання виконавчого документа є окремою характеристикою та не залежить від статусу виконавчого документа як електронного об'єкта у Підсистемі.
3. Статус виконавчого документа як електронного об'єкта Підсистеми визначає стан його внесення та реєстрації (чернетка, проєкт, оригінал) і не відображає стан його виконання.

Статус виконання	Опис
не підлягає виконанню	встановлюється у випадках, коли виконавчий документ визнано таким, що не підлягає виконанню відповідно до рішення суду або в інших випадках, визначених законодавством
не пред'явлений до виконання	відображає стан виконавчого документа, який не був поданий до органу, що здійснює виконання рішення, у встановленому законодавством порядку, а також

	встановлюється після повернення виконавчого документа стягувачу до моменту поновлення виконавчого провадження та після отримання постанови виконавця про відмову у поновленні виконавчого провадження
очікує прийняття до виконання	встановлюється після подання виконавчого документа (або заяви про виконання рішення) до відповідного органу, що здійснює виконання рішення та до моменту прийняття рішення про відкриття або відмову у відкритті провадження
відмовлено у прийнятті до виконання	встановлюється у разі відмови у відкритті виконавчого провадження або відмови у прийнятті документа до виконання з підстав, визначених законодавством
перебуває на виконанні	відображає стан виконавчого документа після прийняття його до виконання і до закриття всіх виконавчих проваджень або процесів виконання цього документа
виконання зупинено	встановлюється у випадках зупинення виконавчого провадження або виконання з підстав, передбачених законодавством
виконання припинено	встановлюється у разі припинення виконавчого провадження або виконання з підстав, визначених законодавством
виконання закінчено	встановлюється у разі завершення виконання (у тому числі фактичного виконання або завершення провадження) відповідно до законодавства

4. Підсистема повинна забезпечувати формування та оновлення станів пов'язаних процесів виконання на підставі:
 - отриманих даних з інших інформаційних систем, в яких працюють органи та особи, які здійснюють виконання рішень;
 - дій уповноважених осіб (з визначеним процесуальним статусом) у випадках, передбачених законодавством та відповідно до ролей та прав доступу у Підсистемі.
5. У межах інформаційної взаємодії з зовнішніми системами в яких працюють органи та особи, які здійснюють виконання рішень, Підсистема повинна забезпечувати отримання, інтерпретування та відображення процесів виконання (у т.ч. через вебпосилання на ресурси органів виконання), пов'язаних з виконавчим документом, та їх станів.
6. У разі неможливості реалізації інформаційної взаємодії з зовнішніми системами в яких працюють органи та особи, які здійснюють виконання рішень, повинен бути реалізований функціонал внесення інформації про процеси виконання та їх стани через вебінтерфейс.
7. Підсистема повинна визначати процесуальний статус виконання виконавчого документа залежно від наявності та статусів пов'язаних з документом:
 - заяв про виконання виконавчого документа (заяви на виконання рішення, заяви про поновлення виконавчого провадження, заяви про повернення виконавчого документа, повідомлення від Міністерства юстиції або Уповноваженого ЄСПЛ стягувачу, заяви про відшкодування за рішенням ЄСПЛ);
 - процесів виконання;

- ухвал або рішень про визнання виконавчого документа таким, що не підлягає виконанню.
8. Один виконавчий документ може мати один або декілька процесів виконання. Процесуальний статус виконання виконавчого документа повинен формуватися з урахуванням станів пов'язаних процесів виконання виконавчого документа.
 9. Можливі переходи між процесуальними статусами виконання представлені на діаграмі статусів:



Діаграма процесуальних статусів виконавчого документа

10. Стягувачу та боржнику, зазначеним у виконавчому документі, повинні надсилатися повідомлення про зміну процесуального статусу виконання виконавчого документа.
11. Органу, який видав виконавчий документ, повинна надсилатися інформація про зміну процесуального статусу та інші атрибути, які стосуються виконання виконавчого документа.
12. Відправка повідомлень повинна відбуватися засобами функціонального компонента «Нотифікації».
13. Підсистема повинна зберігати історію змін процесуальних статусів виконання виконавчого документа та пов'язаних з ним процесів виконання.
14. Перелік процесуальних статусів виконання не є вичерпним та може бути доповнений за погодженням із Власником Підсистеми на етапі розробки технічного завдання.

5.1.6 Архівування виконавчого документа

1. Підсистема повинна забезпечувати можливість автоматичного архівування виконавчих документів та пов'язаних з ним документів відповідно до налаштованих критеріїв, зокрема:
 - дата створення;
 - процесуальний статус документа (не підлягає виконанню, виконання закінчено);
 - термін зберігання відповідно до законодавства.
2. Підсистема повинна забезпечувати архівування виконавчих документів відповідно

до вимог законодавства України у сфері діловодства та архівного зберігання, з урахуванням строків зберігання документів, їх класифікації та порядку передачі до архіву.

3. Під час архівування повинно забезпечуватися збереження всіх структурованих даних, пов'язаних документів та метаданих, а також цілісність і простежуваність інформації.
4. Користувачі можуть здійснювати пошук архівованих документів за різними критеріями (назва документа, автор, дата архівування, ключові слова) та відновлювати архівовані дані до активної бази.
5. Архівовані документи не можуть бути змінені.
6. Користувачі можуть відновити архівовані документи за правилами, встановленими Підсистемою. Відновлення архівованих документів передбачає відновлення виконавчих документів, пов'язаних документів та усіх метаданих.
7. Факт архівування повинен фіксуватися як окрема системна подія зі збереженням інформації про:
 - дату та час архівування;
 - підставу архівування.

5.1.7 Знищення виконавчого документа

1. У Підсистемі має бути передбачено можливість знищення виконавчих та пов'язаних з ними документів після встановленого терміну зберігання відповідно до законодавства.
2. Встановлення терміну зберігання має відбуватися за налаштованим алгоритмом відповідно до норм законодавства.
3. В Підсистемі повинна зберігатися інформація про знищення кожного виконавчого документа.

5.1.8 Пошук виконавчого документа

1. У Підсистемі має бути реалізована можливість пошуку та фільтрації доступних користувачу виконавчих документів.
2. Пошук та фільтрація повинні відбуватися за реквізитами виконавчого документа та ключовими словами.
3. Має бути реалізована можливість пошуку та фільтрації за кількома реквізитами виконавчого документа.
4. Підсистема повинна надавати можливість сортувати виконавчі документи, які відображаються в результатах пошуку.

5.2 Визнання виконавчого документа таким, що не підлягає виконанню

5.2.1 Реєстрація ухвали або рішення про визнання виконавчого документа таким, що не підлягає виконанню

1. Реєстратор, Підсистема Документообігу суду або ІКС Реєстратора повинні мати функціональну можливість зареєструвати ухвалу або рішення про визнання виконавчого документа таким, що не підлягає виконанню.
2. Ухвала або рішення, що визнає виконавчий документ таким, що не підлягає виконанню, повинна реєструватися в підсистемі аналогічно виконавчому документу.
3. Перед реєстрацією ухвали або рішення про визнання виконавчого документа таким, що не підлягає виконанню, Підсистема повинна перевірити коректність заповнення його реквізитів та КЕП.

4. При реєстрації в Підсистемі ухвали або рішення про визнання виконавчого документа таким, що не підлягає виконанню, йому має присвоюватися унікальний номер.
5. Після реєстрації ухвали або рішення про визнання виконавчого документа таким, що не підлягає виконанню, воно не може бути змінено.
6. В реквізитах ухвали або рішення про визнання виконавчого документа таким, що не підлягає виконанню, обов'язково має бути зазначений виконавчий документ, з яким пов'язано ухвала або рішення.
7. Після реєстрації в Підсистемі ухвали або рішення про визнання виконавчого документа таким, що не підлягає виконанню, пов'язаному виконавчому документу присвоюється статус «не підлягає виконанню».
8. Після реєстрації ухвали або рішення про визнання виконавчого документа таким, що не підлягає виконанню, воно повинно стати доступним для перегляду користувачам, які мають для цього відповідні права.
9. Стягувачу та боржнику, зазначеним у пов'язаному виконавчому документі, повинні надсилатися повідомлення про реєстрацію ухвали або рішення про визнання виконавчого документа таким, що не підлягає виконанню, з використанням функціонального компонента «Нотифікації».
10. Якщо на момент реєстрації ухвали або рішення про визнання виконавчого документа таким, що не підлягає виконанню, пов'язаний виконавчий документ має процесуальний статус «перебуває на виконанні», Підсистема повинна забезпечити передачу зазначеної ухвали або рішення до органу, який здійснює виконання рішень, та отримати відповідь про статус відправки.

5.2.2 Перегляд ухвали або рішення про визнання виконавчого документа таким, що не підлягає виконанню

1. Користувач може переглядати ухвалу або рішення про визнання виконавчого документа таким, що не підлягає виконанню.
2. В Підсистемі має бути реалізована можливість фільтрації та сортування ухвал та рішень про визнання виконавчого документа таким, що не підлягає виконанню.
3. В Підсистемі має бути реалізована можливість виконувати пошук серед доступних для перегляду ухвал та рішень про визнання виконавчого документа таким, що не підлягає виконанню.
4. Користувач повинен мати можливість експортувати доступні ухвали та рішення про визнання виконавчого документа таким, що не підлягає виконанню.

5.3 Виправлення помилки у виконавчому документі

5.3.1 Реєстрація документа про виправлення помилки у виконавчому документі

1. Реєстратор, Підсистема Документообігу суду або ІКС Реєстратора повинні мати функціональну можливість зареєструвати документ про виправлення у раніше створеному виконавчому документі.
2. Документ, яким виправлено помилку у виконавчому документі, повинен реєструватися в підсистемі аналогічно виконавчому документу.
3. Перед реєстрацією документа про виправлення помилки у виконавчому документі Підсистема повинна перевірити коректність заповнення його реквізитів та КЕП.
4. При реєстрації в Підсистемі документа про виправлення помилки у виконавчому документі йому має присвоюватися унікальний номер.
5. В реквізитах документа про виправлення помилки у виконавчому документі обов'язково має бути зазначений виконавчий документ, з яким він пов'язаний.

6. Підсистема не повинна змінювати первинні дані виконавчого документа, а повинна зберігати їх разом із внесеними виправленнями як окремий пов'язаний об'єкт.
7. Після реєстрації документа про виправлення помилки у виконавчому документі такий документ не може бути змінений.
8. Стягувачу та боржнику, зазначеним у пов'язаному виконавчому документі, повинні надсилатися повідомлення про реєстрацію документа про виправлення помилки у виконавчому документі за допомогою функціонального компонента «Нотифікації».
9. Документ про виправлення помилки у виконавчому документі повинен відображатися сторонам, зазначеним у пов'язаному виконавчому документі.
10. Якщо на момент реєстрації документа про виправлення помилки у виконавчому документі, пов'язаний виконавчий документ має процесуальний статус «перебуває на виконанні», Підсистема повинна забезпечити передачу зазначеного документа про виправлення до органу, який здійснює виконання рішень, та отримати відповідь про статус відправки.

5.3.2 Перегляд документа про виправлення помилки у виконавчому документі

1. Користувач може переглядати документ про виправлення помилки у виконавчому документі та пов'язаний з ним виконавчий документ.
2. В Підсистемі має бути реалізована можливість фільтрації та сортування доступних користувачу документів про виправлення помилки у виконавчому документі.
3. В Підсистемі має бути реалізована можливість виконувати пошук серед доступних для перегляду документів про виправлення помилки у виконавчому документі з опцією збереження структури пошукових запитів.

5.4 Пред'явлення виконавчого документа до виконання

5.4.1 Створення заяви про виконання рішення

1. Користувач може створити заяву про виконання рішення у випадках, коли він зазначений у реквізитах ВД як сторона стягнення.
2. Заява про виконання рішення повинна реєструватися в Підсистемі, аналогічно процесу реєстрації виконавчого документа.
3. В реквізитах заяви про виконання має бути зазначений виконавчий документ. До заяви можуть додаватися інші пов'язані документи (додатки), передбачені законодавством.
4. Перед створенням заяви про виконання рішення Підсистема має виконати перевірку валідності виконавчого документа та відсутність інших заяв по виконавчому документу. У разі неуспішної перевірки система повинна блокувати можливість створення заяви про виконання рішення, повідомити про це Користувача та запропонувати подати заяву про поновлення виконавчого провадження.
5. Після успішного створення заяви про виконання рішення, Підсистема повинна надіслати її до органів, які здійснюють виконання рішень, та отримати відповідь про статус відправки.
6. Після успішної відправки заяви про виконання рішення Підсистема повинна присвоїти виконавчому документу процесуальний статус виконання «очікує прийняття до виконання».

5.4.2. Створення заяви про повернення виконавчого документа

1. Користувач, зазначений у реквізитах виконавчого документа як сторона стягнення повинен мати можливість подати заяву про повернення виконавчого документа у випадках, визначених законодавством.
2. Заява про повернення виконавчого документа повинна реєструватися в Підсистемі аналогічно процесу реєстрації виконавчого документа.
3. В реквізитах заяви про повернення виконавчого документа має бути зазначений пов'язаний виконавчий документ. До заяви можуть додаватися інші пов'язані документи, передбачені законодавством.
4. Перед створенням заяви про повернення виконавчого документа Підсистема повинна перевірити, що виконавчий документ має процесуальний статус виконання «перебуває на виконанні». У разі неуспішної перевірки Підсистема повинна блокувати подання заяви та повідомити про це користувача.
5. Після успішного створення заяви про повернення виконавчого документа Підсистема повинна надіслати її до органів, які здійснюють виконання рішень, та отримати відповідь про статус відправки.

5.4.3 Поновлення виконавчого провадження

1. Заяву про поновлення виконавчого провадження може подати стягувач або боржник, інший користувач у разі представництва інтересів громадянина або держави в суді, а також суд шляхом направлення відповідної заяви або повідомлення.
2. Заява про поновлення виконавчого провадження повинна реєструватися в Підсистемі аналогічно процесу реєстрації виконавчого документа.
3. В реквізитах заяви про поновлення виконавчого провадження має бути зазначений пов'язаний виконавчий документ. До заяви можуть додаватися інші пов'язані документи (додатки), передбачені законодавством.
4. Перед поданням заяви про поновлення виконавчого провадження Підсистема повинна перевірити наявність постанови про повернення виконавчого документа стягувачу. У разі неуспішної перевірки Підсистема повинна блокувати подання заяви та повідомити Користувача.
5. Після успішного подання заяви про поновлення виконавчого провадження Підсистема повинна надіслати її до органів, які здійснюють виконання рішень, та отримати відповідь про статус відправки.
6. Після успішної відправки заяви про поновлення виконавчого провадження Підсистема повинна присвоїти виконавчому документу процесуальний статус виконання «очікує прийняття до виконання».

5.4.4 Перегляд заяви про виконання рішення, заяви про повернення виконавчого документа та заяви про поновлення виконавчого провадження

1. Користувач може переглядати заяви про виконання рішення, заяви про повернення виконавчого документа та заяви про поновлення виконавчого провадження, а також пов'язані з ними документи.
2. В Підсистемі має бути реалізована можливість фільтрації та сортування доступних користувачу заяв про виконання рішення, заяв про повернення виконавчого документа та заяв про поновлення виконавчого провадження.
3. Користувач повинен мати можливість формувати заяви про виконання рішення, заяв про повернення виконавчого документа та заяви про поновлення виконавчого провадження у форматі PDF на основі актуальних структурованих даних.

4. Сформований PDF-документ повинен містити реквізити заяв та дані кваліфікованого електронного підпису, включаючи дані про підписувача, дату та час підписання.
5. У сформований PDF-документ повинні автоматично вбудовуватися QR-коди або штрих-коди, що містять унікальний ідентифікатор відповідної заяви або посилання на сервіс перевірки його автентичності в ЄДРВД.

5.4.5 Зміна статусу заяви на виконання рішення

1. Користувач, зазначений в реквізитах виконавчого документа як стягувач, повинен мати можливість відкликати створену раніше заяву про виконання рішення.
2. Відкликання заяви про виконання рішення має бути реалізовано шляхом зміни статусу заяви на «Відкликано».
3. Зміна статусу заяви про виконання рішення повинна підписуватися КЕП.
4. Після зміни статусу заяви про виконання рішення, Підсистема повинна надіслати до органів та осіб, які здійснюють виконання рішень, інформацію про зміну статусу заяви та присвоїти виконавчому документу статус «не пред'явлений до виконання».
5. Система повинна зберігати інформацію про всі зміни статусів заяв про виконання рішення.

5.5 Інтеграції

5.5.1 Внутрішні інтеграції

1. Підсистема повинна взаємодіяти з іншими підсистемами та функціональними компонентами ЄСІКС через компонент ЄСІКС «Електронна взаємодія» з метою використання їх функціональних можливостей та забезпечення узгодженої роботи складових Підсистеми. У разі якщо під час розроблення технічного завдання Виконавець визначить недоцільність використання компонента ЄСІКС «Електронна взаємодія» для окремих інтеграцій, таке рішення повинно бути належним чином обґрунтоване та погоджене із Власником Підсистеми.
2. Внутрішні інтеграції повинні забезпечувати обмін даними між Підсистемою та іншими підсистемами ЄСІКС, а також доступ до функціональних компонентів, зокрема компонентів роботи з документами, компоненту підписання електронних об'єктів, управління довідниковою інформацією, а також інших компонентів, передбачених архітектурою ЄСІКС.
3. Інтеграція між підсистемами повинна здійснюватися, зокрема, але не виключно, з використанням програмних інтерфейсів взаємодії (API) із забезпеченням контролю доступу, журналюванням та дотриманням вимог інформаційної безпеки.
4. Виконавець повинен забезпечувати складання, тестування та розгортання складових Підсистеми з використанням систем безперервної інтеграції та доставки, наданих Адміністратором Підсистеми: GitLab CI з використанням GitLab Runner та Argo CD. Магістралі (pipelines) складання та розгортання зберігаються в системі керування кодом GitLab і застосовуються автоматизовано окремо для кожного середовища (DEV/QA/STAGE/PROD).
5. У межах реалізації функціональності Підсистема повинна забезпечувати використання наступних внутрішніх підсистем та функціональних компонентів ЄСІКС, перелік яких не є вичерпним та може уточнюватися на етапі розробки технічного завдання, зокрема:
 - функціонального компонента «Керування доступом» управління ідентифікацією та доступом (IAM);
 - Єдиного персонального простору користувача;
 - функціональних компонентів для роботи з документами (Документ-сервіс);

- підсистеми Електронного документообігу суду;
- функціонального компонента «Підписання документів» (Крипто-сервіс);
- функціональних компонентів «Довідка та рекомендації», «База знань»;
- функціонального компонента «Довідники і класифікатори»;
- Майстер-реєстрів;
- функціонального компонента «Оркестрація» (BPMS);
- функціонального компонента «Нотифікації»;
- функціонального компонента «Аналіз та звітність»;
- функціонального компонента «Пошук і фільтри»;
- функціонального компонента «Логування»;
- функціонального компонента «Моніторинг»;
- функціонального компонента «Сканування та OCR»;
- функціонального компонента «Архів документів»;
- функціонального компонента «Конструктор відкритих даних»;
- функціонального компонента «Виявлення сутностей та тегування»;
- функціонального компонента «Сервіс-деск»;
- функціонального компонента «Календарі та завдання»;
- функціонального компонента «Електронна взаємодія»;
- функціонального компонента «Платежі».

5.5.1.1 Керування доступом (Управління ідентифікацією та доступом (IAM))

- Забезпечення ідентифікації користувачів, автентифікації, управління ролями та розмежування доступу до функціональних можливостей і даних Підсистеми здійснюється шляхом інтеграції з функціональним компонентом «Керування доступом» (Управління ідентифікацією та доступом (IAM)) ЄСІКС. Підсистема не реалізує власних механізмів керування користувачами або ролями, а перевикористовує функціональні можливості компонентів ЄСІКС.
- Підсистема повинна передбачати внутрішню інтеграцію з IAM для отримання та використання інформації про користувачів, зокрема:
 - ідентифікатора користувача;
 - ролей користувача;
 - юридичного статусу користувача;
 - атрибутів користувача;
 - належності користувача до організації;
 - членство в групах.
- Отримання зазначеної інформації забезпечується:
 - у складі токенів доступу, що містять ідентифікатори користувача та контекст доступу;
 - у режимі реального часу для перевірки ролей доступу до конкретної дії або ресурсу.
- Контроль доступу до функцій, довідників, реєстрів, документів і процедур Підсистеми здійснюється на основі даних, які використовуються в політиках доступу, зафіксованих в IAM і даних, що зберігаються в цій Підсистемі та інших складових ЄСІКС.
- Підсистема повинна забезпечувати використання механізму єдиного входу (Single Sign-On) та не вимагати повторної автентифікації користувача.
- Перевірка прав доступу до Підсистеми повинна забезпечуватись на основі:
 - ролей користувача;
 - атрибутів користувача;
 - юридичного статусу користувача;
 - участі користувача у виконавчому документі або відповідному бізнес-процесі (процесуальний статус користувача).

- Функціональний компонент IAM повинен забезпечувати для Підсистеми, зокрема, такі можливості:
 - централізовану ідентифікацію та автентифікацію користувачів ЄСІКС;
 - авторизацію користувачів;
 - делегування повноважень користувачів;
 - ведення списку організацій та груп користувачів;
 - визначення та зберігання ролей і повноважень користувачів;
 - призначення ролей користувачам відповідно до організаційної структури та повноважень;
 - ведення журналів безпеки та аудит дій користувачів у частині доступу.
- Адміністрування користувачів, ролей і прав доступу здійснюється засобами функціонального компонента IAM уповноваженими адміністраторами ЄСІКС.
- Підсистема повинна підтримувати використання результатів роботи IAM та забезпечувати коректну реакцію на зміну ролей, юридичного статусу користувачів або їх повноважень та атрибутів користувачів без дублювання відповідної логіки у власному функціоналі.
- Виконавцем повинно бути зпроектовано та зареєстровано в функціональному компоненті «Керування доступом» (Управління ідентифікацією та доступом (IAM)) ЄСІКС користувацькі ролі та політики доступу, які будуть відповідати технічній специфікації функціонального компонента «Керування доступом» (Управління ідентифікацією та доступом (IAM)) ЄСІКС. Технічна специфікація взаємодії буде надана Виконавцю на етапі розробки Технічного завдання.

5.5.1.2 Єдиний персональний простір користувача

1. Підсистема повинна взаємодіяти з користувачами ЄСІКС через Єдиний персональний простір користувача, який є єдиною точкою доступу користувачів до функціональних можливостей ЄСІКС.
2. В рамках розробки Підсистеми Виконавець не реалізує власний автономний кабінет користувача, а забезпечує реалізацію власних функціональних сценаріїв, сторінок, форм, таблиць, відображення та редагування даних для їх роботи в межах єдиного інтерфейсу Системи відповідно до вимог Єдиного персонального простору користувача.
3. Розробка інтерфейсів Підсистеми повинна здійснюватися Виконавцем з використанням централізованої дизайн-системи, спільних UI-компонентів та уніфікованих принципів UX/UI ЄСІКС без створення ізольованих або дублюючих інтерфейсних рішень.
4. Виконавець повинен забезпечити узгодження роботи Єдиного персонального простору користувача з функціональними можливостями Підсистеми.
5. Доступ до функцій Підсистеми має бути забезпечений через уніфіковані механізми навігації після того, як користувач обрав відповідний елемент в інтерфейсі Кабінету користувача.
6. Підсистемою можуть бути використані (за потреби) функціональні можливості профілю користувача, які забезпечуються Єдиним персональним простором користувача.
7. Підсистемою може бути використана можливість відображення у профілі користувача інформації, що стосується його взаємодії з виконавчими документами. Деталізація складу та обсягу такої інформації визначається на етапі розробки технічного завдання.
8. Підсистема не повинна зберігати дані про користувача, якщо такі дані отримуються з функціональних компонентів, а повинна використовувати їх шляхом інтеграційної взаємодії.

5.5.1.3 Функціональні компоненти для роботи з документами (Документ-сервіс)

1. Підсистема повинна бути інтегрована з функціональними компонентами ЄСІКС, призначеними для створення, формування, обробки, візуалізації, оцифрування та маркування документів (надалі – Документ-сервіс), для забезпечення роботи з документами, що створюються або використовуються в Підсистемі.
2. У межах інтеграції Підсистема повинна використовувати такі функціональні компоненти Документ-сервісу:
 - «Текстовий редактор»;
 - «Шаблонізатор»;
 - «Сканування та OCR»;
 - «PDF-генератор документів»;
 - «Генератор QR- та штрих-кодів».
- 2.1. Підсистема повинна бути інтегрована з функціональним компонентом «Текстовий редактор», який забезпечує створення, редагування та форматування текстових документів, у тому числі:
 - створення текстових документів (виконавчих документів, заяв та інших документів Підсистеми);
 - редагування документів до моменту їх підписання або набрання ними статусу, що унеможлиблює внесення змін;
 - автоматичне заповнення реквізитів документа даними, що містяться у Підсистемі;
 - використання довідників та класифікаторів Підсистеми під час формування документів;
 - форматування документів відповідно до затверджених шаблонів;
 - відображення актуального змісту документа під час його створення та редагування;
 - забезпечення збереження структурованих даних документа незалежно від його візуального представлення.
- 2.2. Підсистема повинна використовувати функціональний компонент «Шаблонізатор» для формування документів на основі затверджених шаблонів, зокрема:
 - створення та редагування шаблонів виконавчих документів та заяв із використанням вбудованих інструментів формування документів, з можливістю створення нових шаблонів або зміни існуючих;
 - централізоване збереження шаблонів із можливістю їх структурування за типами і категоріями документів;
 - використання окремих шаблонів для різних типів документів із можливістю автоматичного формування документів на основі наявних у Підсистемі даних;
 - динамічне підставлення структурованих даних у шаблони під час формування документів;
 - налаштування прав доступу до шаблонів для їх створення, редагування та використання відповідно до ролей користувачів;
 - підтримку версійності шаблонів із можливістю збереження історії змін, порівняння версій та відновлення попередніх варіантів;
 - забезпечення пошуку та фільтрації шаблонів за визначеними критеріями;
 - налаштування автоматичних сповіщень та нагадувань, пов'язаних з використанням або оновленням шаблонів;
 - використання шаблонів як основи для формування виконавчих документів та заяв у межах Підсистеми.
- 2.3. Компонент «Сканування та OCR» — забезпечує розпізнавання тексту з відсканованих або завантажених зображень і документів, зокрема:
 - розпізнавання тексту завантажених виконавчих документів та додатків;

- використання розпізнаного тексту для подальшого повнотекстового пошуку та автоматизованого виявлення сутностей у документі.
- 2.4 Підсистема повинна бути інтегрована з функціональним компонентом «PDF-генератор документів» для формування візуального представлення документів:
- формування PDF-документів на підставі структурованих даних;
 - забезпечення відповідності PDF-представлення структурованим даним документа;
 - формування PDF після внесення змін до документа;
 - підготовку документів до друку;
 - формування PDF-документів для експорту, надсилання та підписання.
- 2.5. Підсистема повинна бути інтегрована з функціональним компонентом «Генератор QR- та штрих-кодів» для забезпечення:
- автоматичного формування QR-коду або штрих-коду під час створення документа;
 - включення до QR-коду ідентифікатора документа або посилання на сервіс перевірки;
 - нанесення QR-коду на PDF-представлення документа;
 - використання QR-коду для швидкої ідентифікації документа;
 - використання штрих-кодів для автоматизації обробки документів у разі роботи з паперовими примірниками.
3. У разі, якщо на етапі розроблення технічного завдання буде встановлено, що використання окремого функціонального компонента Документ-сервісу є недоцільним для забезпечення функціональних вимог ЄДРВД, Виконавець повинен надати відповідне технічне обґрунтування. Виключення будь-якого функціонального компонента з переліку інтеграцій допускається виключно після погодження такого обґрунтування із Власником Підсистеми.

5.5.1.4 Підсистеми електронного документообігу суду

1. Підсистема ЄДРВД повинна бути інтегрована з наступними підсистемами електронного документообігу суду для автоматизованого отримання виконавчих документів:
 - Комп'ютерна програма «Д-3»;
 - Комп'ютерна програма «Діловодство спеціалізованого суду»;
 - Підсистема «Електронний документообіг суду» ЄСІКС;
 - Підсистема «Електронний кабінет».
2. Підсистема повинна забезпечувати отримання структурованих даних виконавчого документа, сформованого у відповідній підсистемі електронного документообігу суду, а також пов'язаних з ним документів та метаданих та передавати дані про результат реєстрації документа в ЄДРВД.
3. У межах реалізації інтеграції повинна бути передбачена перевірка коректності отриманих даних та фіксація інформації про джерело створення виконавчого документа — відповідна підсистема електронного документообігу суду.
4. Підсистема повинна забезпечувати передачу до відповідної Підсистеми електронного документообігу суду інформації про зміну процесуального стану виконання виконавчого документа, хід його виконання, а також інших відомостей, отриманих від органів та осіб, які здійснюють виконання рішень із забезпеченням однозначного встановлення зв'язку між виконавчим документом та судовою справою, у межах якої його сформовано.

5.5.1.5 Довідники і класифікатори

1. Підсистема повинна бути інтегрована з функціональним компонентом «Довідники та класифікатори», який призначений для ведення нормативно-довідкової інформації (НДІ) та централізованих реєстрів, а також забезпечення Підсистеми еталонними, юридично значущими даними, що виключають дублювання та розсинхронізацію з маскуванням процесів, які генерують ці дані.
2. Підсистема також повинна забезпечувати використання локальних статичних довідників, специфічних для предметної області Підсистеми, у випадках, коли такі довідники:
 - використовуються виключно в межах Підсистеми;
 - не мають загальносистемного характеру.
3. Локальні статичні довідники Підсистеми повинні мати чітке розмежування з централізованими довідниками та не дублювати їх зміст.
4. Підсистема повинна використовувати такі довідники:
 - класифікатор видів документів (у т.ч. виконавчих);
 - класифікатор процесуальних статусів учасників виконавчого процесу.
5. В межах Підсистеми користувач з відповідними правами повинен мати змогу переглядати загальний перелік довідників, що зареєстровані в Системі та їх вміст.
6. Значення довідників використовуються:
 - при заповненні структурованих полів форм;
 - для забезпечення уніфікованих значень атрибутів даних;
 - для відображення довідкової інформації в інтерфейсі користувача.
7. Детальний перелік довідників та їх значень має бути визначений на етапі розробки технічного завдання за погодженням із Власником Підсистеми.

5.5.1.6 Майстер-реєстри

1. Підсистема повинна бути інтегрована з Майстер-реєстрами, які призначені для централізованого зберігання та управління базовими обліковими сутностями ЄСІКС, що використовуються як джерело істини (Source of Truth) для інших підсистем ЄСІКС.
2. Інтеграція повинна забезпечувати використання Підсистемою уніфікованих даних про об'єкти та суб'єкти, що беруть участь у процесах життєвого циклу виконавчих документів.
3. Підсистема повинна використовувати такі майстер-реєстри:
 - класифікатор органів державної виконавчої служби;
 - класифікатор приватних виконавців.
4. У межах реалізації інтеграції Підсистема повинна забезпечувати:
 - використання облікових карток ключових об'єктів та суб'єктів обліку з відповідних майстер-реєстрів при створенні, реєстрації та обробки виконавчих документів;
 - використання єдиного унікального ідентифікатора для ідентифікації об'єктів та суб'єктів обліку;
 - забезпечення логічної зв'язності між виконавчими документами та відповідними записами в майстер-реєстрах (щодо сторін, зазначених у виконавчому документі, органів, що видали виконавчий документ, органів виконання рішень тощо);
 - використання інформації про представництво інтересів, що зберігається у майстер-реєстрах, для визначення можливості виконання користувачем дій від імені відповідних сторін, зазначених у виконавчому документі;
 - отримання актуальних даних та їх оновлення відповідно до визначеної бізнес-логіки;

- підтримку пошуку та вибору сутностей (фізичних осіб, юридичних осіб тощо) за ідентифікаторами або атрибутами при роботі користувачів із Підсистемою;
- врахування історичності змін у майстер-реєстрах під час роботи з виконавчими документами;
- дотримання встановлених правил розмежування доступів до даних майстер-реєстрів відповідно до ролей користувачів;
- використання уніфікованої моделі інтеграції для взаємодії з Сервісом майстер-реєстрів;
- врахування можливості реалізації прав суб'єктів персональних даних (доступ, уточнення, обмеження обробки, видалення), визначення строків їх зберігання, а також ведення аудиту операцій з такими даними відповідно до вимог законодавства України;
- використання базових принципів управління даними (Data Governance), включаючи визначення джерел достовірних даних, контроль їх якості, унікальності, узгодженості та відстеження змін. Політика управління даними (Data Governance) надається технічним адміністратором та має відповідати поточним вимогам системи ЄСІКС.

5.5.1.7 Оркестрація (BPMS)

1. Підсистема повинна забезпечувати можливість інтеграції з функціональним компонентом ЄСІКС «Оркестрація» (BPMS) для виконання, автоматизації та керування бізнес-процесами Підсистеми, а також координації взаємодії з функціональними компонентами та іншими підсистемами ЄСІКС та зовнішніми ІКС відповідно до визначених моделей процесів.
2. Під час розроблення технічного завдання Виконавець визначає перелік бізнес-процесів, сценаріїв взаємодії, подій, даних та правил їх виконання, що реалізуються із застосуванням функціонального компонента «Оркестрація» (BPMS) та повинен погодити цей перелік із Власником Підсистеми.
3. У разі, якщо під час розроблення технічного завдання Виконавець визначить недоцільність застосування функціонального компонента «Оркестрація» (BPMS) для окремих бізнес-процесів або для Підсистеми в цілому, він зобов'язаний надати технічне обґрунтування щодо такого рішення, запропонувати альтернативний спосіб реалізації відповідних бізнес-процесів та отримати погодження Власника і Замовника Підсистеми.
4. Інтеграція з функціональним компонентом «Оркестрація» (BPMS) повинна забезпечувати:
 - запуск та виконання бізнес-процесів Підсистеми відповідно до визначених моделей процесів;
 - автоматичне керування життєвим циклом виконавчих документів відповідно до подій, дій користувачів та результатів інформаційної взаємодії;
 - маршрутизацію виконання бізнес-процесів між функціональними компонентами та підсистемами ЄСІКС;
 - виконання автоматизованих дій, передбачених бізнес-процесами Підсистеми;
 - керування процесами, що передбачають участь користувачів, включаючи призначення, виконання та завершення завдань;
 - підтримку виконання довготривалих процесів, що передбачають очікування настання подій, отримання відповідей від зовнішніх інформаційно-комунікаційних систем або впливу визначених строків;
 - автоматичний запуск процесів у відповідь на події, що надходять від інших підсистем ЄСІКС та зовнішніх інформаційно-комунікаційних систем;

- обробку помилок виконання бізнес-процесів та підтримку механізмів повторного виконання або компенсації відповідно до визначених сценаріїв;
- ведення інформації про виконання бізнес-процесів для забезпечення моніторингу, аудиту та аналізу їх виконання.

5.5.1.8 Нотифікації користувачів

1. Підсистема повинна бути інтегрована з функціональним компонентом «Нотифікації», який забезпечує формування, відправлення та відображення повідомлень користувачам про події, що відбуваються у Підсистемі.
2. Підсистема повинна визначати події та умови їх виникнення, що є підставою для формування нотифікацій відповідно до бізнес-логіки Підсистеми.
3. Підсистема повинна забезпечувати формування та передачу подій до функціонального компонента «Нотифікації» із використанням визначених механізмів інтеграції (API або повідомлень через брокер).
4. Виконавцем повинні бути зпроектовані та зареєстровані в функціональному компоненті «Нотифікації» шаблони та сценарії доставки повідомлень, які будуть відповідати технічній специфікації функціонального компонента «Нотифікації» ЄСІКС. Технічна специфікація взаємодії та інструкція з використання будуть надані на етапі розробки технічного завдання.
5. Залежно від передумов для відправлення, нотифікації мають поділятися на:
 - Сервісні нотифікації:
 - критичні помилки;
 - помилки середнього рівня;
 - заплановані оновлення системи;
 - планові технічні роботи;
 - позапланові технічні роботи.

Крім того, сервісні нотифікації охоплюють будь-які підозрілі події або події з безпеки, що вимагають уваги та реагування адміністратора.

- Нотифікації про строки:
 - загальні нагадування про строки;
 - проміжні нагадування про строки;
 - критичні нагадування про строки;
 - строки для пред'явлення виконавчих документів.
 - Користувацькі нотифікації:
 - новий виконавчий документ;
 - зміна статусу виконавчого документа;
 - нове судове рішення яке є виконавчим документом;
 - зміна статусу заяви на примусове виконання рішення;
 - наближення кінцевого строку;
 - закінчення строку.
6. Детальний перелік подій в Підсистемі, які ініціюють створення нотифікацій, має бути визначений на етапі розробки технічного завдання за погодженням з Адміністратором Підсистеми.

5.5.1.9 Підписання документів (Крипто-сервіс)

1. Підсистема повинна бути інтегрована з функціональним компонентом «Підписання документів» (Крипто-сервіс) та використовувати його функціональні можливості для накладання та перевірки кваліфікованого та удосконаленого електронного підпису відповідно до вимог законодавства у сфері електронних довірчих послуг.

2. Інтеграція повинна забезпечувати використання централізованих механізмів підписання документів у межах ЄСІКС для формування та обробки електронних виконавчих документів та інших пов'язаних з ними електронних документів.
3. Підсистема повинна забезпечувати ініціювання процесу підписання з використанням:
 - системи електронного підпису ЄСІКС (Віджет підпису ЄСІКС);
 - системи електронного підпису id.gov.ua (Віджет підпису id.gov.ua).
4. У межах реалізації інтеграції повинно бути забезпечено:
 - накладання КЕП/УЕП на виконавчі документи та інші пов'язані електронні документи;
 - перевірку чинності та коректності електронних підписів під час створення, отримання або обробки документів;
 - отримання та збереження результатів перевірки КЕП/УЕП у складі метаданих документа;
 - забезпечення цілісності та незмінності підписаних електронних документів.

5.5.1.10 Довідка та рекомендації. База знань

1. Підсистема повинна бути інтегрована з функціональними компонентами «Довідка та рекомендації», «База знань», які забезпечують централізоване управління інформаційними матеріалами про роботу Підсистеми, зокрема статтями, довідками, інструкціями для користувачів та відповідями на поширені запитання (FAQ).
2. Виконавець повинен забезпечити наповнення бази знань інформаційними матеріалами щодо роботи Підсистеми, зокрема, створення та підтримку довідкових матеріалів, інструкцій для користувачів, а також формування структури їх взаємозв'язків та використання для надання контекстних підказок і навчальних матеріалів.
3. Інтеграція повинна забезпечувати надання користувачам ЄДРВД доступу до актуальної довідкової інформації безпосередньо в інтерфейсі Підсистеми.
4. У межах реалізації інтеграції повинно бути забезпечено:
 - використання централізованої бази знань, що містить нормативно-правові акти, інструкції, методичні матеріали, роз'яснення та інші інформаційні ресурси, необхідні для роботи з виконавчими документами;
 - відображення релевантних довідкових матеріалів безпосередньо в інтерфейсі Підсистеми під час виконання користувачами відповідних операцій;
 - надання контекстних інтерактивних підказок під час виконання дій у системі або під час заповнення форм;
 - забезпечення доступу до поширених запитань (FAQ), покрокових інструкцій та навчальних матеріалів;
 - каталогізацію матеріалів бази знань за категоріями, темами та типами документів для зручного пошуку та використання;
 - підтримку різних рівнів доступу до матеріалів бази знань відповідно до ролей користувачів;
 - можливість для уповноважених користувачів додавати нові матеріали або оновлювати існуючі записи бази знань;
 - відстеження змін у довідкових матеріалах із фіксацією інформації про дату та автора змін;
 - можливість пошуку інформації за ключовими словами, фразами, синонімами та частковим збігом слова;
 - можливість експорту або друку довідкових матеріалів у форматі PDF або інших форматах.

5. База знань повинна забезпечувати постійне оновлення та підтримку актуальності довідкових матеріалів, зокрема з урахуванням змін у законодавстві або судовій практиці.

5.5.1.11 Аналіз та звітність

1. Підсистема повинна бути інтегрована з функціональним компонентом «Аналіз та звітність» ЄСІКС, який забезпечує створення, візуалізацію та аналіз звітів на основі даних ЄДРВД.
2. Інтеграція повинна забезпечувати передачу структурованих даних ЄДРВД до функціонального компонента «Аналіз та звітність» для формування статистичних, аналітичних та управлінських звітів, а також для візуалізації відповідної інформації у вигляді аналітичних панелей.
3. На рівні функціонального компонента «Аналіз та звітність» повинно бути забезпечено:
 - генерацію типових та нетипових звітів з можливістю налаштування параметрів формування звітності;
 - формування аналітичних та статистичних звітів на основі даних ЄДРВД;
 - побудову звітів за реквізитами виконавчих документів та іншими параметрами з можливістю групування даних за визначеними критеріями, включаючи вид боржника, ознаку належності боржника до державного сектору/державної форми власності, орган, що видав виконавчий документ та суму коштів, що підлягає стягненню;
 - налаштування та повторне використання типових форм звітів;
 - експорт сформованих звітів у різних форматах, зокрема PDF, Excel або CSV;
 - формування спеціалізованих звітів на запит користувачів, у тому числі звіту/аналітичного представлення щодо загальної суми коштів, що підлягає стягненню за виконавчими документами, виданими на підставі рішень національних судів, у яких боржником є держава, державний орган, державна установа, державна організація або державне підприємство;
 - аналіз поточних даних ЄДРВД, зокрема інформації про виконавчі документи, їх статуси, суми стягнення, сторони/учасників та інші параметри;
 - налаштування інформаційних панелей (дашбордів) для візуалізації аналітичних звітів та узагальнення інформації;
 - відображення аналітичних даних у вигляді графіків, гістограм, діаграм та інших інструментів візуалізації.
4. Звіти повинні формуватися, зокрема, на основі таких даних ЄДРВД:
 - кількість користувачів Реєстру;
 - кількість опрацьованих виконавчих документів;
 - кількість стягувачів;
 - кількість боржників;
 - кількість виконавців;
 - суми заборгованості (у тому числі заборгованість державних органів);
 - суми стягнення за результатами виконання рішень;
 - типи боржників;
 - інші статистичні та аналітичні показники, що формуються на основі даних ЄДРВД.

5.5.1.12 Платежі

1. Підсистема повинна бути інтегрована з функціональним компонентом «Платежі» ЄСІКС у частині забезпечення ініціювання платежів користувачами та отримання результату обробки таких платежів.

2. Інтеграція повинна забезпечувати обмін інформацією щодо фінансових операцій, пов'язаних із виконанням виконавчих документів у випадках, передбачених законодавством.
3. У складі Підсистеми повинен бути реалізований (створений) реєстр платежів за виконавчими документами, який забезпечує зберігання, облік та обробку інформації про платежі залежно від джерела їх походження (ініційовані в Підсистемі, отримані від Казначейства та його територіальних органів, отримані від АСВП).
4. У межах реалізації інтеграції повинно бути забезпечено:
 - можливість ініціювання користувачем оплати за виконавчим документом через інтерфейс Підсистеми з використанням компонента «Платежі»;
 - передачу компонента «Платежі» необхідних платіжних даних, сформованих на підставі виконавчого документа та пов'язаних із ним даних;
 - отримання від компонента «Платежі» інформації про стан обробки платежу (зокрема щодо його прийняття, виконання або відхилення);
 - перевірку унікальності платежу на підставі його ідентифікатора та джерела походження перед збереженням у реєстрі платежів з метою запобігання подвоюванню даних;
 - отримання та збереження підтверджуючих документів (квитанцій) від компонента «Платежі» (у разі можливості);
 - отримання та обробку інформації про здійснені платежі, пов'язані з виконанням виконавчих документів;
 - дотримання вимог інформаційної безпеки та захисту даних під час обробки платіжної інформації.

5.5.1.13 Пошук і фільтри

1. Підсистема повинна використовувати функціональний компонент «Пошук і фільтри» для забезпечення повнотекстового та структурованого пошуку за даними Підсистеми, побудови та підтримки пошукових індексів у стані, синхронізованому з основним сховищем даних, а також формування результатів пошуку з урахуванням релевантності. Компонент використовується для реалізації функцій пошуку виконавчих документів, реєстраційних карток та інших об'єктів Підсистеми, для яких необхідна швидка вибірка за множинними критеріями.
2. Підсистема повинна забезпечувати передавання даних до компонента «Пошук і фільтри» для індексації через подієво-орієнтований механізм із використанням Брокера повідомлень (п. 7.8) для забезпечення слабкої пов'язаності та відмовостійкості процесу індексації, із гарантією доставки подій, автоматичними повторними спробами їх обробки та переміщенням подій, які не вдалося обробити, до окремої черги невдалих повідомлень із подальшим сповіщенням. Недоступність або деградація компонента «Пошук і фільтри» не повинна блокувати роботу Підсистеми: у такому випадку недоступною стає виключно функція пошуку, тоді як створення та зміна даних продовжується у штатному режимі, а накопичені події повинні бути проіндексовані після відновлення роботи компонента.
3. Підсистема повинна взаємодіяти з компонентом «Пошук і фільтри» через уніфікований програмний інтерфейс виконання пошукових запитів, який є контрактом взаємодії між Підсистемою та компонентом і не повинен транслювати безпосередньо інтерфейс запитів конкретного пошукового рушія. Програмний інтерфейс повинен підтримувати версіонування. Прямий доступ Підсистеми до пошукового рушія в обхід зазначеного програмного інтерфейсу не допускається.
4. Підсистема повинна забезпечувати використання експлуатаційних метрик, що формуються компонентом «Пошук і фільтри» та передаються до функціонального компонента «Моніторинг», зокрема:
 - час виконання пошукового запиту за перцентилями (p50, p95, p99);

- розмір індексу та кількість проіндексованих об'єктів;
 - глибина черги індексації та фактична затримка індексації;
 - кількість помилок індексації та пошуку;
 - стан вузлів кластера і реплік індексу.
5. Підсистема повинна забезпечувати використання інформації про події та помилки індексації, що передаються компонентом «Пошук і фільтри» до функціонального компонента «Логування», із зазначенням ідентифікатора об'єкта та причини помилки, достатніх для повторної обробки.
 6. Підсистема повинна забезпечувати застосування актуальних прав доступу користувачів під час виконання пошукових запитів. Зміна прав доступу користувача у функціональному компоненті «Керування доступом» (Управління ідентифікацією та доступом (IAM)) повинна відображатися у результатах пошуку без необхідності повторної індексації даних у строк, що не перевищує строку поширення змін прав доступу, визначеного для Підсистеми загалом.
 7. Технічна специфікація взаємодії та інструкція з використання будуть надані Виконавцю на етапі розробки технічного завдання.

5.5.1.14 Логування

1. Підсистема повинна використовувати функціональний компонент ЄСІКС «Логування» як централізоване сховище для агрегації логів з усіх шарів Підсистеми (інфраструктура, бази даних, функціональні компоненти, прикладне програмне забезпечення), що містять інформацію про технічні події. Компонент використовується як первинне джерело даних для пошуку помилок, технічної діагностики та аналізу роботи Підсистеми.
2. Підсистема повинна забезпечувати передавання до функціонального компонента «Логування» технічних подій із використанням відкритих стандартів збору та передачі даних.
3. Підсистема повинна забезпечувати передавання до функціонального компонента «Логування» журналів подій без персональних даних або з урахуванням їх автоматичного знеособлення до моменту збереження відповідно до правил, визначених компонентом.
4. Підсистема повинна забезпечувати передавання до функціонального компонента «Логування» інформації про юридично значущі події, дії користувачів і адміністраторів, зміни даних та зміну станів бізнес-об'єктів, що здійснюються в межах Підсистеми.
5. Підсистема повинна використовувати функціональний компонент «Логування» для формування доказової бази щодо дій, виконаних у Підсистемі, з метою забезпечення внутрішнього контролю, інформаційної безпеки, службових перевірок, розслідування інцидентів та виконання вимог законодавства.
6. Підсистема повинна забезпечувати використання функціональних можливостей компонента «Логування» для:
 - отримання історії дій користувачів;
 - отримання історії змін конкретних об'єктів Підсистеми;
 - фільтрації записів за періодом, типом дії, користувачем, об'єктом та результатом виконання;
 - використання пагінації та сортування результатів;
 - відображення журналів аудиту в інтерфейсах Підсистеми відповідно до наданих прав доступу;
 - експорту записів аудиту у форматах CSV та JSON/CEF у випадках, передбачених законодавством або технічними вимогами.

7. Підсистема повинна взаємодіяти з функціональним компонентом «Логування» через стандартизований механізм передачі подій аудиту із використанням уніфікованого формату даних (JSON).
8. Підсистема повинна використовувати функціональний компонент «Керування доступом» (Управління ідентифікацією та доступом (IAM)) для отримання ідентифікаційних атрибутів користувачів, що передаються разом із подіями аудиту до функціонального компонента «Логування».
9. Підсистема повинна забезпечувати контроль доступу до журналів аудиту відповідно до ролей користувачів, визначених функціональним компонентом «Керування доступом» (Управління ідентифікацією та доступом (IAM)). Зміна або видалення записів аудиту засобами Підсистеми не допускається.
10. Підсистема повинна забезпечувати синхронізацію часових позначок подій відповідно до єдиного джерела часу ЄСІКС для забезпечення коректної кореляції подій між компонентами Системи.
11. Технічна специфікація взаємодії та інструкція з використання функціонального компонента «Логування» будуть надані Виконавцю на етапі розробки технічного завдання.

5.5.1.15 Моніторинг

1. Підсистема повинна використовувати функціональний компонент ЄСІКС «Моніторинг» для контролю працездатності Підсистеми (Health Checks), моніторингу її технічного стану, навантаження, а також візуалізації експлуатаційних показників і формування оперативних сповіщень.
2. Підсистема повинна забезпечувати інтеграцію з функціональним компонентом «Моніторинг» шляхом передавання експлуатаційних метрик та використання даних функціонального компонента «Логування» для аналізу частоти помилок.
3. Підсистема повинна реалізувати програмний інтерфейс /health відповідно до технічної специфікації функціонального компонента «Моніторинг» для забезпечення автоматизованої перевірки працездатності компонентів Підсистеми.
4. Підсистема повинна забезпечувати передавання до функціонального компонента «Моніторинг» базових експлуатаційних метрик, зокрема:
 - часу відповіді (Latency);
 - кількості помилок (Error Rate);
 - кількості запитів (Throughput);
 - інших метрик, визначених на етапі розроблення технічного завдання.
5. Технічна специфікація взаємодії та інструкція з використання функціонального компонента «Моніторинг» будуть надані Виконавцю на етапі розробки технічного завдання.

5.5.1.16 Архів документів

1. Підсистема повинна бути інтегрована з функціональним компонентом «Архів документів» для довгострокового зберігання виконавчих документів, пов'язаних з ними електронних документів, матеріалів, додатків та їх метаданих після завершення відповідних бізнес-процесів або життєвого циклу документів.
2. Підсистема повинна забезпечувати передачу до компонента «Архів документів» електронних виконавчих документів, пов'язаних процесуальних документів, додатків, електронних підписів, реєстраційних відомостей та інших метаданих, необхідних для формування архівної електронної справи.
3. Передача документів до компонента «Архів документів» повинна здійснюватися із забезпеченням цілісності даних, збереження зв'язків між документами, їх версіями, реквізитами та історією проходження.

4. Підсистема повинна забезпечувати можливість отримання від компонента «Архів документів» інформації про результати архівування документів, їх архівний статус, дату архівування та інші відомості, необхідні для відображення у Підсистемі.
5. Підсистема повинна забезпечувати можливість отримання архівних документів та їх метаданих із компонента «Архів документів» для перегляду авторизованими користувачами відповідно до їх ролей та прав доступу.
6. У разі переведення виконавчого документа або пов'язаних матеріалів до архіву Підсистема повинна відображати актуальний статус архівування та забезпечувати доступ до архівної копії через функціональний компонент «Архів документів».
7. Підсистема повинна забезпечувати передачу до компонента «Архів документів» інформації, необхідної для визначення строків зберігання документів відповідно до вимог законодавства та затверджені номенклатури справ.
8. Підсистема повинна отримувати від компонента «Архів документів» інформацію про завершення строків зберігання, знищення архівних документів або інші події, що впливають на життєвий цикл виконавчого документа, та відображати відповідні відомості у Підсистемі.
9. Технічна специфікація взаємодії та інструкція з використання будуть надані Виконавцю на етапі розробки технічного завдання.

5.5.1.17 Конструктор відкритих даних

1. Підсистема повинна бути інтегрована з функціональним компонентом «Конструктор відкритих даних», призначеним для оприлюднення в автоматичному режимі наборів відкритих даних на Єдиному державному вебпорталі відкритих даних за допомогою механізму отримання інформації з баз даних Підсистеми та формування архіву зі структурованими даними відповідно до вимог чинного законодавства.
2. Технічна специфікація взаємодії та інструкція з використання будуть надані Виконавцю на етапі розробки технічного завдання.

5.5.1.18 Виявлення сутностей та тегування

1. Підсистема повинна бути інтегрована з функціональним компонентом «Виявлення сутностей та тегування», призначеним для автоматичного аналізу текстового вмісту виконавчих документів, пов'язаних процесуальних документів та інших інформаційних об'єктів, що обробляються Підсистемою.
2. Підсистема повинна забезпечувати передачу до компонента «Виявлення сутностей та тегування» текстового вмісту документів та необхідних метаданих для автоматичного виявлення, класифікації сутностей і формування тегів.
3. Підсистема повинна забезпечувати отримання результатів автоматичного аналізу тексту, зокрема переліку виявлених сутностей, їх категорій, значень, координат у тексті (за наявності) та сформованих тегів.
4. Підсистема повинна забезпечувати можливість використання отриманих від компонента тегів та виявлених сутностей під час пошуку, фільтрації, класифікації та групування виконавчих документів і пов'язаних з ними інформаційних об'єктів.
5. Підсистема повинна забезпечувати можливість підтвердження, відхилення або коригування користувачем результатів автоматичного виявлення сутностей та автоматично сформованих тегів відповідно до наданих прав доступу.
6. Підсистема повинна забезпечувати повторне направлення документів на аналіз у разі зміни їх змісту або за ініціативою користувача відповідно до бізнес-процесів Підсистеми.
7. Підсистема повинна забезпечувати можливість використання централізовано створених тегів, а також отримання актуального переліку тегів із функціонального

компонента «Виявлення сутностей та тегування» без реалізації власного механізму їх ведення.

8. Підсистема повинна забезпечувати використання тегів під час формування пошукових запитів, вибірок документів, фільтрів та інших механізмів навігації по інформаційних ресурсах Підсистеми.
9. Підсистема повинна забезпечувати передачу інформації про присвоєні або змінені теги до компонента «Виявлення сутностей та тегування» у випадках, коли зміна тегів здійснюється користувачем відповідно до наданих повноважень.
10. Технічна специфікація взаємодії та інструкція з використання будуть надані Виконавцю на етапі розробки технічного завдання.

5.5.1.19 Сервіс-деск

1. Підсистема повинна бути інтегрована з функціональним компонентом «Сервіс-деск», призначеним для автоматизація процесів підтримки внутрішніх та зовнішніх користувачів Підсистеми, реєстрації їх звернень, управління інцидентами та проблемами.
2. Технічна специфікація взаємодії та інструкція з використання будуть надані Виконавцю на етапі розробки технічного завдання.

5.5.1.20 Календарі та завдання

1. Підсистема повинна використовувати функціональний компонент ЄСІКС «Календарі та завдання» для автоматичного створення, відображення та супроводу календарних подій, дедлайнів і завдань, пов'язаних із бізнес-процесами Підсистеми.
2. Підсистема повинна забезпечувати автоматичне створення календарних об'єктів у компоненті «Календарі та завдання» внаслідок настання визначених бізнес-подій, зокрема:
 - реєстрації виконавчого документа;
 - пред'явлення виконавчого документа до виконання;
 - зміни процесуального статусу виконавчого документа;
 - настання або обчислення процесуальних строків;
 - інших подій, визначених бізнес-процесами Підсистеми.
3. Підсистема повинна забезпечувати передачу до компонента «Календарі та завдання» інформації, необхідної для формування календарних подій, дедлайнів та завдань, зокрема відомостей про дату, час, строк виконання, відповідальних осіб, опис події, пов'язані виконавчі документи та інші метадані.
4. Підсистема повинна забезпечувати отримання від компонента «Календарі та завдання» інформації про створені календарні об'єкти, їх поточний стан, строки виконання та інші відомості, необхідні для відображення у Підсистемі.
5. Підсистема повинна забезпечувати можливість переходу користувача від календарного об'єкта до відповідного виконавчого документа або іншого інформаційного об'єкта Підсистеми з урахуванням ролей та прав доступу користувача.
6. Підсистема повинна забезпечувати використання календарних подій та дедлайнів для контролю процесуальних строків, строків пред'явлення виконавчих документів до виконання та інших строків, визначених законодавством або бізнес-процесами Підсистеми.
7. Підсистема повинна забезпечувати використання компонента «Календарі та завдання» для формування персональних завдань користувачів, якщо виконання відповідних дій передбачено бізнес-процесами Підсистеми.

8. Підсистема повинна забезпечувати використання відомостей про календарні події та дедлайни під час формування повідомлень користувачам із застосуванням функціонального компонента «Нотифікації користувачів».
9. Технічна специфікація взаємодії та інструкція з використання будуть надані Виконавцю на етапі розробки технічного завдання.

5.5.1.21 Електронна взаємодія

1. Підсистема повинна бути інтегрована з функціональним компонентом «Електронна взаємодія», призначеним для забезпечення процесів управління електронною взаємодією між Підсистемою та інформаційними, інформаційно-комунікаційними системами, реєстрами, базами даних державних органів, органів місцевого самоврядування, суб'єктів господарювання тощо.
2. Технічна специфікація взаємодії та інструкція з використання будуть надані Виконавцю на етапі розробки технічного завдання.

5.5.2 Зовнішні інтеграції

1. Підсистема повинна бути інтегрована з АСВП для забезпечення можливості пред'явлення виконавчого документа до виконання та отримання актуальних статусів виконавчих документів.
2. Підсистема повинна бути інтегрована з ІКС Державної казначейської служби України (за технічної можливості) для забезпечення можливості передачі (подання) виконавчих документів на виконання до Державної казначейської служби, а також моніторингу та контролю виконання виконавчих документів, в яких державні органи, державні установи або державні підприємства є боржниками.
3. Підсистема повинна надавати API для інтеграції з ІКС органів та установ, які уповноважені видавати виконавчі документи та/або уповноважені на внесення виконавчих документів до ЄДРВД, для забезпечення можливості автоматичного створення виконавчих документів в Підсистемі.
4. Підсистема повинна бути інтегрована з мобільним додатком Єдиного державного вебпорталу електронних послуг (Дія) для забезпечення можливості доступу користувачів до інформації про виконавчі документи та процесуальний стан їх виконання, отримання повідомлень, а також ініціювання дій щодо таких документів у межах функціональних можливостей такої системи.

6. НЕФУНКЦІОНАЛЬНІ ВИМОГИ

Архітектура Підсистеми та нефункціональні вимоги мають виключати технологічну залежність від конкретного постачальника хмарних або інфраструктурних сервісів та відповідати загальним архітектурним принципам ЄСІКС.

Підсистема повинна мати можливість розгортання в середовищі інфраструктури ЄСІКС або інфраструктури будь-якого постачальника без зміни прикладної логіки.

Не допускається використання пропріетарних керованих сервісів (managed services), які:

- не мають функціонально еквівалентних self-hosted реалізацій;
- потребують використання специфічних API, SDK або механізмів керування, прив'язаних до конкретного постачальника;
- унеможливають або істотно ускладнюють міграцію Підсистеми до альтернативного інфраструктурного середовища.

Зазначене обмеження не стосується використання стандартних протоколів, відкритих API та загальноприйнятих галузевих стандартів, незалежних від конкретного постачальника.

6.1 Вимоги до чисельності та кваліфікації персоналу, залученого до експлуатації та супроводу Підсистеми

Експлуатація Підсистеми має забезпечуватися персоналом Адміністратора Підсистеми та/або уповноваженої організації відповідно до цих технічних вимог та чинних нормативно-правових актів України.

Виконавець має запропонувати та погодити з Адміністратором Системи мінімальну чисельність ролей, наведених нижче, але не обмежуючись ними, необхідних для забезпечення штатного функціонування та підтримки засобу інформатизації у наведеному нижче форматі:

Функціональні вимоги до персоналу	Чисельність (людино-місяці)
Фахівець з управління проєктами та програмами (менеджер продукту)	
Аналітик процесів автоматизації (бізнес-аналітик)	
Фахівець з розробки та тестування програмного забезпечення (розробник)	
Фахівець з розробки та тестування програмного забезпечення (QA інженер)	
Інженер із впровадження нової техніки і технології (інженер підтримки)	
Дизайнер (інформаційні технології) (UX/UI Дизайнер)	
Інженер з інтеграції (DevOps інженер)	

Детальні вимоги до кваліфікації працівників, що забезпечують штатну функціональність засобу інформатизації має бути остаточно визначено в ТЗ базуючись на вибраних технологічних рішеннях.

6.2 Вимоги до безпеки

Продуктивне (PROD) середовище та NON-PROD середовище повинні бути відокремлені. У назвах об'єктів в різних середовищах слід використовувати префікси або суфікси, які однозначно вказують на середовище, до якого належить об'єкт.

Підсистема повинна відповідати сучасним міжнародним стандартам інформаційної безпеки, встановленим для ЄСІКС, включаючи NIST SP 800-63B та NIST SP 800-53.

Для раннього виявлення вразливостей у програмному коді розробниками на етапі розробки потрібно застосовувати інструменти SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing), які надаються Власником Системи.

Підсистема має передбачати механізми захисту від найбільш поширених типів атак, передбачених OWASP Топ 10.

Інформація в повідомленнях зовнішнім сторонам про помилки в Підсистемі не має відображати технічні подробиці складу та версії Підсистеми.

На фізичному рівні мають бути виконані наступні правила:

1. Фізичний доступ до обладнання повинен бути обмеженим та усі дії повинні бути зафіксовані.
2. Фізичний доступ до резервних копій системи повинен бути обмеженим відповідно до регламенту адміністрування системи та усі дії повинні бути зафіксованими.
3. Підсистема повинна мати функціонал для обмеження кількості запитів до неї з метою захисту від перевантаження.
4. Підсистема має успішно пройти тестування на наявність вразливостей за допомогою інструмента, наданого Власником Системи у режимах (у разі наявності):
 - 4.1. Без автентифікованого Користувача;
 - 4.2. З автентифікованим Користувачем.

За результатами такого тестування мають бути сформовані протокол тестування та звіт щодо відсутності та/або наявності вразливостей. У випадку наявності критичних вразливостей (пріоритет high та вище) — Виконавець має надати роз'яснення, план дій та виконати дії з усунення або мінімізації впливу виявлених вразливостей Підсистеми. Після виконання дій з усунення або мінімізації впливу виявлених вразливостей у Підсистемі мають бути відсутні вразливості рівня high та вище.

Підсистема повинна підтримувати використання стандартних шаблонів безпечної конфігурації та готових образів для розгортання операційних систем, обладнання, програмного забезпечення, додаткових сервісів, необхідних для штатного функціонування Підсистеми.

Підсистема повинна функціонувати з урахуванням логічної ізоляції від інших сервісів, що функціонують в межах спільної інфраструктури ЄСІКС.

Для забезпечення роботи адміністраторів та користувачів із Підсистемою формуються і використовуються типові рольові моделі кінцевих адміністраторів/користувачів, що визначаються на рівні Підсистеми, з персоналізованим інтерфейсом та визначеним набором операцій відповідно до ролей і повноважень

адміністраторів/користувачів. Набір дозволених операцій та доступних об'єктів в межах окремої ролі має формуватися керуючись наступними принципами інформаційної безпеки: «необхідність знати» (тобто суб'єкту надається доступ лише до тієї інформації, яка необхідна йому для виконання своїх завдань) та «необхідність у використанні» (тобто суб'єкту надається доступ до інформаційно-технологічної інфраструктури лише тоді, коли в цьому є чітко визначена потреба). Виконавцем повинно бути спроектовано та зареєстровано в базовому сервісі управління ідентифікацією та доступом (IAM) ЄСІКС користувацькі ролі та політики доступу, які будуть відповідати технічній специфікації базового сервісу управління ідентифікацією та доступом (IAM) ЄСІКС. Технічна специфікація взаємодії буде надана Виконавцю на етапі розробки Технічного завдання.

Підсистема має працювати тільки з конфіденційною інформацією за рівнем класифікації відповідно до статті 21 Закону України «Про інформацію». Відповідно до п. 5.1 КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ в Концепції ЄСІКС, інформація з грифами «ДСК» або «таємно» не обробляється в Підсистемі. Відповідальність за недопущення внесення такої інформації покладається на користувачів, які повинні бути належним чином проінструктовані.

Підсистема може підтримувати взаємодію з офіційними сервісами, які надають інформацію про IP адресу та власними локальними базами даних IP адрес, з можливістю налаштування інформування адміністраторів адресних зон про виявлену зону, з якої здійснюється доступ до Підсистеми.

Підсистема не реалізує функціонал автентифікації користувачів і використовує механізми автентифікації, що забезпечуються функціональним компонентом IAM на рівні Системи, зокрема на основі логіну та паролю, коду мультифакторної автентифікації (опціонально та обов'язково для визначеного переліку користувачів — наприклад, адміністраторів організацій, адміністраторів користувачів тощо) або через КЕП.

6.3 Вимоги до ергономіки та технічної естетики

Кінцеві користувачі отримують доступ до Підсистеми через інтерфейс Єдиного персонального простору ЄСІКС. Підсистема не реалізує власний автономний кабінет користувача, а надає функціональні можливості та дані для відображення в межах єдиного інтерфейсу Системи. Після переходу з Єдиного персонального простору користувача взаємодія користувача з Підсистемою здійснюється через вебінтерфейс Підсистеми, інтегрований з Єдиним персональним простором ЄСІКС. Спосіб інтеграції інтерфейсів визначається на етапі розробки технічного завдання з урахуванням вимог до користувацького досвіду та архітектурних обмежень.

Вебінтерфейс Підсистеми повинен формуватися з урахуванням ролей, прав доступу та юридичного статусу користувача, отриманих із сервісу «Керування доступом» (Управління ідентифікацією та доступом (IAM)), та забезпечувати відображення доступного користувачеві функціоналу відповідно до його повноважень.

Підсистема повинна надавати користувачеві гнучкі механізми персоналізації її інтерфейсу, збереження користувацьких налаштувань та стану інтерфейсу, адаптації інтерфейсу відповідно до ролей та прав доступу тощо. Підсистема повинна дозволяти налаштовувати свою функціональність під конкретні потреби користувачів, що можуть змінюватися, без необхідності звернення до розробників програмного забезпечення. Деталізація вимог щодо такого механізму має бути проведена в технічному завданні.

З метою погодження концепції взаємодії користувача та основних інтерфейсних рішень, Виконавець повинен забезпечити розробку клікабельного прототипу, який

покриває один або декілька ключових сценаріїв використання інтерфейсу Підсистеми. Такі прототипи повинні відображати основні сценарії взаємодії користувача, поведінку ключових UI-компонентів, структуру інтерфейсу, логіку навігації. Прототипи повинні бути перевірені на відповідність бізнес-процесам та представлені кінцевим користувачам для збору зворотного зв'язку. За результатами такого тестування Виконавець може внести відповідні корективи. Прототипи підлягають погодженню Власником Підсистеми до початку реалізації відповідного функціоналу.

Інші елементи інтерфейсу та сторінки Підсистеми можуть бути представлені у вигляді статичних прототипів або макетів та погоджуватися у робочому порядку без обов'язкового створення клікабельного прототипу.

Розробка інтерфейсів Підсистеми повинна здійснюватися з використанням затвердженої дизайн-системи ЄСІКС. Деталізація вимог до прототипування та перелік сценаріїв визначаються на етапі розробки технічного завдання.

Усі компоненти інтерфейсу Підсистеми мають бути спроектовані відповідно до останньої версії WCAG на момент реалізації.

Підсистема повинна мати можливість запуску і роботи вебінтерфейсу використовуючи браузер Microsoft Edge, Safari або Google Chrome найсучаснішої версії на момент проведення випробувань Підсистеми.

Вебінтерфейс повинен бути адаптивним та забезпечувати коректне відображення і функціональну доступність на різних типах пристроїв, зокрема, на настільному комп'ютері та на мобільному пристрої користувача (планшет, ноутбук, смартфон) з урахуванням особливостей їх екранів та способів взаємодії.

6.4 Вимоги до захисту інформації

Захист інформації, яка оброблятиметься в Підсистемі, повинен здійснюватися шляхом створення, оновлення та забезпечення функціонування системи захисту інформації (далі – СЗІ):

- або шляхом створення Підсистеми з використанням базових та цільових профілів безпеки, вибір заходів захисту яких відповідає вимогам НД ТЗІ 3.6-006-24, що є перекладом NIST Cybersecurity Framework (далі – профіль безпеки);
- або впровадження системи управління інформаційною безпекою відповідно до вимог національного стандарту України з питань інформаційної безпеки ДСТУ ISO/IEC 27001:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги», який прийнято наказом Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 17.08.2023 № 210.

Метою створення СЗІ є забезпечення конфіденційності, цілісності, спостережності та доступності (відповідно до наданих повноважень) інформації, яка циркулює в Підсистемі.

Остаточні вимоги до СЗІ будуть частиною окремого технічного завдання на побудову СЗІ для Підсистеми.

Інфраструктура, на якій функціонуватиме Підсистема, має забезпечувати щонайменше:

- виявлення та блокування комп'ютерних атак і несанкціонованої мережевої активності;

- фільтрацію та аналіз мережевого трафіку за протоколами, портами та IP-адресами відправника й одержувача;
- захист програмного забезпечення від зовнішніх загроз, внутрішнього несанкціонованого доступу, зловмисного програмного забезпечення та хакерських атак;
- завершення з'єднання з атакуючими вузлами у разі виявлення спроби атаки;
- протоколювання (реєстрація) подій, що мають відношення до кібербезпеки.

6.5 Вимоги до уніфікації

Підсистема повинна забезпечувати стандартизацію та уніфікацію функцій шляхом використання сучасних інструментальних програмних засобів, що підтримують єдину технологію проєктування, розробки та супроводу функціонального, інформаційного та програмного забезпечення.

Архітектура Підсистеми повинна будуватися на уніфікованих принципах проєктування та реалізації програмних компонентів, відповідати єдиному архітектурному підходу та наслідувати загальноприйняті патерни поведінки Системи.

Підсистема та всі програмні компоненти повинні відповідати чинним міжнародним угодам, національним нормативно-правовим актам та стандартам у сфері ІТ.

Підсистема має підтримувати вимоги стандартів даних/сумісності, зокрема забезпечувати обробку та зберігання даних у форматах кодування ASCII та Unicode (UTF-8), забезпечуючи коректну роботу з текстовими даними різними мовами та символами.

Для розробки документації етапу розробки програмного забезпечення мають бути застосовані міжнародні стандарти створення і розвитку інформаційних засобів, закладені в «Обов'язкових вимогах до створення (модернізації, модифікації, розвитку), адміністрування та забезпечення функціонування засобу інформатизації», затверджених [постановою Кабінету Міністрів України від 21 лютого 2025 р. № 205](#).

6.6 Вимоги до надійності засобу інформатизації та збереженості інформації

Надійність Підсистеми повинна забезпечуватися стабільною роботою, збереженням цілісності та доступності даних, а також мінімальною потребою у втручанні системного адміністратора для відновлення працездатності. Впроваджена Підсистема повинна забезпечувати постійну доступність всіх сервісів в режимі 24x7, окрім випадків, коли виконуються планові профілактичні роботи або відбувається оновлення програмного забезпечення, про що користувачі Підсистеми заздалегідь поінформовані.

Відмовостійкість Підсистеми повинна забезпечуватися автоматично. Повинна вимагатися мінімальна увага з боку адміністратора щодо реакції на усунення наслідків відмов компонентів, а також має бути забезпечене збереження даних програмно-апаратними засобами.

Підсистема та її складові мають бути забезпечені засобами резервного копіювання даних і конфігурацій, що дозволяють оперативно відновлювати їх роботу у разі збоїв, відмов або аварійних ситуацій, а саме:

- працездатність Підсистеми у разі відмови або виходу з ладу будь-якого одного з програмно-апаратних компонентів;
- збереження інформації на момент відмови або виходу з ладу Підсистеми з наступним відновленням після проведення ремонтних і відновлювальних робіт;

- резервування критично важливих даних Підсистеми, конфігурації та налаштувань;
- архівація даних та налаштувань Підсистеми за графіком та за потребою, а також відновлення даних з резервної копії.

Резервне копіювання повинно здійснюватися з періодичністю, що забезпечує повне збереження та відновлення даних з урахуванням встановленого графіка резервного копіювання, та в режимі безперервної роботи Підсистеми, без зупинки її функціонування та з мінімальним впливом на продуктивність. Збереження даних має забезпечуватися у випадках:

- вимкнення живлення;
- відмови технічних засобів обробки інформації;
- помилок, збоїв або руйнування програмного забезпечення.

Збереження інформації, що обробляється в Підсистемі, повинно бути гарантоване у повному обсязі, втрата даних не допускається. Підсистема повинна гарантувати цілісність даних під час збоїв чи помилок за допомогою відповідних програмно-апаратних засобів, зокрема через механізми резервного копіювання, реплікації та забезпечення транзакційності операцій. Надійність повинна забезпечуватись за рахунок:

- забезпечення якісного випробування;
- організації систематичного резервного копіювання та архівного зберігання інформації;
- апаратно-програмного захисту від стороннього несанкціонованого програмно-апаратного втручання;
- архівного збереження інформації;
- здатності до горизонтального масштабування в режимі реального часу без зупинки сервісу;
- можливості формування «холодних» резервних копій усіх компонентів із забезпеченням цілісності даних та можливості розгортання усіх складових Підсистеми з «холодних» копій у цілісному та працездатному вигляді;
- RTO (Recovery time objective, максимальний час відновлення працездатності Підсистеми за умови наявності серверної інфраструктури): не більше 2 годин;
- забезпечення доступності Підсистеми не менше ніж 99,5% без урахування часу планових відключень, недоступності основних та резервних серверних потужностей і засобів зв'язку;
- оперативності заміни програмно-технічних засобів, що вийшли з ладу;
- сумісності технічних засобів та програмного забезпечення.

Усі функціональні складові Підсистеми повинні мати надлишковість за схемою щонайменше N+1 з метою технічного обслуговування та оновлення ПЗ окремих складових без перешкоджання роботі всієї Підсистеми (тобто для кожної ключової складової має бути щонайменше один резервний вузол, у разі відмови основного вузла система автоматично перемикається на резервний).

Підсистема повинна забезпечувати реєстрацію та аудит подій, пов'язаних із її функціонуванням, зокрема фіксацію дій користувачів, змін даних та інших подій. Інформація про події та технічний стан повинна бути передана до відповідних функціональних компонентів ЄСІКС для централізованого моніторингу, журналювання та аналізу функціонування Системи. Моніторинг інфраструктури, резервування даних та відновлення функціонування забезпечуються на рівні ЄСІКС.

6.7 Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації

Програмне забезпечення повинне забезпечувати роботу з різними типами каналів зв'язку, включаючи мобільні мережі, канали з обмеженою пропускнуою спроможністю та високою затримкою, а також мережі із тимчасовим з'єднанням.

Програмне забезпечення має бути розраховане на роботу з мінімальною швидкістю інтернету користувача 1 Мбіт/с. Деталізовані вимоги до Підсистеми будуть визначені у технічному завданні.

6.8 Вимоги до режимів функціонування засобу інформатизації

З метою забезпечення умов розробки та експлуатації Підсистема має бути розгорнута на окремих середовищах, які наведені у таблиці нижче.

Тип	Середовище	Опис
PROD	PROD	Продуктивне середовище призначене для роботи з реальними даними.
NON-PROD	STAGE	Середовище, яке за конфігурацією та функціональністю повторює продуктивне. Призначене для приймальних тестувань та відтворення інцидентів.
	QA	Середовище для тестування розробленого блоку функціональності, усунених несправностей перед передачею напрацювань на STAGE для проведення приймальних тестувань.
	DEV	Середовище для розробки та тестування прототипів функціональності. Використовується для проміжного тестування нової функціональності розробниками.

Початкове розгортання DEV, QA, STAGE середовищ має бути реалізоване Виконавцем на ресурсах Адміністратора Підсистеми.

Розгортання PROD-середовища та його подальше адміністрування будуть виконуватися силами Адміністратора Підсистеми. PROD-середовище Підсистеми повинно функціонувати в режимі active-active у мінімум двох географічно розподілених центрах обробки даних для забезпечення безперервності роботи та відмовостійкості. Вимоги до конфігурації центрів обробки даних визначаються Адміністратором Підсистеми.

Адміністрування DEV, QA, STAGE середовищ — на весь період розробки має виконуватись Виконавцем. Усі видатки, пов'язані із розгортанням, функціонуванням та адмініструванням DEV, QA, STAGE, покладаються на Виконавця.

6.9 Вимоги щодо придатності системи до розвитку та модернізації

Підсистема повинна мати можливість розвитку та модернізації власними силами з використанням програмних інструментальних засобів, які не потребують обов'язкового залучення розробника.

Підсистема повинна мати перспективи розвитку і дозволяти проведення подальшої модернізації, а саме:

- введення додаткових чи доопрацювання наявних компонентів, розмежування доступу та захисту інформації;
- розширення інформаційно-телекомунікаційної мережі.

Підсистема повинна забезпечувати стандартний механізм оновлення версій будь-яких залежностей (бібліотек, компонентів, плагінів тощо) сторонніх розробників, які використовуються в Підсистемі, щонайменше упродовж 10 наступних років з моменту введення Підсистеми в експлуатацію.

6.10 Вимоги до лінгвістичного забезпечення

Підсистема має підтримувати багатомовність (i18n/l10n) інтерфейсу, повідомлень та довідників із обов'язковою підтримкою української (uk-UA) та англійської мов відповідно до IETF BCP 47, з можливістю в майбутньому розширювати перелік локалей. Перелік та обсяг даних, до яких застосовується багатомовність (зокрема довідники, повідомлення, інтерфейсні елементи тощо), мають бути визначені на етапі розробки ТЗ з урахуванням функціональних потреб Підсистеми та вимог законодавства. Управління мовами та перекладами повинне здійснюватися через інтерфейс користувача.

6.11 Вимоги до потужності Підсистеми

Підсистема має забезпечувати обробку запитів і операцій, що виконуються користувачами, з урахуванням одночасної роботи значної кількості користувачів і можливого зростання навантаження. Архітектура Підсистеми має бути розрахована на пікові навантаження, у тому числі під час виникнення надзвичайних подій.

Підсистема має стабільно функціонувати під час пікових навантажень, які можуть виникати внаслідок зростання кількості одночасних користувачів або масових автоматизованих запитів. Деградація часу відповіді під навантаженням має бути передбачуваною.

Для контролю дотримання вимог до потужності Підсистеми повинні забезпечуватися збір і аналіз статистичних показників, зокрема часу виконання операцій, кількості оброблених операцій, відсотка успішного виконання операцій, а також статистики використання ресурсів інфраструктури (CPU, пам'ять, дискова підсистема, мережеві ресурси) під навантаженням.

Реєстр повинен забезпечувати наступні кількісні показники:

№	Показник	Опис / розріз	
1	мінімальна кількість користувачів, що одночасно працюють з Реєстром	К-сть	5 000
2	кількість користувачів, що працюють з Реєстром	К-сть	понад 20 000 на добу
3	кількість активних користувачів Реєстру	К-сть	понад 4 000 осіб
4	середня кількість операцій користувачів Реєстру	К-сть	від 100 000 000 на місяць

5	прогнозована кількість документів в Підсистемі (на 1 день)	К-сть	70 тис.
6	прогнозована кількість документів в Підсистемі (на 10 років)	К-сть	250 млн.

Підсистема повинна забезпечити час обробки інформаційного запиту зі швидкістю інтернету до 100 МБіт/с із затримкою мережі не більше 100 мс на наступному рівні:

1. 90% запитів повинні виконуватися протягом 1 сек.
2. 95% запитів повинні виконуватися протягом 2 сек.
3. 99% Користувачів повинні успішно увійти в Підсистему з першої спроби.
4. Для комплексних запитів прийнятний час опрацювання запиту має визначатись з урахуванням обсягу даних, ланцюжку запитів.

6.12 Вимоги до умов ліцензування та використання стороннього ПЗ

- Майнові права інтелектуальної власності на Програмне забезпечення (Підсистему), створене в рамках надання послуг з розробки (включаючи вихідний код, документацію, бази даних, графічні елементи тощо), у повному обсязі переходять до Власника Підсистеми з моменту підписання Акту приймання-передачі наданих послуг;
- Виконавець має гарантувати, що передана Підсистема не порушує права інтелектуальної власності третіх осіб;
- У складі Підсистеми може використовуватися програмне забезпечення з відкритим вихідним кодом (Open Source) лише за умови, що положення таких ліцензій (наприклад, MIT, Apache 2.0, BSD) дозволяють Власнику Підсистеми використовувати Підсистему у власних цілях без виплати додаткових роялті та без обов'язкового розкриття власного коду Підсистеми (якщо це не суперечить типу ліцензії);
- Виконавець зобов'язаний надати повний перелік усіх сторонніх бібліотек та компонентів, що використані в Підсистемі, із зазначенням типу їх ліцензій;
- У разі необхідності використання у складі Підсистеми комерційного ПЗ третіх осіб, Виконавець повинен:
 - Попередньо погодити із Власником Підсистеми перелік, вартість та умови подальшого оновлення таких ліцензій;
 - У свою кінцеву вартість пропозиції включити вартість цих ліцензій разом із підтримкою на 10 років;
 - Якщо для функціонування Підсистеми необхідні періодичні ліцензійні платежі (subscription), Виконавець зобов'язаний надати розрахунок вартості володіння (TCO) на період не менше 3 (трьох) років.
- Виконавець має передати Власнику Підсистеми вихідний код (Source Code) усього програмного забезпечення, яке створене на виконання договору, а також налаштування, конфігураційні файли та скрипти розгортання;
- Ліцензії на право користування програмним забезпеченням у складі Підсистеми постачаються у вигляді ліцензійних сертифікатів та (за необхідності) ліцензійних ключів (файлів), що інсталюються разом із відповідним програмним забезпеченням у складі Підсистеми;
- Ліцензії на програмне забезпечення, що використовується у складі Підсистеми, повинні бути безстроковими та необмеженими у часі;
- Програмне забезпечення Підсистеми, що постачається, та її складові частини не повинні мати статус EOL/EOS (End-of-Life/End-of-Support);

- Умови ліцензування програмного забезпечення, що використовується у складі Підсистеми, повинні дозволяти після впровадження створювати декілька серверних інсталяцій (кількість обмежується за згодою сторін) для можливостей тестування, розробки та навчання. Програмне забезпечення системи керування базами даних, яке використовуватиметься у складі Підсистеми, повинне передбачати безкоштовну версію системи керування базами даних, яку можна використовувати для тестування та навчання;
- Тип ліцензії повинен забезпечувати одночасну роботу всієї кількості користувачів Підсистеми, яка дорівнює кількості придбаних ліцензій, на будь-якій кількості комп'ютерів або віртуальних машин;
- Ліцензійне програмне забезпечення, необхідне для впровадження та експлуатації Підсистеми, поставляється у термін, достатній для початку надання послуг з впровадження Підсистеми, її налаштування та введення в дію.

6.13 Вимоги до розробки

Під час розробки Виконавець має керуватися загальноприйнятими стандартами, що актуальні для обраної мови програмування. Використання конкретного стандарту має бути погодженим із Власником Підсистеми на етапі формування технічного завдання. За вимогою Адміністратора Виконавець має проводити консультації щодо архітектури та розробки (орієнтовно до 2 годин на тиждень).

Власник Підсистеми (або уповноважений ним технічний спеціаліст) залишає за собою право на проведення регулярного аудиту коду (Code Review) протягом усього терміну розробки.

Виконавець зобов'язується надавати технічні консультації щодо обраних архітектурних рішень, методів реалізації функціоналу та використаних сторонніх бібліотек/фреймворків за запитом Власника Підсистеми.

У разі виявлення під час рев'ю відхилень від загальноприйнятих стандартів кодування або технічного завдання, Виконавець зобов'язаний усунути ці зауваження у погоджені сторонами терміни.

Виконавець повинен забезпечити розробку та впровадження уніфікованих підходів до міжсистемної взаємодії, включаючи стандартизацію API, форматів обміну даними, обробки помилок та версіонування.

Складання, тестування та розгортання складових Підсистеми здійснюються з використанням систем безперервної інтеграції та доставки — GitLab CI з використанням GitLab Runner та Argo CD. Магістралі (pipelines) складання та розгортання зберігаються в системі керування кодом GitLab і застосовуються автоматизовано окремо для кожного середовища (DEV/QA/STAGE/PROD). Виконавець повинен забезпечити автоматизоване виконання перевірок якості коду та тестів у складі магістралей складання, з фіксацією результатів кожного запуску.

Виконавець повинен забезпечити трасування вимог Технічних вимог у відповідному технічному завданні, а також визначення критеріїв приймання та способів перевірки для істотних вимог.

6.14 Вимоги до міграції даних

Виконавець зобов'язаний забезпечити наповнення Підсистеми даними у частині, необхідній для її функціонування, з урахуванням вимог законодавства щодо порядку внесення відомостей до Єдиного державного реєстру виконавчих документів.

Підсистема не передбачає централізовану повну міграцію даних з усіх зовнішніх інформаційно-комунікаційних систем як єдиного механізму наповнення Реєстру, натомість повинно бути забезпечено наповнення Підсистеми структурованими даними виконавчих документів, наявних в ЄСІКС.

Міграція даних не замінює встановленої законодавством процедури внесення виконавчого документа до Реєстру та не впливає на строки пред'явлення виконавчого документа до виконання.

У разі реалізації інформаційної взаємодії з іншими інформаційно-комунікаційними системами допускається часткове автоматизоване перенесення даних у межах функціональності Підсистеми.

Процес міграції повинен включати наступні етапи:

- Виконавець має провести комплексний аналіз структур даних та фактичного наповнення діючих систем з метою виявлення розбіжностей у форматах, типах даних та логічних зв'язках.
- У ході аналізу Виконавець зобов'язаний виявити дефекти (неповні, некоректні або застарілі записи) та потенційні конфлікти даних, що можуть виникнути при об'єднанні інформації з різних джерел (зокрема дублювання записів, суперечливі дані про одні й ті самі об'єкти тощо).
- На основі проведеного аналізу Виконавець має розробити та подати на затвердження Адміністратору Підсистеми Методологію міграції. Цей документ має містити опис правил виправлення дефектів, алгоритми вирішення конфліктів даних та порядок дій у разі виявлення невідповідностей, що не можуть бути виправлені автоматично. Методологія також повинна містити опис методів перевірки (тестування) результатів міграції.
- Після затвердження Методології Виконавець має розробити спеціалізовані програмні інструменти для автоматизованої міграції даних у частині, що стосується Підсистеми.
- Виконавець повинен провести міграцію та надати звіти про результати міграції, що підтверджують цілісність, повноту та коректність перенесених даних у межах Підсистеми.

Перед початком міграції історичних даних Адміністратор Підсистеми має забезпечити Виконавцю доступ до баз даних, які використовуються у Підсистемі, дані з яких будуть переноситися, та опис таблиць цих баз даних (за наявності), а також погодити склад даних, що підлягають перенесенню (включно з атрибутами, метаданими, журнальними активностями та іншими подіями, що будуть уточнені на етапі технічного завдання).

7. ТЕХНОЛОГІЧНИЙ СТЕК

Технологічний стек Підсистеми сформовано відповідно до концепції ЄСІКС з урахуванням принципів уніфікації, масштабованості та довгострокової експлуатаційної спроможності та не передбачає використання технологій, які не сумісні з затвердженим технологічним стеком ЄСІКС. При виборі технологій враховано їх поширеність на ринку, рівень зрілості, активність професійних спільнот, наявність документації та практик промислового використання, а також можливості Адміністратора Підсистеми щодо подальшої підтримки, розвитку та супроводу Підсистеми власними або залученими ресурсами.

Застосований технологічний стек має забезпечувати безперервність функціонування, зменшення залежності від окремих виконавців, а також можливість подальшого розвитку та інтеграції Засобу інформатизації в межах ЄСІКС без необхідності кардинальної зміни архітектурних підходів.

При цьому Виконавець має право запропонувати альтернативний технологічний стек або окремі технологічні компоненти за умови надання обґрунтованих аргументів доцільності такої заміни та за погодження Власником Підсистеми.

Аргументація повинна враховувати відповідність затвердженому технологічному стеку ЄСІКС, вплив на безпеку, масштабованість, вартість володіння, складність супроводу, кадрову доступність, а також ризики подальшої експлуатації та розвитку Підсистеми Адміністратором Підсистеми.

Версії мов програмування, фреймворків, бібліотек та сервісів Підсистеми повинні бути узгоджені з Власником Підсистеми.

Підсистема повинна функціонувати на базі UNIX-подібних операційних систем з відкритим програмним кодом. Використовувана операційна система має належати до версій, визначених розробником як Long Term Support (LTS), та забезпечувати довгострокову підтримку, оновлення безпеки та стабільність експлуатації.

Для зберігання коду Підсистеми потрібно використовувати розподілену систему керування версіями Git.

При виборі рішень із відкритим кодом при однакових функціональних можливостях надається перевага тим рішенням, що відповідають запропонованому стеку технологій у пункті 7.1.

Виконавець повинен реалізовувати функціонал Підсистеми на базі розгорнутої інфраструктури на ресурсах Власника Підсистеми. У випадку недостатності або необхідності зміни запропонованого цими вимогами технологічного стека, Виконавець може запропонувати альтернативне рішення, яке має бути погоджене з Власником Підсистеми.

7.1 Мови програмування, Фреймворки та бібліотеки

Стек програмування:

1. Front-end – Vue.js, починаючи з v.3;
2. Back-end, основні процеси, пов'язані з ЄСІКС – Java або C#;
3. Back-end, робота з даними та процесами аналітики – Python.

Виконавець має право запропонувати альтернативні технічні рішення. У разі пропозиції таких рішень Виконавець повинен надати обґрунтування їх вибору та погодити вибір із Власником Підсистеми.

7.2 Бази даних

База даних має бути побудована в режимі кластера, з передбаченням уникнення можливості збою типу split-brain.

Типи баз даних:

1. Реляційна SQL – PostgreSQL.
2. Документорієнтована NoSQL – MongoDB.
3. Об'єктне сховище – S3-сумісне сховище даних, що наявне у Власника Підсистеми.

Для реалізації окремих функціональних або нефункціональних потреб Підсистеми можуть використовуватися інші типи баз даних за умови їх обґрунтованості, сумісності з цільовою архітектурою та погодження вибору із Власником Підсистеми.

Виконавець має право запропонувати альтернативні технічні рішення. У разі пропозиції таких рішень Виконавець повинен надати обґрунтування їх вибору та погодити вибір із Власником Підсистеми.

7.3 Інструменти інтеграції та API

Підсистема повинна взаємодіяти з іншими підсистемами та функціональними компонентами базової інфраструктури ЄСІКС через стандартизовані API та/або подієві механізми.

Базовим механізмом синхронної взаємодії є використання RESTful вебсервісів поверх HTTP(S) з передачею даних переважно у форматі JSON. Сервіси повинні підтримувати стандартні HTTP-методи (GET, POST, PUT, PATCH, DELETE) відповідно до реалізованого сценарію. Для сценаріїв, що потребують підвищеної продуктивності, масової обробки даних, потокової передачі або низьких затримок, допускається використання інших протоколів, форматів даних та асинхронних механізмів взаємодії за умови їх архітектурного обґрунтування.

У межах інтеграції Підсистеми зі складовими ЄСІКС має бути забезпечена можливість роботи з протоколом SOAP (з використанням XML) та іншими форматами даних. Можливість трансформації даних між різними форматами має бути закладена.

Підсистема повинна забезпечувати можливість автоматизованої електронної інформаційної взаємодії та обміну даними як внутрішньо (в рамках ЄСІКС), так і зовнішньо.

7.4. Контейнеризація та оркестрація

7.4.1 Загальний опис

Платформа контейнерної оркестрації — рівень середовища виконання, що забезпечує роботу сервісів Системи у вигляді контейнерів, які відповідають специфікації OCI (Open Container Initiative), а також їхнє горизонтальне масштабування, самовідновлення (self-healing), автоматичне балансування навантаження та безпечне керування чутливими даними контейнеризованих складників у розподіленому кластері обчислювальних вузлів.

Відповідно до Концепції ЄСІКС, на цьому рівні мають використовуватися OpenSource-системи контейнерної оркестрації.

Цільовим рішенням є Kubernetes. Допускається використання платформ, побудованих на базі Kubernetes та сумісних з його програмним інтерфейсом (зокрема OpenShift), за погодженням із Власником Підсистеми.

7.4.2 Основні функціональні вимоги

1. Платформа має забезпечувати декларативне визначення гарантованого та граничного обсягу обчислювальних ресурсів (CPU, RAM) для кожного складника з відповідними класами пріоритетності при витісненні у разі нестачі ресурсів вузла.
2. Платформа має забезпечувати спільне планування групи контейнерів як єдиної неподільної одиниці розгортання — зі спільним мережевим простором імен, спільними томами та узгодженим життєвим циклом, — а також виконання контейнерів попередньої ініціалізації до старту основного застосунку. Ця можливість є необхідною умовою для роботи допоміжних контейнерів: збирачів логів і телеметрії, проксі-агентів.
3. Платформа має підтримувати виконання разових та періодичних (за розкладом) завдань як окремого типу навантаження — з гарантією одноразового завершення, політикою повторних спроб, обмеженням часу виконання та контролем паралельності.
4. Платформа має забезпечувати для складників, що зберігають стан, стабільну мережеву ідентичність екземпляра, сталу прив'язку екземпляра до персистентного тому та контрольований порядок розгортання, оновлення й зупинки реплік.
5. Платформа має забезпечувати мікросегментацію мережевої взаємодії між складниками на основі політик рівня L3/L4 із застосуванням принципу заборони за замовчуванням та можливістю визначати дозволені напрямки трафіку за атрибутами складників, а не за IP-адресами.

7.4.3 Вимоги до інтеграції та використання

1. Платформа має забезпечувати динамічне виділення персистентних томів на вимогу складника через стандартизований інтерфейс підключення сховищ, з підтримкою класів сховищ різної продуктивності та створення знімків томів для потреб резервного копіювання.
2. Платформа має забезпечувати маршрутизацію та кероване розділення внутрішнього (east-west) трафіку між складниками Системи на прикладному рівні (L7) — за іменем сервісу та шляхом запиту, з можливістю поетапного розподілу трафіку між версіями складника під час впровадження змін; ці можливості стосуються виключно взаємодії складників між собою в межах кластера й не дублюють функції зовнішнього вхідного шлюзу (п. 7.4.2).

7.5 Вебсервер та реверс-проксі

Вебсервер та реверс-проксі — nginx. Використовувана версія має належати до визначених розробником як Long Term Support (LTS).

7.6 Вхідний мережевий шлюз

7.6.1 Загальний опис

Рішення забезпечує прийом, розподіл і маршрутизацію вхідного мережевого трафіку до відповідних складників Системи, а також термінацію захищеного з'єднання на межі периметра. Рішення є єдиною контрольованою точкою входу зовнішнього трафіку до

внутрішньої інфраструктури Системи та основою для реалізації політик мережевої безпеки на рівні вхідних запитів.

Вхідний мережевий шлюз – рішення, сумісне з програмним інтерфейсом Kubernetes Gateway API.

Цільовим рішенням є контролер вхідного трафіку, що реалізує стандартизований програмний інтерфейс Kubernetes Gateway API та має підтверджений статус відповідності (conformance) для відповідного профілю. Конкретна реалізація обирається Виконавцем з наданням обґрунтування та погоджується із Власником Підсистеми; як орієнтир розглядаються Kong Ingress Controller, Envoy Gateway, NGINX Gateway Fabric, HAProxy Kubernetes Ingress Controller. Не допускається використання реалізацій, знятих виробником або спільнотою з підтримки чи таких, що не отримують оновлень безпеки, — зокрема контролера Ingress NGINX (kubernetes/ingress-nginx), супровід якого припинено.

Функції шлюзу API та функції вхідного мережевого шлюзу можуть реалізовуватися як одним, так і різними програмними рішеннями — за умови збереження єдиної контрольованої точки входу зовнішнього трафіку та відсутності дублювання політик маршрутизації і безпеки між компонентами.

7.6.2 Основні функціональні вимоги

1. Рішення має забезпечувати маршрутизацію запитів на прикладному рівні (HTTP/HTTPS) за доменним іменем, шляхом, методом і заголовками запиту, з підтримкою HTTP/2, WebSocket та проксіювання gRPC.
2. Рішення має забезпечувати термінацію захищеного з'єднання (TLS) з обслуговуванням кількох доменних імен на одній точці входу, контролем мінімальної версії протоколу та дозволених криптографічних наборів, примусовим перенаправленням на захищене з'єднання; якщо трафік далі перетинає межу довіреного мережевого сегмента — повторне встановлення захищеного з'єднання до цільового сервісу.
3. Рішення має забезпечувати передавання внутрішнім сервісам достовірної мережевої адреси клієнта-джерела, генерування унікального ідентифікатора запиту та поширення контексту трасування у ланцюгу внутрішніх викликів.
4. Рішення має забезпечувати розподіл навантаження між репліками кожного складника Системи за налаштуваним алгоритмом балансування, з можливістю прив'язки сесії до екземпляра; автоматичне виключення з балансування екземплярів, що не підтвердили готовність, на підставі відомостей від платформи контейнерної оркестрації (п. 7.4.1), без дублюючого власного механізму перевірки стану.
5. Рішення має забезпечувати коректне завершення обслуговування наявних з'єднань під час виведення екземпляра з експлуатації (graceful drain), кероване визначення таймаутів і політику повторних спроб для ідемпотентних запитів, а також кероване розділення трафіку між версіями складника для поетапного впровадження змін (canary/blue-green).
6. Рішення має забезпечувати обмеження інтенсивності запитів (rate limiting) із єдиним обліком лічильників для всіх реплік рішення, з визначенням ключа обмеження та стандартизованою відповіддю про перевищення ліміту; а також обмеження розміру тіла й заголовків запиту та кількості одночасних з'єднань з одного джерела.
7. Публікація мережевих служб складників Системи у зовнішню мережу в обхід даного рішення має бути унеможливлена; службові, адміністративні та діагностичні інтерфейси складників не повинні бути доступними ззовні периметра.
8. Рішення має бути розгорнутий у відмовостійкій конфігурації не менш ніж із двома одночасно активними екземплярами в різних доменах відмови, з утриманням стійкої зовнішньої точки входу незалежно від відмови окремих вузлів кластера; рішення

має підтримувати власне горизонтальне масштабування та оновлення версії без простою сервісу.

9. Конфігурація маршрутизації, керування трафіком та політик безпеки має описуватися типізованими ресурсами програмного інтерфейсу платформи контейнерної оркестрації (без нестандартизованих розширень конкретної реалізації), зберігатися в системі контролю версій та застосовуватися автоматизовано окремо для кожного середовища (DEV/QA/STAGE/PROD); внесення змін безпосередньо на працюючому екземплярі рішення має бути унеможливлене.

7.6.3 Вимоги до інтеграції та використання

1. Рішення має інтегруватися з платформою контейнерної оркестрації (п. 7.4.1) для автоматичного оновлення переліку цільових екземплярів і маршрутів під час масштабування, оновлення чи переміщення складників Системи, без ручного втручання та без перезапуску рішення.
2. Відомості про готовність екземплярів складників до приймання трафіку рішення має отримувати від платформи контейнерної оркестрації на підставі визначених там перевірок стану, без реалізації власного дублюючого механізму контролю працездатності.
3. Рішення має забезпечувати передавання метрик вхідного трафіку до функціонального компонента «Моніторинг» з деталізацією до окремого маршруту, методу та коду відповіді, включно з розподілом часу відгуку за перцентилями (p50, p95, p99), а також метрик стану самого рішення (кількість активних з'єднань, використання ресурсів, відмови у обслуговуванні).
4. Рішення має забезпечувати передавання журналів доступу та подій до функціонального компонента «Логування». Запис журналу має містити ідентифікатор запиту, достовірну адресу джерела, обраний маршрут, код відповіді та час обробки окремо на стороні рішення і на стороні цільового сервісу. Значення заголовків автентифікації, службові токени та інші конфіденційні дані до журналів не заносяться.

7.7 Кешування даних

7.7.1 Загальний опис

Кешування даних — механізм прискорення роботи функціональних складників Системи шляхом оперативного зберігання результатів частих запитів та зниження навантаження на реляційні бази даних. Рішення виконує роль високопродуктивного посередника між складовими Системи та основними базами даних і має бути реалізований як розподілене сховище даних у пам'яті (In-memory data store) в окремому логічному просторі.

Кешування даних – Redis / Redis Cluster. Як альтернатива допускається KeyDB або інше рішення, сумісне з протоколом Redis, за погодженням із Власником Підсистеми.

7.7.2 Основні функціональні вимоги

1. Рішення має підтримувати роботу в режимі кластера та георозподілення для забезпечення відмовостійкості та збереження даних при виході з ладу окремих вузлів.
2. Витіснення кешованих даних за нестачею оперативної пам'яті за налаштовуваною політикою (LRU/LFU) є допустимим.
3. Управління життєвим циклом тимчасових даних (TTL): рішення має автоматично видаляти застарілі кеші на основі налаштованих термінів зберігання, визначених окремо від строків зберігання сесій та чернеток.

4. Рішення має бути сумісним із протоколом In-memory рішень для забезпечення мінімальної затримки (latency) при доступі до даних.

7.8 Брокер повідомлень

7.8.1 Загальний опис

Черга повідомлень — це інфраструктурний сервіс, призначений для забезпечення асинхронної комунікації між підсистемами ЄСІКС та зовнішніми інформаційними системами. Рішення виступає як посередник, що дозволяє реалізувати подієво-орієнтовану архітектуру, забезпечуючи слабку пов'язаність компонентів Системи. Сервіс відповідає за приймання, маршрутизацію, тимчасове та/або постійне зберігання та гарантовану доставку повідомлень від видавців до підписників.

Брокер повідомлень – Apache Kafka.

Цільовим рішенням є Apache Kafka. Використання RabbitMQ допускається як альтернативне або додаткове рішення для сценаріїв, що потребують складної маршрутизації повідомлень та класичної черги завдань, за умови надання Виконавцем обґрунтування та погодження із Власником Підсистеми.

7.8.2 Основні функціональні вимоги

Рішення повинно забезпечувати:

1. Підтримку основних патернів обміну:
 - Публікація/Підписка — для розсилки подій декільком сервісам;
 - Точка-Точка — для розподілу завдань між екземплярами одного сервісу.
2. Гарантовану доставку: збереження повідомлень до моменту успішного підтвердження отримання підписником, що мінімізує ризики втрати даних при перезавантаженні або оновленні компонентів Системи.
3. Горизонтальне масштабування: можливість динамічного збільшення кількості обробників для забезпечення високої пропускну здатності в пікові періоди навантаження.
4. Пріоритезацію повідомлень: можливість обробки критично важливих системних подій поза чергою або з вищим пріоритетом.

7.8.3 Вимоги до надійності та продуктивності

1. Висока доступність: розгортання в кластерному режимі для виключення єдиної точки відмови.
2. Асинхронна взаємодія: звільнення ресурсів сервісу-відправника одразу після прийняття повідомлення брокером, не очікуючи на завершення обробки повідомлення отримувачем.
3. Ізоляція: кожна підсистема повинна працювати у власному логічному просторі для запобігання конфліктам імен черг та несанкціонованого доступу до чужих даних.

7.8.4 Вимоги до інтеграції та безпеки

1. Стандартизація протоколів: підтримка відкритих протоколів взаємодії (наприклад, Kafka Protocol, AMQP 0.9.1, MQTT).
2. Уніфікований формат даних: використання уніфікованого формату тіла повідомлення з обов'язковим включенням метаданих.
3. Інтеграція з моніторингом: передача метрик щодо довжини черг, швидкості обробки повідомлень та кількості помилок до функціонального компонента «Моніторинг».
4. Безпека та аудит:
 - Автентифікація підсистем при підключенні до брокера;
 - Шифрування трафіку між відправником, брокером та отримувачем;

- Обмеження прав доступу — сервіс повинен мати доступ лише до визначених для нього черг та топіків;
- Логування: фіксація фактів публікації та доставки повідомлень у функціональному компоненті «Логування» для можливості трасування бізнес-процесів.

7.9 Індексатор

7.9.1 Загальний опис

Індексатор — розподілене сховище індексів, що забезпечує повнотекстовий і структурований пошук, аналітичні агрегації та зберігання і аналіз журнальних даних. Індексатор є спільною технологічною основою для функціональних компонентів «Пошук і фільтри» та «Логування» і не реалізує самостійно їхніх функціональних вимог.

Індексатор – Elasticsearch / OpenSearch.

Цільовим рішенням є OpenSearch. Як альтернатива допускається Elasticsearch за умови дотримання вимог щодо ліцензування, наведених у п. 7.9.3, та погодження із Власником Підсистеми.

7.9.2 Основні функціональні вимоги

1. Рішення має бути розгорнуте в режимі кластера з передбаченням уникнення можливості збою типу split-brain та відсутністю єдиної точки відмови.
2. Рішення має забезпечувати резервне копіювання індексів та власної конфігурації за розкладом з періодичною перевіркою відновлюваності.
3. Рішення має забезпечувати керування життєвим циклом індексів, зокрема ротацію та дотримання визначених строків зберігання, з роздільним налаштуванням для пошукових та журнальних індексів.
4. Рішення має забезпечувати автентифікацію всіх звернень без можливості анонімного доступу, з роздільними обліковими записами для індексації та для виконання запитів, та розмежування прав доступу на рівні окремих індексів.
5. Рішення має забезпечувати шифрування даних індексу у стані спокою та захищене з'єднання для всіх звернень.
6. Рішення має забезпечувати захист від запитів, що надмірно споживають ресурси: обмеження максимального часу виконання запиту, граничної складності та обсягу вибірки з поверненням визначеної помилки замість деградації обслуговування.

7.9.3 Вимоги до інтеграції та використання

Доступ функціональних компонентів Системи до рушія безпосередньо, в обхід програмних інтерфейсів функціональних компонентів «Пошук і фільтри» та «Логування», має бути унеможливлений.

Збір та доставка журнальних даних до рушія мають здійснюватися з використанням відкритих стандартів телеметрії та легких агентів збору, що розгортаються на вузлах кластера і не потребують зміни коду функціональних складників Системи.

Рішення має забезпечувати передавання власних експлуатаційних метрик до функціонального компонента «Моніторинг», зокрема стану вузлів кластера та реплік індексу, обсягу індексів та часу виконання запитів за перцентилями.

Умови ліцензування обраного рішення мають дозволяти використання всієї передбаченої цим розділом функціональності у промисловій експлуатації без додаткових платежів, розмір яких залежить від обсягу даних, кількості вузлів кластера або кількості користувачів Системи.

8. ВИМОГИ ДО СУПРОВОДУ ТА ОБСЛУГОВУВАННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ

Рівень деталізації вимог — користувацький сценарій до групи функціональності Підсистеми з розділами — Ціль, Передумови (за потреби), Основний та Альтернативні Сценарії / Групи функціональних вимог (у разі необхідності), Приймальні критерії.

Мови моделювання вимог — BPMN відповідно до ДСТУ ISO/IEC 19510:2017.

Менеджмент-системи — ClickUp тощо, в яких відбуватиметься процес розробки, надаються Адміністратором Підсистеми.

Інфраструктура NON-PROD для розробки буде виділена Адміністратором Підсистеми:

1. Система керування кодом – GitLab.
2. Доступ до NON-PROD середовищ за використанням VPN.

Адаптація інфраструктури під потреби розробки має виконуватись силами Виконавця після узгодження з Адміністратором Підсистеми.

8.1 Вимоги до гарантійної підтримки

Всі складові Підсистеми мають забезпечуватися гарантійною підтримкою (виправлення помилок у разі невідповідності технічному завданню, потребам Адміністратора Підсистеми, які визначені в цих технічних вимогах, Концепції ЄСІКС) на термін 12 місяців, встановлений умовами договору.

Виконавець зобов'язаний виконати наступні дії в рамках гарантування роботи та відповідності функцій складових Підсистеми:

5. Усунути всі виявлені недоліки складових Підсистеми, які не відповідають вимогам технічного завдання та функціональних вимог в терміни, визначені в SLA, що є додатком до договору.
6. Оновлювати документацію, коли виникає потреба через зміни, викликані відмінностями у порівнянні зі станом на момент поставки складових Підсистеми.
7. Виконувати оновлення та/або відновлення складових Підсистеми, включаючи оновлення операційних систем, мережі та комунікаційного обладнання, серверних операційних систем та системного програмного забезпечення, систем управління базами даних, серверів додатків, вебсерверів відповідно до вимог, визначених в SLA, що є додатком до договору.

8.2 Вимоги до навчання користувачів

З метою забезпечення ефективного використання складових Підсистеми Виконавець повинен забезпечити підготовку та надання навчальних матеріалів для користувачів.

В мінімальному наборі навчальні матеріали мають включати:

1. інструкції з використання основного функціоналу сервісів у форматі електронної довідки (вікі), що описують типові сценарії роботи користувачів відповідно до їх ролей;
2. короткі відео-інструкції по кожному бізнес-процесу за потреби (загальною тривалістю максимально 5 годин відео).

Навчальні матеріали повинні бути доступні в електронному вигляді та підтримуватися в актуальному стані з урахуванням змін функціоналу складових Підсистеми.

Конкретна спеціалізована форма, в якій мають бути представлені ті чи інші навчальні матеріали про певний аспект роботи Підсистеми має бути узгоджена на етапі розробки технічного завдання. Форма навчальних матеріалів буде обиратися залежно від складності матеріалу та загальної готовності відповідної категорії користувачів до експлуатації Підсистеми. Окрім зазначеного, навчальні матеріали можуть бути також у вигляді сформованого курсу лекцій в спеціалізованій навчальній підсистемі, що буде розгорнута Адміністратором Підсистеми, у вигляді відеокурсів, у вигляді автоматизованих тестів з можливістю налаштувати перелік питань та спосіб надання відповідей тощо.

8.3 Вимоги до документації

Підсистема повинна мати таку документацію:

1. Інструкція користувача Підсистеми (за наявними ролями). Інструкція користувача повинна містити покрокові описи дій користувачів по всіх операціях з візуальним відображенням (скріншоти інтерфейсу).
2. Інструкція адміністратора Підсистеми:
 - 2.1. Інструкція для Підсистеми з початкового розгортання, оновлення, повернення до попередньої версії;
 - 2.2. Інструкція з резервного копіювання та відновлення даних;
 - 2.3. Helm charts та/або ansible плейбуки;
 - 2.4. Політики та процедури SDLC у вигляді документа та магістралей (pipelines) в Gitlab CI/CD з використанням gitlab runner;
 - 2.5. Документацію з моніторингу та журналювання, що містить опис контрольованих метрик, логів, подій аудиту, правил сповіщення, порогових значень та порядку реагування на інциденти.
3. Документація для розробника та тестувальника:
 - 3.1. Має містити перелік підтримуваних методів та їх описи;
 - 3.2. Має містити перелік параметрів запиту та їх опис;
 - 3.3. Має містити перелік атрибутів відповіді та їх опис;
 - 3.4. Дозволяє емулювати запит/відповідь з описом статусу відповіді (успіх, помилка);
 - 3.5. Повинна бути забезпечена можливість перегляду специфікації та інтерактивної взаємодії з методами API (виконання запитів, перегляд прикладів/схем) через будь-який інструмент, сумісний з OpenAPI (не прив'язуючись до конкретного продукту);
 - 3.6. Опис моделі даних/структури даних Підсистеми, включаючи опис основних сутностей, їх атрибутів, зв'язків, правил валідації, довідників, класифікаторів та форматів обміну даними;
 - 3.7. Перелік використаних сторонніх компонентів, бібліотек та сервісів із зазначенням їх призначення, ліцензій та обмежень використання, факт перевірки безпечності під час розроблення Підсистеми;
 - 3.8. Опис порядку керування релізами, версіювання, випуску змін та ведення переліку змін (release notes/changelog);
 - 3.9. Документація з тестування (план тестування, тестові сценарії з умовами прийняття, чек-листи, тестові дані, протоколи результатів тестування, звіти про дефекти, звіти про покриття тестування, звіти про виконання тестів).
4. Архітектурний опис Підсистеми, її взаємодії з іншими підсистемами та функціональними компонентами ЄСІКС, середовищ розгортання, зовнішніх інтеграцій та потоків даних.
5. Програма та методика випробувань (попередніх або дослідної експлуатації).
6. Протокол випробувань.
7. Акт випробувань.
8. Програма навчання та навчальні матеріали користувачів різних ролей.

Документація повинна бути повною, інформативною, зрозумілою, структурованою, зручною для читання, достатньою, однозначною та несуперечливою (повинні використовуватися тотожні терміни, визначення, ідентифікатори тощо). Документація повинна бути виконана українською мовою і має надаватися в електронному вигляді, який надає змогу редагувати текстову частину.

9. ВИМОГИ ДО ПРИЙМАННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ

9.1 Вимоги до проведення випробувань

Випробування складових Підсистеми проводяться з метою перевірки відповідності реалізованого функціоналу, інтеграцій, показників безпеки та якості вимогам технічного завдання та функціональним вимогам, а також підтвердження готовності складових Підсистеми до експлуатації.

Випробування повинні охоплювати всі ключові функціональні можливості сервісів.

Випробування проводяться на визначеному NON-PROD середовищі відповідно до документа «Програма та методика попередніх випробувань», який розробляється Виконавцем і затверджується Адміністратором Підсистеми до початку проведення випробувань.

Під час випробувань повинна бути підтверджена працездатність Підсистеми в архітектурі, що підтримує експлуатацію в режимі active-active та збереження її доступності для користувачів у разі недоступності одного з майданчиків.

Результати випробувань підлягають документуванню та оформлюються у вигляді протоколів і звітів, які містять опис перевірених сценаріїв, результати виконання тестів, виявлені невідповідності (за наявності) та рекомендації щодо їх усунення. Виявлені зауваження та дефекти мають бути усунуті Виконавцем у строки, погоджені з Адміністратором Підсистеми, з подальшим повторним тестуванням.

9.1.1 Функціональне тестування

Функціональне тестування проводиться на всіх етапах створення та доопрацювання складових Підсистеми, що пов'язані з реалізацією або зміною функціоналу.

Під час випробувань перевіряється коректність реалізації функцій складових Підсистеми відповідно до функціональних вимог технічного завдання.

Результати функціонального тестування оформлюються протоколом випробувань, який підписується представниками Адміністратора Підсистеми за участі Виконавця. Додатком до протоколу є звіт про проведені випробування з описом перевірених сценаріїв і виявлених зауважень (за наявності).

9.1.2 Інтеграційне тестування

Інтеграційне тестування проводиться з метою перевірки взаємодії з іншими підсистемами ЄСІКС та зовнішніми інформаційно-комунікаційними системами.

Під час випробувань перевіряється коректність обміну даними, обробки відповідей, стійкість інтеграцій до помилок та відповідність реалізованих механізмів вимогам технічного завдання.

9.1.3 Тестування на проникнення

Тестування на проникнення та безпекові випробування проводяться з метою перевірки рівня захищеності складових Підсистеми від несанкціонованого доступу, зловживань правами доступу, витоків інформації та інших загроз інформаційній безпеці.

Безпеківі випробування повинні охоплювати перевірку механізмів автентифікації та авторизації користувачів, управління сесіями, розмежування прав доступу, захисту персональних та службових даних, а також стійкості складових Підсистеми до типових мережових і прикладних атак.

За результатами тестування формується звіт, який містить опис виявлених вразливостей, їхню критичність, можливі наслідки та рекомендації щодо усунення.

У разі виявлення критичних або високих ризиків інформаційної безпеки Виконавець зобов'язаний забезпечити їх усунення у найкоротші строки та надати підтвердження готовності складових Підсистеми до повторного тестування. Складові Підсистеми не можуть бути прийняті Адміністратором Підсистеми до моменту усунення та повторної перевірки всіх критичних і високих ризиків.

9.1.4 Тестування під навантаженням

Тестування під навантаженням та продуктивності проводяться з метою перевірки здатності Підсистеми стабільно функціонувати при визначених цими технічними вимогами прогнозованих параметрах інтенсивності роботи, визначення її пропускну здатності, часу відгуку та стійкості до пікових навантажень.

Випробування повинні охоплювати перевірку роботи Підсистеми при нормальному (цільовому), піковому та стресовому навантаженнях, аналіз споживання ресурсів серверної інфраструктури, оцінку швидкодії основних сценаріїв використання, а також перевірку механізмів відновлення працездатності після відмов.

За результатами тестування формується звіт, який містить опис фактичних показників продуктивності, виявлені «вузькі місця» (bottlenecks), оцінку відповідності Підсистеми нефункціональним вимогам та рекомендації щодо оптимізації або масштабування.

У разі невідповідності Підсистеми встановленим вимогам до продуктивності або виявлення критичних помилок при навантаженні, Виконавець зобов'язаний провести оптимізацію коду чи конфігурації та надати підтвердження готовності Підсистеми до повторного тестування. Складові Підсистеми не можуть бути прийняті Адміністратором Підсистеми до моменту досягнення цільових показників продуктивності та стабільності.

9.2 Вимоги до передачі результатів виконаних робіт

Для проведення попередніх випробувань складових Підсистеми повинна бути створена комісія, затверджена Адміністратором Підсистеми.

Підсистема має успішно пройти випробування відповідно до програми та методики попередніх випробувань, які розробляються Виконавцем на базі технічного завдання.

Крім того, Виконавець у складі пропозиції повинен надати опис підходу до подальшого доопрацювання та розвитку функціоналу Підсистеми за моделлю Change Request, зокрема порядок ініціювання змін, їх оцінки, погодження, реалізації та впровадження, а також принципи оцінки вартості та строків виконання таких змін.

Всі майнові права інтелектуальної власності, у тому числі виключні, на Програмне забезпечення, що набуває Власник Підсистеми стосуються лише Програмного забезпечення, спеціально створеного за Договором, в рамках Проєкту.

Повна передача прав у тому числі виключних, на Програмне забезпечення означає передання у повному складі майнових прав інтелектуальної власності, встановлених статтями

424 та 440 Цивільного кодексу України, статтею 12 Закону України "Про авторське право і суміжні права", без обмежень способів використання Програмного забезпечення, зазначених Цивільним кодексом України та Законом України "Про авторське право і суміжні права".

У результаті передачі майнових прав (у тому числі виключних) Виконавець втрачає будь-які майнові права, а Власник Підсистеми отримує право, зокрема, але не виключно:

- використовувати Програмне забезпечення усіма способами, передбаченими Цивільним кодексом України та Законом України "Про авторське право і суміжні права";
- дозволяти третім особам використовувати Програмне забезпечення способами, передбаченими Цивільним кодексом України та Законом України "Про авторське право і суміжні права";
- перешкоджати неправомірному використанню Програмного забезпечення, в тому числі забороняти таке використання;
- передавати (відчужувати) повністю або частково права на Програмне забезпечення третім особам;
- перекладати, адаптувати модифікувати (переробляти), модернізувати, вчиняти будь-які інші дії та/або зміни Програмного забезпечення або його частини;
- інші майнові права інтелектуальної власності, встановлені законом.

Власник Підсистеми набуває майнові права інтелектуальної власності, у тому числі виключні на Програмне забезпечення на строк дії таких прав відповідно до норм законодавства України. Майнові права інтелектуальної власності на Програмне забезпечення поширюються на територію всього світу без обмежень.

Передача Виконавцем майнових прав інтелектуальної власності (у тому числі виключних) на Програмне забезпечення Власнику Підсистеми здійснюється на безоплатній основі. Вартість майнових прав інтелектуальної власності (у тому числі виключних) на Програмне забезпечення включена у вартість Договору на створення Підсистеми.

Положення цього пункту діють з урахуванням положень пункту 6.12.

9.3 Вимоги до патентної чистоти

9.3.1 Вимоги до програмного забезпечення, яке розробляється Виконавцем

На момент передання Підсистеми Виконавець зобов'язаний врегулювати всі правовідносини з авторами та третіми особами, залученими ним до створення Підсистеми, та забезпечити набуття від них майнових прав інтелектуальної власності на Підсистему повністю (на всі способи використання твору на території всіх держав світу) та на весь строк чинності майнових прав інтелектуальної власності, передбачений українським законодавством. Детальні умови щодо майнових прав інтелектуальної власності визначаються відповідними договорами, укладеними з авторами та третіми особами, залученими до створення Підсистеми.