(гриф обмеження доступу за наявності)

ЗАТВЕРДЖУЮ
Власник Системи

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

_____ **Леонід САПЕЛЬНИКОВ**
(посада, підпис, Ім'я, ПРІЗВИЩЕ)
"29" червня 2026 року

ТЕХНІЧНІ ВИМОГИ

НА СТВОРЕННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ - КОМПОНЕНТІВ "КЕРУВАННЯ ДОСТУПОМ", БАЗОВИХ СЕРВІСІВ ТА ІНФРАСТРУКТУРИ ЄДИНОЇ СУДОВОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ

(вибрати мету, зазначити повну назву ІКС)

Шифр роботи: ЄСІКС - Базові сервіси та інфраструктура
(шифр ІКС)

На 59 аркушах

ПОГОДЖЕНО

Розробник технічних вимог

Виконавча директорка ГО "Лабораторія законодавчих ініціатив"

_____ **Світлана МАТВІЄНКО**
(посада, підпис, Ім'я, ПРІЗВИЩЕ)
"29" червня 2026 року

КИЇВ - 2026

ЗМІСТ

1 ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1 Підстава для розроблення технічних вимог

Останні роки в Україні триває активний процес реформування судової системи. У зв'язку з цим виникла необхідність покращення та розширення засобів автоматизації діяльності судових установ. Рішення про створення та подальшу модернізацію Єдиної судової інформаційно-комунікаційної системи (далі - ЄСІКС) було зумовлене потребою у сталій підтримці цифрової трансформації судової системи України відповідно до стратегічних цілей держави у сфері правосуддя, зокрема підвищення доступності судових процедур, швидкості судового розгляду та можливості повноцінної онлайн-взаємодії учасників процесу з судами.

Поточний стан електронної судової системи не відповідає зазначеним цілям. На сьогодні система функціонує як сукупність незалежних підсистем та окремих рішень, створених у різний час, із відсутньою або обмеженою інтеграцією та різним рівнем інформаційної безпеки. Така фрагментація унеможливлює побудову єдиного інформаційного простору судової влади, призводить до проблем інтеграції, дублювання функціональності та ускладнює подальший розвиток системи.

Частина рішень базується на технологіях, які не відповідають сучасним вимогам до масштабованості, продуктивності, надійності та інформаційної безпеки. Подальше використання таких компонентів створює ризики збоїв, втрати даних, а також обмежує можливість впровадження нової функціональності.

Практика часткових оновлень і локальних доопрацювань окремих рішень не усуває системних проблем, а, навпаки, призводить до накопичення технічного боргу. За відсутності єдиної архітектурної основи такі рішення лише тимчасово знижують прояви окремих проблем, водночас підвищуючи складність супроводу та вартість підтримки.

Таким чином, подальший розвиток шляхом фрагментарних доопрацювань є недоцільним, а досягнення стратегічних цілей цифровізації судової системи можливе лише завдяки створенню нової, цілісної та архітектурно узгодженої інформаційно-комунікаційної системи у відповідності до Концепції ЄСІКС.

1.2 Найменування засобу інформатизації

Повне найменування Системи: Єдина судова інформаційно-комунікаційна система

Скорочена назва: ЄСІКС

Вживання термінів "Система" та ЄСІКС є тотожними.

1.3 Мета створення засобу інформатизації

З метою забезпечення узгодженої, безпечної та ефективної роботи ЄСІКС, а також унеможливлення фрагментації підходів до управління доступом, даними та інфраструктурою, в рамках ЄСІКС є необхідним створення та впровадження централізованих спільних компонентів, зокрема:

1. **Базові сервіси:**
   - **1.1. Керування доступом - IAM (Identity Access Mgmnt) — Управління користувачами, організаціями (в контексті агрегатора користувачів), ролями, ідентифікацією, аутентифікацією, авторизацією, фіксацією подій доступу для подальшого логування в сервісі логування;**
   - **1.2. Довідники та класифікатори - Dictionary — Ведення нормативно-довідкової інформації (класифікаторів і довідників);**

1.3. **Нотифікації - Notifications — Інформування користувачів про актуальні для них події в Системі та або в бізнес процесах, що автоматизує Система;**
1.4. **Підписання документів - Crypto-service — Перевірка, підписання КЕП об'єктів та об'єднання підписаних об'єктів;**
1.5. **Довідка та рекомендації, База знань - Wiki — Управління інформацією (статті, інструкції, FAQ);**
1.6. **Майстер-реєстри — організації, штатна структура, посади, кадри тощо.**

2. **УНІФІКОВАНОЇ ІНФРАСТРУКТУРИ, спільної для складових ЄСІКС, що забезпечує стандартизовані підходи до розгортання, експлуатації, масштабування, моніторингу та інформаційної безпеки.**

Реалізація зазначених складових є передумовою побудови цілісної, масштабованої та керованої архітектури ЄСІКС, зниження витрат на розробку та супровід складових, а також забезпечення єдиних стандартів безпеки та користувацького досвіду.

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 Системи	**юридична особа, завданням якої відповідно до її повноважень або договору з Власником Системи є здійснення організаційних, технічних та інших заходів, необхідних для забезпечення супроводу, адміністрування та функціонування засобу інформатизації**
API (АПІ)	**Автоматизовані програмні інтеграції, відомі також як "прикладний інтерфейс програмування - application programming interface"**
База даних або БД	**Організована колекція даних, яка зберігається та управляється з використанням комп'ютерної системи; забезпечує зберігання, організацію та доступ до даних з метою ефективного використання та обробки**
Бізнес-процес	**Сукупність дій необхідних для здійснення людиною або системою, в результаті яких відбувається досягнення бажаного результату**
Валідація	**Встановлення об'єктивних і задокументованих доказів того, що визначені вимоги до спеціально призначеного застосування можливо послідовно виконати**
Вебсайт	**Сукупність програмних засобів, розміщених за унікальною адресою в обчислювальній мережі, у тому числі в мережі Інтернет, разом з інформаційними ресурсами, що перебувають у розпорядженні певних суб'єктів і забезпечують доступ юридичних та фізичних осіб до цих інформаційних ресурсів та інших інформаційних послуг через обчислювальну мережу**
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**
ВКЗ	**Підсистема відеоконференцзв'язку**
ЕДО	**Електронний документообіг**

ЄСІКС	**Єдина судова інформаційно-комунікаційна система**
ІКС	**Інформаційно-комунікаційна система**
КЕП	**Кваліфікований електронний підпис**
КМУ	**Кабінет Міністрів України**
Користувач	**Особа, яка має активний доступ до функціональності Системи відповідно до налаштованої ролі**
Система	**Засіб інформатизації, щодо якого створені ці технічні вимоги**
Складові ЄСІКС (складові)	**Інформаційно-комунікаційні системи, функціональні підсистеми та компоненти, їх модулі, базові спільні та інфраструктурні сервіси, які входять в склад ЄСІКС та призначені для виконання певної функціональної задачі**
ТВ	**Технічні вимоги. Документ, що визначає планові потреби Власника Системи 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**
Трембіта	**Системи електронної взаємодії державних електронних інформаційних ресурсів "Трембіта"**
IAM	**Identity Access Management - модуль управління ідентифікацією та доступом**
BI	**Підсистема Business Intelligence в ЄСІКС**
фізична особа ЄСІКС (ФО ЄСІКС, ФО)	**це громадянин України, особа без громадянства, громадянин іншої держави, персональні відомості про яку зареєстровані в ЄСІКС з метою участі цієї особи в процесах, що автоматизуються за допомогою ЄСІКС. Не всі ФО ЄСІКС можуть бути користувачами ЄСІКС, тобто вони можуть бути зареєстровані в ЄСІКС з метою зазначення їх в документах або процесах, але при цьому такі ФО не зареєстровані в якості користувачів та не мають прав на виконання дій в ЄСІКС. Для ведення обліку таких осіб в системі створюється внутрішній майстер-реєстр "Реєстр фізичних осіб ЄСІКС", який оперує обліковими картками ФО, в яких власне і зберігаються персональні відомості про ФО**
авторизований користувач ЄСІКС (користувач)	**це ідентифікована та автентифікована фізична особа ЄСІКС, яка має призначений набір прав на виконання дій в ЄСІКС. Облік користувачів ведеться в сервісі IAM. Обліковий запис (синонім - Облікова картка) користувача містить мінімально необхідний набір персональних даних про ФО, який потрібний для ідентифікації та автентифікації, а також додаткову технічну інформацію, яка стосується технічних аспектів ідентифікації, автентифікації, авторизації, юридичних статусів ФО, сесій та таке інше. Одному обліковому запису користувача відповідає тільки одна активна облікова картка ФО**
профіль користувача в кабінеті користувача	**це окремий розділ (сторінка) в кабінеті користувача, в якому користувачу надається можливість переглянути персональні відомості про себе та виправити те, що можна правити; переглянути поточний та або змінити юридичний статус користувача; переглянути які можливості відповідно до наданих ролей доступні користувачу; переглянути зведену довідкову інформацію з інших складових ЄСІКС, які дотичні до поточного користувача; ініціювати деякі базові процеси**
юридичний статус користувача ЄСІКС (юрстатус)	**це спеціалізований блок інформації, в якому зазначається, від імені кого користувач входить в систему і має намір здійснювати дії. Різні юрстатуси 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 має намір виконувати дії в Системі як посадова особа, що перебуває на певній посаді в певному органі судової влади України. Користувач з таким юрстатусом має отримати ролі та права, що відповідають його посадовим обов'язкам в цьому органі 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 органу в КЕП. Незважаючи на те, що сумісна робота на посадах в судовій владі та держорганах заборонена, технічно один працівник може "посідати" дві посади: одну свою основну, другу — тимчасове виконання обов'язків працівника на іншій посаді, поки він у відпустці або відрядженні. Якщо ці дві посади мають різний, і, особливо конкуруючий набір ролей, Система під час авторизації забезпечує користувачу можливість обрати, з якої саме посади він хоче зараз працювати в Системі;** ● **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 із забезпеченням всіх юридичних вимог до цієї процедури. Користувач в цьому юрстатусі 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 одного конкретного СГ або одну конкретну ФО**
контекст доступу	**це технічний блок інформації, який створюється в результаті процесу авторизації в сервісі IAM та передається складовим ЄСІКС. Містить ідентифікаційну інформацію про користувача; юридичний контекст користувача та його деталі; набір ролей, виданий користувачу; технічні параметри щодо організації сесії користувача для роботи в Системі. Повний перелік має бути визначений в ТЗ**
Електронний кабінет (ЕК)	**це персональна сторінка Користувача в ЄСІКС, 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, Кодекс адміністративного судочинства України, Кримінальний процесуальний кодекс України**
Кабінет користувача (КК)	**це узагальнений функціональний інтерфейс («цифрове робоче місце») будь-якої особи, зареєстрованої в Системі (працівника суду, ВРП, ВККС, 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)
Єдиний персональний простір користувача (ЄППК)	**це 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.**

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. **Закон України “Про судоустрій і статус суддів”**
3. **Закон України “Про Вищу раду правосуддя”**
4. **Закон України “Про Вищий антикорупційний суд”**
5. **Закон України “Про запобігання корупції”**
6. **Закон України “Про державну службу”**
7. **Закон України “Про інформацію”**
8. **Закон України “Про доступ до публічної інформації”**
9. **Закон України “Про публічні електронні реєстри”**
10. **Закон України “Про захист персональних даних”**
11. **Закон України “Про електронні документи та електронний документообіг”**
12. **Закон України “Про електронну ідентифікацію та електронні довірчі послуги”**
13. **Закон України “Про захист інформації в інформаційно-комунікаційних системах”**
14. **Закон України “Про основні засади забезпечення кібербезпеки України”**
15. **Постанова КМУ від 21 лютого 2025 р. № 205 “Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації”**
16. **Постанова КМУ від 28 червня 2024 р. № 764 "Деякі питання електронної ідентифікації та електронних довірчих послуг"**
17. **Положення про порядок функціонування окремих підсистем Єдиної судової інформаційно-телекомунікаційної системи, затверджене Рішенням ВРП від 17.08.2021 р. № 1845/0/15-21**
18. **ISO/IEC 19510 — Інформаційні технології — Нотація моделювання бізнес-процесів BPMN версії 2.0**
19. **ISO/IEC 1012 (серія стандартів) — Вимоги до випробувань електронного обладнання**
20. **ISO 9001 — Системи управління якістю — Вимоги**
21. **ISO/IEC 25010 — Системна та програмна інженерія — Вимоги та оцінювання якості систем і програмного забезпечення (SQuaRE) — Моделі якості систем і ПЗ**
22. **ISO/IEC 8807 — Інформаційні технології — Телекомунікації та обмін інформацією між системами — Протокол внутрішньодоменної маршрутизації IS-IS**
23. **ISO/IEC 9126 — Програмна інженерія — Якість програмного продукту (попередник ISO/IEC 25010)**
24. **ISO/IEC 12207 — Системна та програмна інженерія — Процеси життєвого циклу програмного забезпечення**
25. **IETF BCP 47 — стандарт позначення мовних тегів в поєднанні з кодами країн**
26. **ДСТУ 4145-2002 — Інформаційні технології. Криптографічний захист інформації. Електронний цифровий підпис на основі еліптичних кривих**
27. **RFC 5545 — Специфікація об’єктів календаря та планування iCalendar**

28. NIST / FIPS (серія стандартів) — Стандарти Національного інституту стандартів і технологій США та Федеральні стандарти обробки інформації (криптографія та кібербезпека)

2 ПРИЗНАЧЕННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ

2.1 Основні завдання та функції засобу інформатизації

Ключовими функціями компонентів Системи є:

Забезпечення функціонування Системи як єдиного цифрового середовища з централізованим управлінням доступом, користувачами, організаціями та ролями. Він має забезпечувати ідентифікацію, автентифікацію та авторизацію користувачів, ведення журналів доступу і дій, а також підтримку нормативно-довідкової інформації, майстер-реєстрів і класифікаторів як єдиного джерела достовірних даних для всіх функціональних компонентів Системи.

Забезпечення функціонування засобу інформатизації у межах уніфікованої інфраструктури ЄСІКС, яка формує спільне технологічне середовище для розгортання, експлуатації та масштабування всіх сервісів Системи. Така інфраструктура повинна забезпечувати реалізацію єдиних підходів до моніторингу, журналювання, управління конфігураціями та інформаційної безпеки, а також підтримку надійності, безперервності та керованості функціонування Системи з урахуванням вимог до масштабованості та відмовостійкості.

Перелік ключових функцій не є остаточним та може бути уточнений на етапі розробки технічного завдання.

2.2 Очікувані результати від впровадження засобу інформатизації

Впровадження модулів управління ідентифікацією та доступом, базових довідників і спільних сервісів, а також уніфікованої інфраструктури в рамках ЄСІКС дозволить досягти наступних результатів:

- **Забезпечення єдиного підходу до управління доступом — централізована автентифікація користувачів для всіх сервісів ЄСІКС з розмежуванням ролей і прав, а також авторизація сервісів.**
- **Підвищення рівня інформаційної безпеки — зменшення ризиків несанкціонованого доступу, підвищення прозорості дій користувачів та можливості повного аудиту подій доступу і використання системи.**
- **Уніфікація нормативно-довідкової інформації та функціоналу — використання єдиних довідників і спільних майстер-реєстрів забезпечує узгодженість даних, скорочення дублювання функціоналу та підвищення якості взаємодії між сервісами.**
- **Зниження витрат на розробку та супровід — перевикористання спільних компонентів і уніфікованої інфраструктури скорочує витрати на створення, підтримку та модернізацію складових ЄСІКС.**
- **Підвищення масштабованості та керованості системи — єдині підходи до розгортання, моніторингу та експлуатації дозволяють швидко підключати нові складові ЄСІКС та адаптувати ЄСІКС до змін навантаження і функціональних вимог.**
- **Покращення користувацького досвіду — єдина автентифікація, узгоджені інтерфейси взаємодії та передбачувана поведінка складових ЄСІКС спрощують роботу користувачів і зменшують операційне навантаження.**

2.3 Порядок розвитку засобу інформатизації

Розвиток ЄСІКС здійснюється поетапно з дотриманням принципів модульності, масштабованості, сумісності та перевикористання програмних компонентів. Поточна ітерація розвитку Системи спрямована на формування архітектурного фундаменту, що включає впровадження модуля управління ідентифікацією та доступом (IAM), базових довідників і спільних сервісів, а також розгортання уніфікованої інфраструктури.

Зазначені компоненти формують спільне технологічне середовище та організаційну основу для функціонування всіх складових ЄСІКС і визначають єдині підходи до управління доступом, інформаційної безпеки та експлуатації Системи.

У подальших ітераціях розвитку передбачається поетапне розширення функціональних можливостей існуючих модулів, а також впровадження нових функціональних компонентів відповідно до визначених пріоритетів і потреб користувачів. Розвиток Системи здійснюватиметься з урахуванням необхідності інтеграції з існуючими інформаційними системами, забезпечення сумісності з зовнішніми сервісами та підтримки нових бізнес-процесів і користувацьких сценаріїв.

Такий підхід до розвитку забезпечує еволюційне нарощування функціональності ЄСІКС без порушення стабільності базових компонентів, збереження цілісності даних і безперервності функціонування Системи, а також дозволяє гнучко адаптувати її до змін нормативно-правових, організаційних та технологічних вимог.

3 ХАРАКТЕРИСТИКИ ОБ'ЄКТА ІНФОРМАТИЗАЦІЇ

Об’єктом інформатизації є Єдина судова інформаційно-комунікаційна система (ЄСІКС) — інтегрована інформаційна система, що являє собою сукупність взаємопов’язаних функціональних компонентів, сервісів та програмно-технічних засобів, які забезпечують автоматизацію процесів діяльності судів, органів та установ у системі правосуддя, а також електронну інформаційну взаємодію між ними.

З метою забезпечення єдності, узгодженості та економічної ефективності функціонування Системи, а також недопущення фрагментації підходів до управління доступом, даними та інфраструктурою, архітектура ЄСІКС передбачає впровадження єдиного централізованого рішення зі спільними функціональними компонентами та сервісами, обов’язковими для використання всіма складовими ЄСІКС. Такий підхід забезпечує перевикористання сервісів і даних, уніфіковану реалізацію однотипної функціональності та актуальність інформації.

До складу спільних функціональних компонентів ЄСІКС належать базові сервіси керування ідентифікацією та доступом користувачів, ведення нормативно-довідкової інформації, інформування про події в Системі, перевірки та накладення кваліфікованих електронних підписів, а також сервіси роботи з знаннями та інформаційними матеріалами. Зазначені компоненти забезпечують централізоване управління доступом до ресурсів Системи, облік та контроль дій користувачів, а також уніфікований підхід до роботи з даними та документами.

Функціонування ЄСІКС здійснюється на основі уніфікованої інфраструктури, спільної для всіх її складових, яка забезпечує стандартизовані підходи до розгортання, експлуатації, масштабування та моніторингу, а також реалізацію вимог інформаційної безпеки. Така інфраструктура є технологічною основою стабільної роботи та подальшого розвитку ЄСІКС.

4 ВИМОГИ ДО ЗАСОБУ ІНФОРМАТИЗАЦІЇ

4.1 Вимоги до структури та функціонування засобу інформатизації

Функціональна схема сформована на основі Концепції ЄСІКС, але не обмежується нею і може бути уточнена в процесі реалізації.

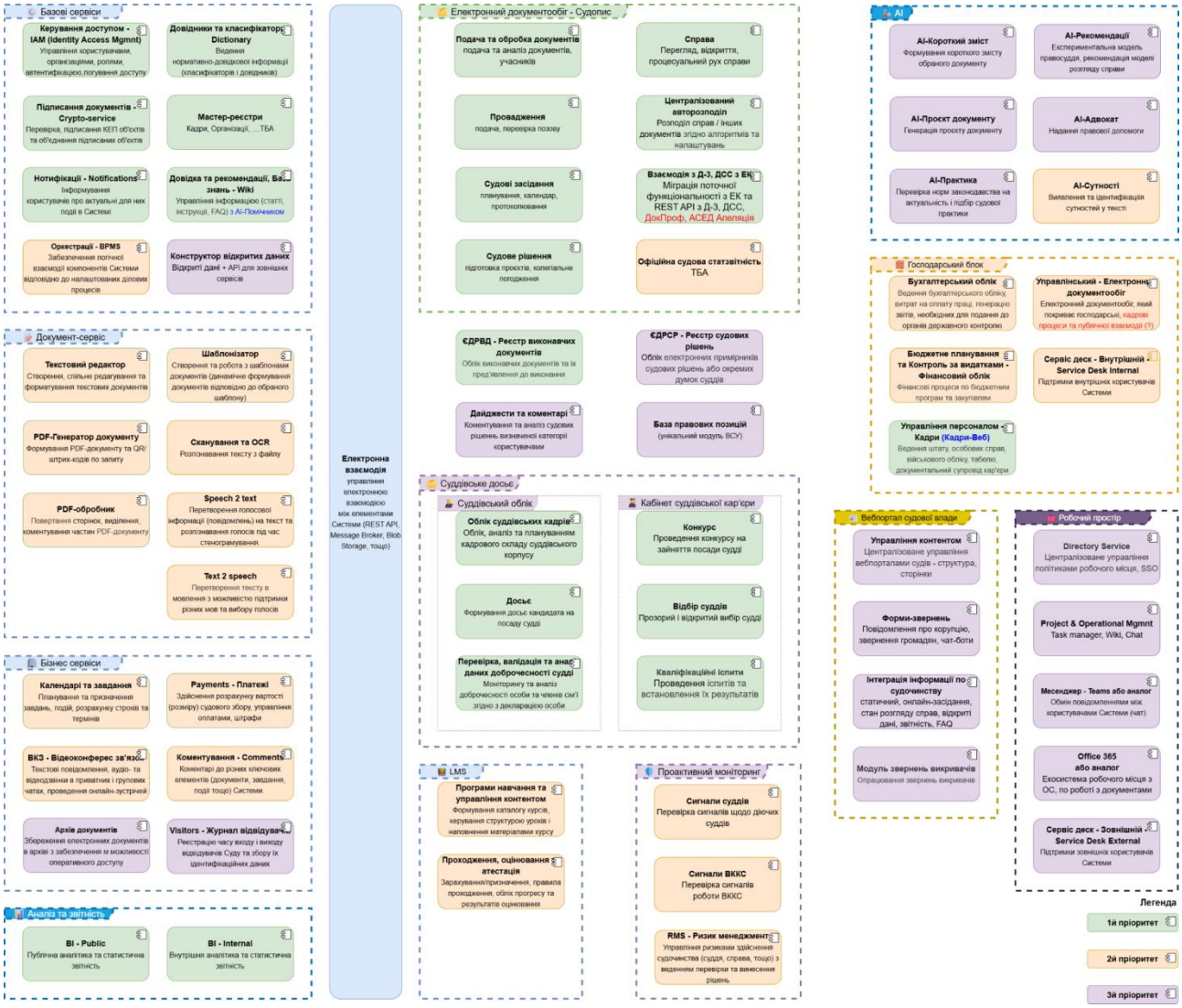

Рис - Функціональна схема Системи

4.2 Вимоги до функцій, що виконуються засобом інформатизації

Опис ключових функцій складових Системи, яка має бути покрита розробкою даного документу:

1. **Базові сервіси складають спільну технологічну платформу (ядро) Системи та забезпечують виконання наступних функцій:**
   - **1.1. Управління ідентифікацією та доступом (IAM): централізована реєстрація користувачів, налаштування ролей та прав доступу, а також ідентифікація, автентифікація, авторизація користувачів з повним логуванням дій.**
   - **1.2. Ведення довідників та нормативно-довідкової інформації (НДІ): створення та підтримка єдиних класифікаторів, системних довідників та майстер-реєстрів, що забезпечують цілісність даних у всіх підсистемах.**
   - **1.3. Криптографічний сервіс: забезпечення юридичної значущості документів через механізми накладення та перевірки КЕП, а також робота з пакетами підписаних даних.**

1.4. **Сервіс сповіщень та нотифікацій: оперативне інформування користувачів про системні події, події бізнес-процесів та задачі через внутрішні та зовнішні канали зв'язку.**

1.5. **Інформаційна підтримка та База знань: ведення електронної документації, інструкцій та відповідей на типові запитання (Wiki/FAQ) для допомоги користувачам у реальному часі.**

1.6. **Сервіс роботи з майстер-реєстрами: облік та реєстрація базових облікових об'єктів та суб'єктів ЄСІКС (органи судової влади включаючи перелік підрозділів та посад, юридичні особи/фізичні особи-підприємці, фізособи, представники, працівники органів судової влади, судді та інше).**

1.7. **Єдиний персональний простір користувача: інструментарій для створення та управління елементами інтерфейсу в кабінеті користувача.**

2. **УНІФІКОВАНОЇ ІНФРАСТРУКТУРИ, спільної для складових ЄСІКС, що забезпечує стандартизовані підходи до розгортання, експлуатації, масштабування, моніторингу та інформаційної безпеки.**

4.3 Основні бізнес-процеси

КЕРУВАННЯ ДОСТУПОМ

Управління ідентифікацією та доступом (далі - IAM) забезпечує бізнес-процеси централізованої реєстрації та обліку, груп і користувачів, призначення ролей і прав доступу відповідно до повноважень, автентифікації та авторизації користувачів при доступі до сервісів Системи, а також управління життєвим циклом доступів, включаючи надання, зміну та відкликання прав. У межах сервісу також реалізуються бізнес-процеси фіксації подій автентифікації, авторизації і доступу з подальшою передачею їх у централізований сервіс логування з метою забезпечення контролю та інформаційної безпеки.

БАЗОВІ ДОВІДНИКИ ТА СПІЛЬНІ СЕРВІСИ

Базові довідники та спільні сервіси забезпечують бізнес-процеси формування, ведення, актуалізації та надання уніфікованої нормативно-довідкової інформації для використання всіма сервісами Системи, а також бізнес-процеси перевикористання типового функціоналу, зокрема підписання електронних об'єктів, відправлення системних повідомлень і сповіщень, обміну даними між складовими Системи та зовнішніми інформаційними системами. Реалізація зазначених процесів спрямована на забезпечення узгодженості даних, скорочення дублювання функціоналу та підвищення ефективності підтримки бізнес-процесів користувачів в Системі.

4.4 Опис ролей та доступу користувачів Системи

Рольова модель може включати як ролі кінцевих користувачів, орієнтовані на обробку інформації, так і ролі з розширеними повноваженнями, призначені для адміністрування, підтримки та забезпечення безпеки Системи.

Наведена нижче рольова модель є прикладом концептуального розподілу ролей у Системі та може бути використана як основа (з можливістю змін та/або доповнень) для подальшої деталізації прав доступу, налаштування ролей і їхньої адаптації відповідно до організаційної структури та потреб користувачів Системи. Це метамодель, яка не обмежує перелік ролей підсистем.

Аліас	Назва	Опис

P1 admin_users	**Адміністратор користувачів**	**Роль, відповідальна за ведення та актуалізацію облікових записів користувачів у Системі, призначення та зміну ролей і прав доступу відповідно до повноважень, а також контроль коректності доступу користувачів до функціоналу та даних ЄСІКС. У межах своєї ролі Адміністратор користувачів здійснює створення, оновлення, блокування та деактивацію облікових записів, забезпечує підтримку життєвого циклу доступів користувачів. Система має забезпечувати можливість керування дозволами адміністраторів, щоб забезпечити можливість конфігурування адмінського доступу.**
P2 admin_organisations	**Адміністратор організацій**	**Роль, відповідальна за ведення, актуалізацію та контроль даних організацій у Системі, включно зі створенням, оновленням і деактивацією облікових записів організацій, управлінням їх структурою та основними атрибутами. У межах своєї ролі Адміністратор організацій забезпечує коректність і цілісність організаційних даних, використання уніфікованих довідників.**

4.4.1 Ролі та права доступу

Система повинна керувати доступом користувачів до функцій і даних за двома основними принципами:

- **за ролями**
- **за атрибутами.**

При цьому система має бути гнучкою, щоб у майбутньому можна було додати інші способи контролю доступу, якщо це буде потрібно. Має бути можливість підключення та/або зміни контролю доступу до кожної окремої підсистеми за необхідності.

Як основні моделі контролю доступу користувачів та інших систем, Виконавець повинен використовувати RBAC та ABAC для розмежування прав доступу користувачів до об'єктів ЄСІКС.

Функціонал керування доступом має також передбачати можливість впровадження додаткових моделей контролю доступу, необхідних для інших підсистем.

Перелік ролей, а також набір прав доступу для кожної ролі є концептуальним і може бути уточнений та доповнений у процесі розробки технічного завдання з урахуванням вимог Власника Системи, особливостей бізнес-процесів та нормативних обмежень. Остаточний склад ролей та відповідні їм права доступу мають бути визначені та описані в документі технічного завдання.

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

✓ - доступ дозволено;

✓ + контекст - доступ обмежений з урахуванням визначеного контексту;

Відсутність інформації — доступу немає.

Сутність	Функція	Адміністратор користувачів	Адміністратор користувачів організації	Адміністратор організацій
Користувачі	Переглянути реєстр користувачів	✓ (усі користувачі)	✓ (своєї організації)	
	Переглянути картку користувача	✓	✓ (своєї організації)	

	Створити користувача	✓	✓ **(своєї організації)**	
	Редагувати картку користувача	✓	✓ **(своєї організації)**	
	Деактивувати користувача	✓	✓ **(своєї організації)**	
	Відновити пароль	✓	✓ **(своєї організації)**	✓
Організації	**Переглянути реєстр організації**	✓		✓
	Переглянути картку організації	✓		✓
	Створити Організацію			✓
	Редагувати картку організації			✓

Перелік ролей не обмежується IAM та може включати ролі підсистем, які реєструються в IAM. Назви та набір сутностей, функцій та ролей є попередніми та можуть бути уточнені в процесі розробки Системи.

5 ФУНКЦІОНАЛЬНІ ВИМОГИ

5.1 Керування доступом - управління ідентифікацією та доступом (IAM)

Призначення IAM забезпечує централізовану автентифікацію користувача, управління користувачами, ролями, правами доступу, сесіями та аудитом дій у межах ЄСІКС. Також сервіс має підтримувати механізми наповнення та зворотного зв'язку даних із існуючих підсистем.

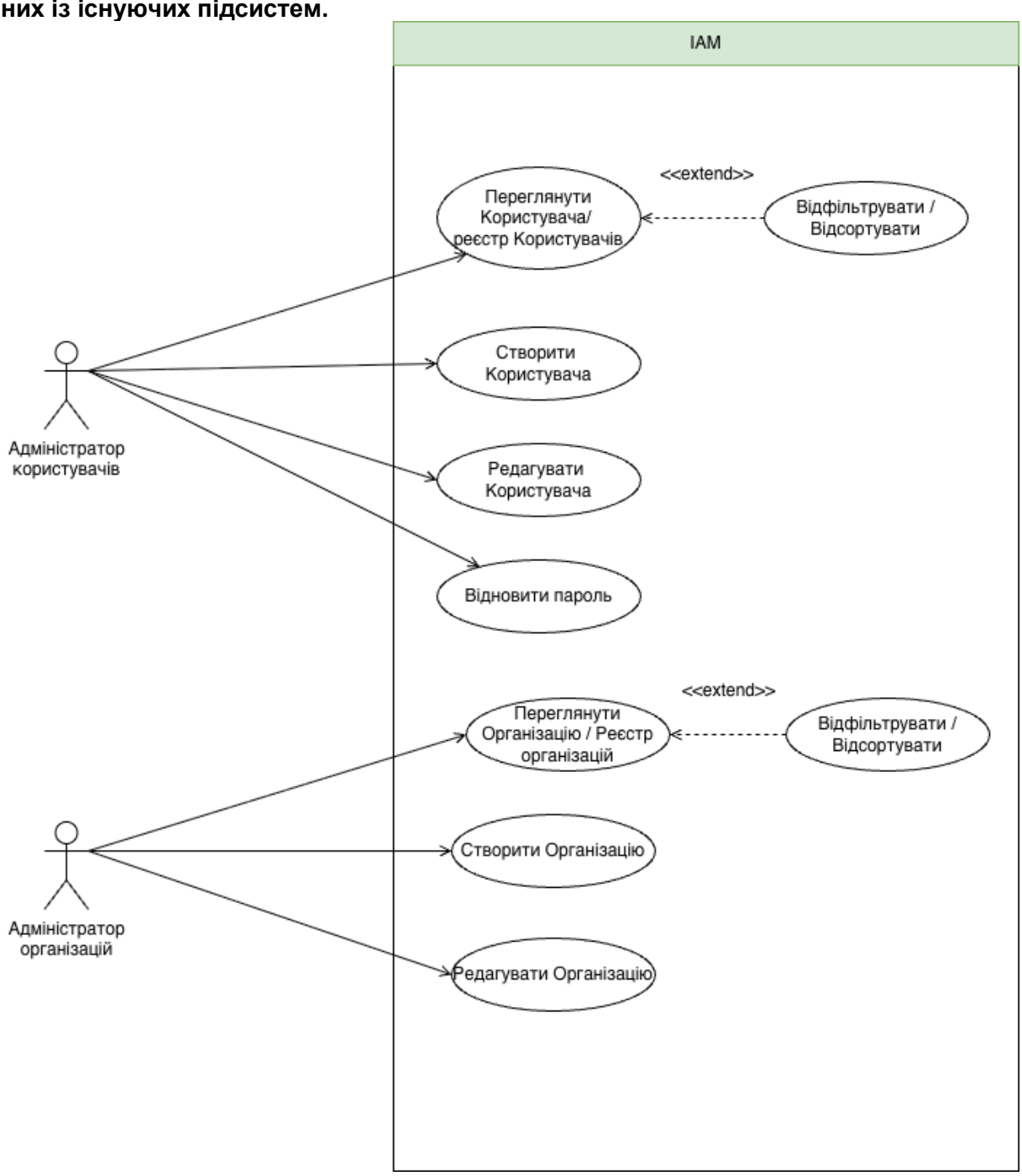

Рис - Use-case по управлінню користувачами та організаціями

1. **Автентифікація та керування сесіями**
   - 1.1. **Система повинна забезпечувати централізовану ідентифікацію, автентифікацію та авторизацію користувачів ЄСІКС через IAM сервіс.**
   - 1.2. **Система повинна підтримувати автентифікацію з використанням:**
     - 1.2.1. **логіна та пароля (для нерезидентів);**
     - 1.2.2. **двофакторної автентифікації (OTP за узгодженим стандартом або еквівалент) з можливістю налаштування часу дії коду;**
     - 1.2.3. **кваліфікованого електронного підпису на захищеному носії або у захищеній хмарі (КЕП), у випадках, визначених законодавством та політиками безпеки Системи;**
     - 1.2.4. **кваліфікованого електронного підпису у вигляді файлу (УЕП), у випадках, визначених законодавством та політиками безпеки Системи;**
     - 1.2.5. **автентифікація засобами, визначеними eIDAS;**
     - 1.2.6. **з використанням BankID**
   - 1.3. **Система має надавати можливість призначення способу автентифікації окремому користувачу або групі користувачів з урахуванням їх юридичних статусів, або вручну адміністратором, або автоматично на підставі додаткових ознак, які будуть остаточно визначені на етапі розробки ТЗ (наприклад, спосіб автентифікації з використанням КЕП на захищеному носії призначається посадовцям органів судової влади).**
   - 1.4. **Для користувачів, які не мають КЕП української посадової чи фізичної особи, обліковий запис може створювати лише Адміністратор Системи.**
   - 1.5. **Система повинна підтримувати механізми захисту від автоматизованих спроб доступу (CAPTCHA або аналогічні механізми).**
   - 1.6. **Система повинна підтримувати файловий, апаратний та хмарний КЕП.**
   - 1.7. **Система повинна забезпечувати інтеграцію з кваліфікованими надавачами електронних довірчих послуг, провайдером BankID автентифікації та підтримувати eIDAS.**
     Адміністратор повинен мати змогу визначити, до яких підсистем та їх елементів користувач має доступи залежно від способу автентифікації.
   - 1.8. **Користувач повинен мати змогу авторизуватися за допомогою КЕП з перевіркою:**
     - 1.8.1. **чинності сертифіката;**
     - 1.8.2. **строку дії;**
     - 1.8.3. **статусу сертифіката;**
     - 1.8.4. **відповідності інших реквізитів (приналежність до організації, посади).**
   - 1.9. **Якщо перевірка КЕП або BankID або логіну/паролю неуспішна, система повинна відмовити в доступі та повідомити користувача про причину з наданням посилання на довідкові матеріали щодо вирішення проблеми та отримання технічної підтримки.**
   - 1.10. **Система повинна забезпечувати механізм єдиного входу (Single Sign-On) для доступу до складових Системи без повторної автентифікації та проміжних редиректів.**
   - 1.11. **Система повинна забезпечувати керування сесіями користувачів, включаючи:**
     - 1.11.1. **налаштування обмеження кількості одночасних сесій (наприклад до 5);**
     - 1.11.2. **налаштування автоматичного завершення сесії у разі бездіяльності упродовж певного часу, який може визначатися для окремих підсистем (модулів, сервісів) ЄСІКС;**
     - 1.11.3. **обмеження часу активності сесії;**
     - 1.11.4. **відкликання сесій;**
     - 1.11.5. **примусове завершення сесій Адміністратором або системою безпеки;**
     - 1.11.6. **фіксацію входів та випадків паралельних входів з логуванням IP-адреси, даних пристрою, звідки здійснювався вхід.**

1.12. Система повинна видавати токени доступу (наприклад, JWT) для інтеграції з іншими сервісами Системи.
1.13. Система повинна забезпечувати можливість доступу до певних сутностей (документів, файлів, сесій ВКЗ, календаря тощо), зокрема з можливістю встановлення часових інтервалів їх дії, одноразовості запиту.
1.14. Система повинна забезпечувати керування життєвим циклом облікових записів користувачів (створення, активація, блокування, деактивація).

2. Підтримка стандартних протоколів автентифікації та авторизації
2.1. Система повинна підтримувати стандартні протоколи (наприклад, OAuth 2.0 та/або OpenID Connect (OIDC)) як основний механізм взаємодії між IAM та сервісами Системи, наприклад:
2.1.1. єдиного входу користувачів до сервісів Системи;
2.1.2. доступу клієнтських застосунків до API сервісів Системи;
2.1.3. взаємодії між системами (machine-to-machine).
2.2. Система повинна забезпечувати централізоване управління клієнтами, включаючи:
2.2.1. реєстрацію клієнтів;
2.2.2. налаштування дозволених redirect URI;
2.2.3. обмеження дозволених потоків.
2.3. Система повинна видавати токени доступу, що містять ідентифікатори користувача та контекст доступу, необхідний сервісам Системи для перевірки прав та подальшої авторизації.
2.4. Система повинна забезпечувати відкликання, перевірку чинності та обмеження строку дії токенів доступу відповідно до політик безпеки Системи шляхом налаштування без необхідності внесення змін в код.

3. Рольова модель та ідентифікація
3.1. Система повинна реалізовувати доступ користувачів на основі ролей (RBAC) з можливістю призначення однієї або кількох ролей одному користувачу, а також атрибутів (ABAC).
3.2. Система повинна дозволяти копіювання ролі з подальшим редагуванням.
3.3. Система повинна забезпечувати підтримку режимів доступу на основі рівня автентифікації користувача, зокрема:
3.3.1. анонімний доступ;
3.3.2. авторизований доступ;
3.4. IAM повинен визначати режим доступу на підставі результатів автентифікації та застосовувати відповідні політики контролю доступу.
3.5. Система повинна забезпечувати перегляд об’єктів обліку та переліку доступних системних прав для кожного об’єкта.
3.6. Система повинна підтримувати перевірку доступу на основі поєднання:
3.6.1. ролей користувача;
3.6.2. атрибутів користувача (наприклад, суд, орган, статус);
3.6.3. типу запитуваної дії (читання, створення, редагування, затвердження тощо).
3.7. Система повинна забезпечувати передачу сервісам Системи інформації про ролі користувача, які інтерпретуються сервісами Системи як набір дозволів на перегляд, редагування або інші дії з інформаційними об’єктами.
3.8. Система повинна забезпечувати ведення централізованого реєстру ролей ЄСІКС як системних об’єктів доступу.
3.9. Виконавець має розробити інструмент реєстрації користувацьких ролей та політик і надати можливість розробникам інших Підсистеми реєструвати свої локальні ролі та політики у базовому IAM сервісі.

4. Управління користувачами
4.1. Система повинна забезпечувати ведення централізованого списку користувачів IAM.
4.2. Адміністратор повинен мати змогу переглядати повний перелік користувачів з фільтрацією та пошуком.

4.3. Система повинна забезпечувати реєстрацію нового користувача з перевіркою унікальності (РНОКПП, УНЗР, серія та номер паспорта).
4.4. Система повинна підтримувати процес запрошення користувача з підтвердженням реєстрації.
4.5. Користувач повинен отримувати доступ до Системи (кабінету користувача) після успішної авторизації.
4.6. Адміністратор повинен мати змогу:
4.6.1. редагувати ролі користувача;
4.6.2. блокувати та розблоковувати користувача;
4.6.3. переглядати історію сесій користувача.
4.7. Блокування користувача повинно відбуватися на рівні юридичного статусу користувача (наприклад, він може бути заблокований як посадова особа, але одночасно мати доступ як проста фізособа).
4.8. Система повинна підтримувати повноцінну CRUD-модель картки користувача, включаючи:
4.8.1. створення;
4.8.2. перегляд;
4.8.3. редагування;
4.8.4. деактивацію.
4.9. Картка користувача повинна містити ідентифікаційні, атрибутивні та організаційні дані, необхідні для:
4.9.1. автентифікації;
4.9.2. авторизації;
4.9.3. застосування політик доступу.
4.10. Система повинна підтримувати управління атрибутами користувачів, які використовуються для авторизації, з можливістю їх оновлення з зовнішніх джерел (довідники, кадрові системи тощо).
4.11. Система повинна забезпечувати можливість налаштування політик доступу без внесення змін у код сервісів Системи.
4.12. Система повинна забезпечувати зв'язок користувача з організацією, якщо така інформація використовується в моделях доступу Системи.
4.13. Система повинна підтримувати управління групами користувачів, включаючи:
4.13.1. створення, редагування та видалення груп;
4.13.2. призначення ролей групам користувачів;
4.13.3. автоматичне застосування ролей до користувачів, включених до групи;
4.13.4. налаштування ролей за замовчуванням для груп користувачів;
4.13.5. перегляд складу груп та їх ролей;
4.13.6. встановлення батьківських груп.

5. Делегування повноважень
5.1. Система повинна підтримувати делегування повноважень користувачів, включаючи:
5.1.1. тимчасове делегування ролей або прав іншому користувачу;
5.1.2. встановлення строку дії делегування;
5.1.3. делегування адміністратором або користувачем;
5.1.4. автоматичне припинення делегованих прав після завершення строку;
5.1.5. аудит делегування повноважень;
5.1.6. делегування може бути багаторівневим.

6. Події безпеки, аудитні сліди та інтеграція з логуванням
6.1. Система повинна фіксувати події безпеки, пов'язані з:
6.1.1. атрибутами Користувача (IP адреса, деталі по пристроям);
6.1.2. спробами автентифікації;
6.1.3. успішною та неуспішною автентифікацією;
6.1.4. змінами ролей, атрибутів та політик доступу;
6.1.5. блокуванням або розблокуванням облікових записів.

6.2. IAM сервіс не повинен реалізовувати централізований аудит, аналітику або моніторинг подій, а лише формувати аудитні події у структурованому вигляді та передавати їх до централізованого компонента логування та моніторингу Системи.

7. Нотифікації IAM сервісу

Сервіс IAM має забезпечити генерацію нотифікацій для передачі через сервіс нотифікації щодо наступних подій:

7.1. Реєстрація користувача;

7.2. Будь-яка зміна в атрибутах облікового запису користувача;

Точний перелік подій, щодо яких потрібно генерувати нотифікації користувачам, має бути визначений в ТЗ.

8. Інтеграція з сервісами Системи

8.1. Система повинна надавати іншим складовим ЄСІКС програмні засоби взаємодії:

8.1.1. перевірки ролей доступу;

8.1.2. отримання ідентифікаційних та атрибутивних даних користувача.

8.2. Система повинна бути єдиною точкою керування доступом до Системи, але не є джерелом бізнес-даних.

8.3. Сервіси Системи повинні мати змогу звертатися до IAM у режимі реального часу для перевірки ролей доступу до конкретної дії або ресурсу.

8.4. Система повинна забезпечувати надання складовим Системи стандартизованого контексту доступу користувача, що включає:

8.4.1. ідентифікатор користувача;

8.4.2. перелік призначених ролей;

8.4.3. членство в групах;

8.4.4. атрибути користувача, що використовуються для процедури перевірки.

9. Інформація про організацію

9.1. Система повинна підтримувати можливість ведення списку організацій, які можуть використовуватись:

9.1.1. як атрибути користувачів;

9.1.2. як контекст для авторизації та політик доступу.

9.2. Система повинна підтримувати CRUD-операції для організацій, включаючи:

9.2.1. створення;

9.2.2. перегляд;

9.2.3. редагування;

9.2.4. деактивацію (soft delete).

9.3. Система має підтримувати процедуру автоматичного створення організацій в сервісі IAM та оновлення відомостей про неї з відповідного майстер-реєстру організацій.

10. Сервіс IAM має забезпечити наступні функції авторизації:

10.1. Система повинна містити окремий сервіс авторизації, що виконує ролі точки прийняття рішень та точки управління політиками.

10.2. Сервіс повинен забезпечувати управління реєстрами об'єктів захисту та визначення допустимих дій над ними.

10.3. Сервіс повинен забезпечувати можливість створення та зберігання політик доступу, що базуються на поєднанні атрибутів користувача, ресурсу, ролі та контексту запиту.

10.4. Сервіс повинен надавати прикладним підсистемам інтерфейс для отримання дозволів у режимі реального часу.

10.5. Функціональні складові Системи (Додатки) повинні виступати точками виконання політик, звертаючись за необхідності до сервісу перед виконанням операцій.

10.6. Певні складові підсистеми можуть являти собою повністю готові рішення (наприклад, підсистема бухгалтерського, кадрового обліку, поточно існуючі системи) і з власним повнофункціональним механізмом регуляції

та контролю доступу користувачів до дій та ресурсів. Для таких підсистем сервіс IAM має забезпечити виконання лише функції SSO.

5.2 Базові сервіси

5.2.1 Довідники та класифікатори

Сфера застосування:

- **Ведення нормативно-довідкової інформації (НДІ) та централізованих реєстрів;**
- **Забезпечення всіх сервісів Системи еталонними, юридично значущими даними, що виключає дублювання та розсинхронізацію з маскуванням процесів, які формують ці дані.**

Сервіс підтримує два типи довідників:

- **централізовані (для всіх підсистем) динамічні:**
  - **мають адміністративний інтерфейс**
  - **дозволяють додавання / редагування / деактивацію значень**
  - **підтримують версійність**
  - **використовуються кількома підсистемами чи сервісами**
- **централізовані (для всіх підсистем) статичні:**
  - **наповнюються через реліз**
  - **не редагуються користувачами**
  - **використовуються кількома підсистемами чи сервісами.**

Сервіс повинен забезпечувати:

1. **інструмент створення довідників;**
2. **централізоване зберігання довідників;**
3. **CRUD-операції над записами довідників відповідно до типу довідника;**
4. **деактивацію записів без фізичного видалення;**
5. **блокування редагування або видалення записів, які вже використовуються в даних підсистем;**
6. **ведення історії змін та версій довідників;**
7. **підтримку ієрархічних довідників;**
8. **можливість ведення множинних мовних форм (включаючи різні відмінки);**
9. **експорт довідників через API;**
10. **автоматичне оновлення довідників через інтеграційні механізми (за наявності);**
11. **пошук, фільтрацію та сортування;**
12. **аудит змін довідників;**
13. **керування правами доступу до адміністрування довідників.**

Точний перелік та наповнення довідників визначаються кожною складовою ЄСІКС під час детального аналізу предметної області цієї підсистеми та мають бути зафіксовані в ТЗ на цю підсистему. Виконавець має врахувати, що в середньому на кожну складову очікується 5–20 довідників та/або класифікаторів. Також очікується, що здебільшого довідники будуть лінійні, в форматі "key: value", але також будуть декілька ієрархічних довідників (наприклад, КАТОТГ — один з довідників в методології формування географічної адреси) та декілька ієрархічно-фасетних класифікаторів як от "Класифікатор типів документів".

5.2.2 Нотифікації

Сервіс нотифікацій призначений для централізованого формування, обробки, доставки та зберігання повідомлень користувачам Системи із використанням визначених каналів нотифікації на підставі подій, що виникають в підсистемах ЄСІКС. Сервіс забезпечує вибір та застосування каналів доставки повідомлень, зокрема електронної пошти, SMS, push-повідомлень в одному з популярних месенджерів та внутрішніх повідомлень у Системі, відповідно до типу події та сценарію використання.

У межах сервісу забезпечується підтримка редагованих шаблонів нотифікацій для різних типів повідомлень, що дозволяє уніфікувати зміст і формат повідомлень, забезпечити їх коректне та однакове відображення для всіх користувачів, а також централізовану доставку повідомлень.

Сервіс нотифікацій повинен забезпечувати:

1. **Подієву модель формування нотифікацій:**
   - 1.1. **формування нотифікацій на підставі подій, отриманих від інших підсистем та сервісів;**
   - 1.2. **підтримку інтеграційного API, в тому числі із зовнішніми сервісами (наприклад Viber), або меседж брокера для передачі подій підсистемами;**
   - 1.3. **обробку подій незалежно від бізнес-логіки підсистем.**
2. **Підтримку класифікації нотифікацій за типами, зокрема:**
   - 2.1. **сервісні (технічні повідомлення, помилки, оновлення, безпекові події);**
   - 2.2. **користувацькі;**
   - 2.3. **нотифікації про строки;**
   - 2.4. **нотифікації щодо документів або процесів;**
   - 2.5. **інші типи, визначені адміністратором Системи.**
3. **Персональні налаштування отримання нотифікацій:**
   - 3.1. **можливість активації або деактивації типів нотифікацій;**
   - 3.2. **вибір каналів доставки для кожного типу;**
   - 3.3. **налаштування часових рамок отримання повідомлень;**
   - 3.4. **налаштування підписки на події або об’єкти;**
   - 3.5. **централізоване зберігання налаштувань користувача.**
4. **Централізоване адміністрування:**
   - 4.1. **визначення типів нотифікацій;**
   - 4.2. **керування доступними каналами доставки;**
   - 4.3. **налаштування шаблонів повідомлень;**
   - 4.4. **визначення нотифікацій, налаштування яких користувачу недоступне;**
   - 4.5. **управління категоріями повідомлень.**
5. **Зберігання та історію нотифікацій:**
   - 5.1. **збереження створених нотифікацій;**
   - 5.2. **збереження інформації про канал доставки;**
   - 5.3. **статуси виконання нотифікацій (нова, прочитана, оброблена тощо);**
   - 5.4. **зміну статусу користувачем або автоматично;**
   - 5.5. **можливість масових операцій над нотифікаціями;**
   - 5.6. **генерацію квітанцій про доставку;**
   - 5.7. **побудову звітів відправлених/отриманих нотифікацій з можливістю налаштування параметрів відображення через адмін панель. Конкретний список звітів має бути уточнений на рівні технічного завдання.**
6. **Категоризацію та групування:**
   - 6.1. **різний пріоритет роботи з нотифікаціями базуючись на категорії нотифікації;**
   - 6.2. **групування нотифікацій за категоріями;**
   - 6.3. **фільтрацію повідомлень за типом або джерелом.**
7. **Взаємодію з іншими сервісами та підсистемами:**
   - 7.1. **Сервіс використовується всіма підсистемами ЄСІКС.**
   - 7.2. **Підсистеми визначають події та умови відправлення нотифікацій.**
   - 7.3. **Сервіс не містить бізнес-логіки підсистем.**
8. **Імпорт історичних наявних даних.**
9. **Взаємодію із зовнішніми провайдерами доставки повідомлень:**
   - 9.1. **Інтеграція з мобільним застосунком "Дія" (Push-сповіщення);**
   - 9.2. **Доставка через офіційні чат-боти (Viber, Telegram, WhatsApp);**
   - 9.3. **Інтеграція з провайдерами доставки SMS-повідомлень за стандартними протоколами взаємодії.**

5.2.3 Підписання документів - Крипто-сервіс

Система має підтримувати на рівні єдиного простору користувача:

- **інтеграцію з системою електронної ідентифікації ЄСІКС (далі - Віджет ідентифікації ЄСІКС);**
- **інтеграцію з системою електронної ідентифікації id.gov.ua (далі - Віджет ідентифікації id.gov.ua);**
- **інтеграцію з системою електронного підпису ЄСІКС (далі - Віджет підпису ЄСІКС);**
- **інтеграцію з системою електронного підпису id.gov.ua (далі - Віджет підпису id.gov.ua).**

Компонент "Підписання документів" (далі крипто-сервіс) – це сервіс Системи, призначений для:

- **перевірки підписаного об'єкта (наприклад, структуровані дані, файл);**
- **об'єднання підписаного об'єкта та отримання у форматі p7s;**
- **підписання об'єкта.**

Крипто-сервіс повинен:

- **підтримувати роботу з форматами ключів відповідно до постанови КМУ від 12 грудня 2023 р. № 1298 та інших вимог законодавства;**
- **забезпечувати підтримку чинних кваліфікованих надавачів електронних довірчих послуг України;**
- **забезпечувати автоматичне визначення надавача електронних довірчих послуг;**
- **забезпечувати автоматичну перевірку дійсності сертифіката за терміном дії та статусом;**
- **забезпечувати ідентифікацію та верифікацію особи підписувача, отримання атрибутів підписувача з сертифіката;**
- **забезпечувати можливість отримання інформації по типу підпису (КЕП/УЕП);**
- **використовувати виключно сертифіковані засоби криптографічного захисту інформації, що мають чинний позитивний експертний висновок ДССЗЗІ України;**
- **виконувати виключно криптографічні операції та не містити бізнес-логіки підсистем.**

Віджет повинен:

- **підтримувати роботу з файловими, хмарними та апаратними ключами;**
- **надавати можливість накладання УЕП/КЕП без повторного завантаження файлу ключа, вибору сертифікаційного центру та введення пароля протягом активної сесії користувача, але з обов'язковим повідомленням користувача про те, що він підписує цифровий документ або файл;**
- **забезпечити можливість пакетного підписання документів.**

5.2.4 Довідка та рекомендації, База знань - Wiki

Компоненти Системи "Довідка та рекомендації" та "База знань" (далі - сервіс Wiki) призначений для управління знаннями та підтримки користувачів через централізоване накопичення, структурування, актуалізацію та надання знань щодо роботи Системи, функціональними можливостями, бізнес-процесами та правилами користування.

Wiki є спільною функціональною можливістю та використовується всіма складовими Системи для:

- **надання довідкової інформації;**
- **підтримки користувачів у процесі роботи з системою.**

Сервіс Wiki не замінює служби підтримки та не виконує функцій управління інцидентами чи зверненнями.

1. **Загальні принципи управління знаннями**
   - 1.1. **Сервіс повинен забезпечувати централізоване накопичення, зберігання та надання знань для користувачів Системи у вигляді єдиного репозиторію інструктивних, довідкових та методичних матеріалів.**

1.2. Сервіс повинен виступати єдиною точкою доступу до знань щодо:
1.2.1. користування функціоналом Систем;
1.2.2. виконання процесуальних і службових дій;
1.2.3. методичних рекомендацій та регламентів.
1.3. Сервіс не повинен містити бізнес-логіки інших сервісів Системи, а має виконувати допоміжну, інформаційно-довідкову функцію.

2. Типи контенту та консолідація знань
2.1. Сервіс повинен підтримувати зберігання та публікацію таких типів контенту:
2.1.1. текстові статті бази знань;
2.1.2. відповіді на поширені запитання (FAQ) з можливістю їх структуризації за темами та категоріями;
2.1.3. нормативно-правові, організаційно-розпорядчі матеріали, дані щодо практики професійної діяльності тощо;
2.1.4. інструкції та регламенти у форматах PDF та HTML;
2.1.5. методичні рекомендації;
2.1.6. відео-інструкції;
2.1.7. зображення, схеми, скріншоти.
2.2. Сервіс повинен забезпечувати зберігання неструктурованого контенту (файлів) у зовнішньому об'єктному сховищі (Object Storage) без зберігання бінарного вмісту безпосередньо в БД підсистеми.
2.3. Сервіс повинен забезпечувати логічну консолідацію всіх типів контенту в межах єдиного інформаційного простору Бази знань незалежно від формату.
2.4. Сервіс повинен підтримувати систематизацію матеріалів бази знань за категоріями, темами та тегами з можливістю їх використання для навігації, фільтрації та пошуку.

3. Управління життєвим циклом контенту
3.1. Користувач із відповідними повноваженнями повинен мати змогу створювати, редагувати та видаляти статті бази знань.
3.2. Сервіс повинен підтримувати життєвий цикл статті, що може включати наступні стани:
3.2.1. Чернетка;
3.2.2. На погодженні;
3.2.3. Опубліковано;
3.2.4. Архів.
3.3. Якщо стаття перебуває в стані "Чернетка" або "На погодженні", вона не повинна бути доступною кінцевим користувачам.
3.4. Сервіс повинен підтримувати версійність статей, з можливістю:
3.4.1. перегляду історії змін;
3.4.2. порівняння версій;
3.4.3. відновлення попередньої версії без втрати історії.
3.5. Сервіс повинен дозволяти оновлення інструкцій без втрати доступу до попередніх версій, що є критичним у разі змін законодавства або процедур.
3.6. Сервіс повинен забезпечувати збереження інформації про автора змін та особи, що погодила, та дату оновлення матеріалів бази знань.

4. Пошук та індексація знань
4.1. Сервіс повинен забезпечувати пошук по базі знань, включаючи:
4.1.1. заголовки;
4.1.2. текст статей.
4.2. Користувач повинен мати змогу шукати інформацію за ключовими словами, фразами та синонімами.
4.3. Результати пошуку повинні враховувати права доступу користувача, визначені IAM сервісом.

5. Контекстна довідка та рекомендації (Context Engine)
5.1. Сервіс повинен надавати контекстну довідку користувачу залежно від:
5.1.1. сторінки Системи, на якій він перебуває;
5.1.2. дії, яку він виконує;

5.1.3. ролі користувача.

5.2. Якщо користувач перебуває на певній сторінці або виконує визначену дію, система повинна автоматично пропонувати релевантні статті або інструкції.

5.3. Модуль повинен містити механізм зіставлення контексту інтерфейсу (URL, ідентифікатор екрану або дії) з відповідними матеріалами бази знань.

5.4. Підсистеми повинні мати можливість визначати відповідність між елементами інтерфейсу та матеріалами довідки через API сервісу Wiki.

6. Розмежування доступу до контенту:

6.1. Сервіс повинен забезпечувати розмежування доступу до контенту залежно від ролі користувача.

6.2. Якщо користувач не має прав доступу до певного матеріалу, такий матеріал:

6.2.1. не повинен відображатися в пошуку;

6.2.2. не повинен бути доступним через пряме посилання.

6.3. Сервіс повинен використовувати централізований IAM ЄСІКС і не реалізовувати власну систему автентифікації.

7. Зворотний зв'язок та аналітика

7.1. Користувач повинен мати змогу оцінити корисність статті (наприклад, "корисно/не корисно").

7.2. Сервіс повинен зберігати статистику використання контенту, включаючи:

7.2.1. перегляди;

7.2.2. пошукові запити;

7.2.3. оцінки користувачів.

8. Сповіщення та актуалізація знань

8.1. Система повинна ініціювати сповіщення користувачів через механізм підписки у разі оновлення критично важливих інструкцій або методичних матеріалів.

8.2. Сповіщення повинні передаватися через централізований сервіс нотифікацій Системи.

9. Інтерфейс користувача

9.1. Сервіс повинен надавати плаваючий віджет довідки, доступний з будь-якого екрану Системи.

9.2. Сервіс повинен надавати окремий портал Бази знань із:

9.2.1. деревом категорій;

9.2.2. пошуком;

9.2.3. фільтрацією контенту.

9.3. Користувач повинен мати можливість експортувати матеріали бази знань або їх частини у форматах PDF або здійснювати їх друк.

5.2.5 Сервіс майстер-реєстрів

Сервіс майстер-реєстрів призначений для централізованого зберігання та управління базовими обліковими сутностями ЄСІКС. Майстер-реєстри є джерелом істини (Source of Truth) для інших підсистем.

Сервіс забезпечує:

- **формування облікових карток об'єктів та суб'єктів обліку, спільних для складових ЄСІКС;**
- **об'єкти та суб'єкти обліку мають однозначно ідентифікуватися в межах усіх складових ЄСІКС;**
- **фіксацію історичності змін, які відбуваються з кожним спільним для всіх складових ЄСІКС об'єктом чи суб'єктом обліку з метою збереження їх життєвого циклу;**
- **уніфіковану модель інтеграції;**
- **розмежування доступу;**
- **логічну зв'язність між майстер-реєстрами.**

Сервіс не є сукупністю електронних реєстрів у контексті Закону України "Про публічні електронні реєстри". Інформація в ньому використовується для внутрішніх потреб ЄСІКС.

Наповнення та перегляд даних в майстер-реєстрах можуть виконуватися як за рахунок власних фронтендів (організаційна структура, фізичні особи), так і в якості бекенд-сервісу за посередництва інших підсистем чи сервісів з API-доступом або через визначені механізми внутрішньої взаємодії.

Бізнес-логіка формування та зміни записів визначається технічним завданням та не повинна суперечити чинним нормативно-правовим актам.

Система повинна забезпечувати можливість реалізації 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.

Система повинна забезпечувати можливість реалізації прав суб'єктів персональних даних (доступ, уточнення, обмеження обробки, видалення), визначення строків їх зберігання, а також аудит операцій з такими даними відповідно до вимог законодавства України.

Основні функціональні вимоги. Сервіс повинен:

1. **Забезпечувати створення, перегляд, оновлення облікових карток відповідно до визначеної бізнес-логіки.**
2. **Підтримувати єдиний унікальний ідентифікатор для кожної сутності.**
3. **Забезпечувати історичність змін (audit-traceable state history).**
4. **Підтримувати інтеграцію з:**
   - 4.1. **кадровою системою;**
   - 4.2. **компонентом "Електронна взаємодія";**
   - 4.3. **підсистемою "Суддівське досьє".**
5. **Інші підсистеми ЄСІКС мають інтегруватися з сервісом майстер-реєстрів з можливістю визначення переліку атрибутів, що будуть доступні кожній підсистемі.**
6. **Забезпечувати розмежування доступу до перегляду повних переліків записів.**
7. **Забезпечувати пошук запису за ідентифікаторами або атрибутами.**
8. **Підтримувати зв'язки між майстер-реєстрами на основі єдиного ідентифікатора.**
9. **Забезпечувати механізм GoldRecord для визначених сутностей.**
10. **Підтримувати версійність організаційної структури.**

Основні майстер-реєстри (перелік може бути уточнений на етапі формування технічного завдання):

Назва реєстру	Призначення
Фізичні особи	**Є централізованим обліковим ядром ЄСІКС та охоплює абсолютно всіх фізичних осіб, які будь-яким чином згадуються або задіяні в процесах судової влади — незалежно від того, чи є вони користувачами системи.** **До реєстру включаються:** ● **процесуальні особи (позивачі, відповідачі, заявники тощо);** ● **судді;** ● **працівники органів судової влади;** ● **кандидати на посади;** ● **представники сторін;** ● **особи, що згадуються в документах;** ● **інші фізичні особи, пов'язані з процесами правосуддя.** **Майстер-реєстр функціонує за принципом єдиного ідентифікатора фізичної особи, який використовується для встановлення зв'язків з усіма іншими майстер-реєстрами та підсистемами.**

Назва реєстру	Призначення
	Джерела формування: ● **Самореєстрація фізичної особи при першому вході (в майбутньому — з валідацією/отриманням даних з державних реєстрів).** ● **Первинне завантаження з кадрової системи (проте надалі кадрова система стає споживачем даних).** ● **Формування облікової картки фіз.особи на підставі потреби посилатися на цю картку про фіз.особу в документах, які створюються у системі.** **Передбачено:** ● **обмежений фронтенд (пошук та перегляд конкретної картки);** ● **неможливість повного перегляду переліку фізичних осіб;** ● **накопичення даних протягом життєвого циклу;** ● **визначення бізнес-логіки наповнення на етапі ТЗ;** ● **юридично достовірну модель змін відповідно до НПА.**
Фотокартки фізичних осіб	**Є спеціалізованим майстер-реєстром для зберігання фотозображень фізичних осіб, пов'язаних із записами в майстер-реєстрі фізичних осіб.** **Забезпечує:** ● **зберігання та версіонування фотокарток;** ● **зв'язок із єдиним ідентифікатором фізичної особи;** ● **використання у сервісах ідентифікації, візуалізації профілю, кадрового обліку;** ● **дотримання вимог щодо захисту персональних даних.** **Джерело:** ● **кадрова система;** ● **самореєстрація;** ● **інтеграційні процеси.**
Профілі адвокатів	**Містить спеціалізований інформаційний блок щодо фізичної особи як адвоката.** **Формується внаслідок бізнес-процесу самореєстрації через Електронний кабінет із валідацією даних у ЄРАУ.** **Особливості:** ● **не містить персональних даних (використовується посилання на майстер-реєстра фізичних осіб);** ● **інформація є статичною і не залежить від конкретної справи;** ● **забезпечує мінімально необхідний набір даних для взаємодії між підсистемами;** ● **адвокат може бути членом адвокатського об'єднання;** ● **запис створюється лише за умови підтвердження статусу адвоката.** **Сукупність записів формує повний перелік адвокатів, що взаємодіють з ЄСІКС.**
Профілі суддів	**Містить інформаційний блок щодо фізичної особи як судді незалежно від:** ● **поточного місця роботи;** ● **статусу (діючий, у відставці, на адміністративній посаді).** **Майстер-реєстр містить мінімально необхідний набір даних для функціонування інших сервісів.** **Повна деталізована інформація ведеться у підсистемі «Суддівське досьє».** **Забезпечує:** ● **перегляд повного переліку суддів (з урахуванням ролей доступу);** ● **зв'язок із майстер-реєстром фізичних осіб;** ● **використання в сервісах авторозподілу, аналітики, кадрового обліку та в всіх інших функціях Системи, де потрібен перелік ВСІХ фізосіб, які коли-небудь або прямо зараз були/є**

Назва реєстру	Призначення
	діючими суддями на певній посаді.
Профілі кандидатів на посаду судді	Формується внаслідок виконання процесів підсистеми Суддівського досьє. Містить: ● власну статусну модель (учасник конкурсу, переможець, рекомендований тощо); ● зв'язок із майстер-реєстром фізичних осіб. Відображає результат процесів без збереження їх детальної логіки (яка зберігається у профільній підсистемі — Суддівському досьє).
Профілі присяжних, арбітражних керуючих, державних та приватних виконавців, судових експертів, нотаріусів, прокурорів	Формуються за логікою, аналогічною до профілю адвоката, судді чи кандидата у судді. Підтвердження надання відповідної посади в профілі відбувається відповідно до законних процедур. Призначені для централізованого обліку спеціалізованих процесуальних статусів фізичних осіб, необхідних для функціонування окремих підсистем. Перелік таких профілів може уточнюватися на етапі формування ТЗ залежно від бізнес-потреб відповідних профільних підсистем.
Юридична особа/фізична особа-підприємець	Є уніфікованим майстер-реєстром, що об'єднує юридичних осіб та фізичних осіб-підприємців (ФОП) як процесуальних суб'єктів, які беруть участь у процесах судової влади. Майстер-реєстр містить: ● облікові дані з ЄДР; ● тип суб'єкта (ЮО / ФОП); ● базові ідентифікаційні та реєстраційні атрибути; ● зв'язки з представниками. Юридичні особи та ФОП не є безпосередніми користувачами ЄСІКС — дії від їх імені здійснюють уповноважені фізичні особи. Формування запису: ● самореєстрація через Електронний кабінет; ● валідація та/або отримання даних з ЄДР.
Уповноважені представники юридичної особи/фізичної особи-підприємця чи фізособи	Містить облікові картки представництва, що фіксують: ● хто саме (фізична особа); ● кого саме представляє (фізособа / ЮО / ФОП); ● правову підставу; ● строк дії повноважень. Особливості: ● представник завжди є конкретною фізичною особою; ● для адвокатів наявність зареєстрованого електронного кабінету є обов'язковою; ● не має власного повноцінного фронтенду, внесення та перегляд даних через електронний кабінет - профіль користувача; ● повний перелік записів недоступний для жодної ролі; ● передбачено механізм пошуку для перевірки повноважень.
Контактні дані	Операційний майстер-реєстр для уніфікованого зберігання контактної інформації щодо: ● фізичних осіб; ● організацій; ● підрозділів. Забезпечує: ● централізоване управління контактними відомостями; ● багаторазове використання в різних підсистемах; ● інтеграцію з кадровою системою та профілем користувача.
Банківські реквізити	Містить централізований блок даних щодо банківських реквізитів:

Назва реєстру	Призначення
	• фізичних осіб; • юридичних осіб/фізичних осіб-підприємців; • органів судової влади. Джерело: • кадрова система; • самореєстрація. Використовується у фінансових та процесуальних сервісах.
Органи судової влади,суддівського самоврядування, консультативно-дорадчі органи органів судової влади, органи державної влади, органи місцевого самоврядування	Є централізованим GoldRecord організаційної структури. Включає: • облікові картки організацій; • облікові картки підрозділів; • облікові картки посад. Організація: • може бути юридичною особою або утворенням без статусу юрособи; • має історичність даних; • створюється технічним адміністратором або уповноваженими особами; • може імпортуватися з кадрової системи; • розширюється даними з ЄДР. Підрозділ: • відображає результат штатної структури; • інтегрується з підсистемою кадрового обліку. Посада: • відповідає потребам двох напрямів обліку: 1 - штатний розпис з точки зору звичайного кадрового обліку; 2 - облік суддівських посад з точки зору процесів в ВККС; • містить статуси з кадрової системи та статуси, сформовані процесами ВККС; • містить історичність як інстанцій типових посад у конкретних органах. Відповідає на питання: «Яка посада існувала в якому органі і в який період?» Майстер-реєстр підтримує історичність, статусність та версіювання. Має складний ролевий інтерфейс. Крім органів та організацій, що є юридичними особами, реєстр забезпечує реєстрові операції з суб'єктами, які не мають такого статусу. Перелік таких організацій буде визначений в положенні про ЄСІКС.
Працівники та робітники органів судової влади	Містить облікові картки працівників (держслужбовців, інших працівників). Формується з кадрової системи. Забезпечує: • зв'язок фізособи з посадою; • використання в інших сервісах.
Судді на посаді	Є спеціалізованим майстер-реєстром активних суддів, які обіймають посади в органах судової влади. Відрізняється від майстер реєстру працівників: • розширеним набором атрибутів; • іншими рівнями доступу; • обов'язковим зв'язком з профілем судді; • специфічною логікою формування. Є GoldRecord для сервісів, що потребують актуального переліку суддів (наприклад, авторозподіл).

5.3 Єдиний персональний простір користувача

5.3.1 Загальний опис

Кабінет користувача Системи — це Єдиний персональний простір користувача, який забезпечує єдиний користувацький досвід (UX) та виступає контейнером для відображення функціональних інтерфейсів складових Системи. Кабінет не містить специфічної бізнес-логіки складових Системи, а відповідає за навігацію та візуальну цілісність.

Відповідно до концепції, Кабінет користувача Системи має через єдині стилі, графічні елементи, єдиний персональний простір користувача, а також уніфіковані процеси, шаблони, довідники та класифікатори, транслювати користувачам єдині підходи до організації роботи та формування внутрішньої культури.

5.3.2 Основні функціональні вимоги

1. **Кабінет користувача має динамічно завантажувати складові Системи. Зміна або оновлення інтерфейсу однієї складової Системи не повинна вимагати перезбірки всього Кабінету користувача.**
2. **Кабінет користувача має мати можливість відкривати сторінки в новій вкладці;**
3. **У Кабінеті користувача має бути реалізовано керування спільними елементами відповідно до UX/UI дизайну:**
    - **Глобальне навігаційне меню (Side/Top Bar) з можливістю приховання сайд бара для малих екранів;**
    - **Уніфікований Header (профіль користувача, вибір ролі, сповіщення);**
    - **Уніфікований Footer;**
    - **Уніфікований Favicon для кожної складової Системи та назву відкритої веб-сторінки (наприклад, для IAM-сервісу: Вхід - 🔑 IAM | ЄСІКС; Користувачі - 🔑 IAM | ЄСІКС; Ім'я Прізвище - 🔑 IAM | ЄСІКС тощо);**
    - **Спільний статус-рядок (Status Bar) для відображення критичних системних станів;**
    - **Елементи доступу до довідки (наприклад, кнопка «Довідка» або відповідний віджет), що забезпечують відкриття релевантних матеріалів сервісу Wiki залежно від контексту роботи користувача;**
    - **Уніфіковані інтерактивні підказки (tooltip) для елементів інтерфейсу відповідно до UX/UI дизайну;**
    - **Інші частини інтерфейсу, обумовлені затвердженим дизайном.**
4. **У Кабінеті користувача має бути реалізовано:**
    - **Можливість збереження індивідуальних налаштувань інтерфейсу для кожного користувача (порядок та видимість колонок у таблицях, стан згорнутих меню, обрані віджети на робочому столі та таке інше відповідно до кожного типового елемента інтерфейсу, для якого буде розроблена спільна інтерфейсна компонента);**
    - **Налаштування мають зберігатися централізовано та підтягуватися при вході з будь-якого пристрою по обліковці Користувача;**
    - **Кабінет користувача має забезпечувати уніфікований механізм підтвердження користувачем критичних дій шляхом відображення попереджувальних повідомлень або діалогових вікон з наданням зрозумілих підказок щодо їх усунення відповідно до UX/UI дизайну;**
    - **Кабінет користувача має забезпечувати відображення повідомлень користувачу, зокрема інформаційних повідомлень, повідомлень про помилки, попереджень та повідомлень про хід виконання операцій, із наданням рекомендацій щодо подальших дій.**
5. **Для підсистем ЄСІКС, які являють собою повноцінний програмний комплекс та поставляються з власним інтерфейсом (як от підсистема кадрового обліку або підсистема бухгалтерського обліку) розробка інтерфейсу в межах єдиного**

персонального простору не є обов'язковою, але має бути забезпечена переадресація користувача у власний інтерфейс профільної підсистеми після того, як користувач обрав відповідний елемент навігації в інтерфейсі кабінета користувача Системи.

6. **Усі компоненти інтерфейсу системи мають бути спроєктовані відповідно до останньої версії WCAG на момент реалізації.**

5.3.3 Вимоги до інтеграції та використання

Розробка та супровід дизайн-системи (UI Kit):

1. **До початку розробки бібліотеки UI-компонентів Виконавець зобов'язаний розробити та надати Власнику Системи клікабельний прототип базових інтерфейсів та UI-компонентів для погодження концепції взаємодії користувача та візуального представлення. Клікабельний прототип повинен:**
   - **1.1. відображати основні сценарії взаємодії користувача;**
   - **1.2. демонструвати поведінку ключових UI-компонентів;**
   - **1.3. відображати навігацію та структуру інтерфейсу;**
   - **1.4. бути погодженим Власником Системи до початку реалізації бібліотеки UI-компонентів.**
2. **Виконавець зобов'язаний розробити, опублікувати (як npm-пакет або аналог) бібліотеку UI-компонентів та надати документацію до неї.**
3. **Виконавець зобов'язаний сформувати та затвердити до моменту розробки клікабельний прототип з урахуванням вимог дизайн-системи.**
4. **Бібліотека має містити: сітки, типографіку, кнопки, форми, таблиці з підтримкою кастомізації (сортування, фільтри), модальні вікна та інші інтерфейсні елементи, передбачені затвердженим дизайном.**

5.3.4 Профіль користувача в єдиному персональному просторі

Система повинна надавати користувачу можливість перегляду власного профілю користувача в єдиному персональному просторі та забезпечувати наступні можливості в цьому профілі:

1. **Система повинна забезпечувати можливість самостійного керування обліковим записом користувача у дозволених межах (наприклад, зміна пароля, верифікованої пошти, керування факторами автентифікації).**
2. **Система повинна надавати можливість перегляду поточного та перемикання між доступними юридичними статусами користувача, які беруться з базового сервісу IAM.**
3. **Система повинна надавати користувачу можливість відстежувати активність власного облікового запису шляхом перегляду логів, що беруться з централізованої підсистеми логування входу у профілі за останній певний період.**
4. **Система повинна забезпечити можливість додавання спеціалізованих розділів у профіль користувача в кабінеті користувача, якими будуть керувати певні складові з метою показати в цьому розділі персональну інформацію, яка стосується виключно цього користувача, наприклад, розділ "Персональні відомості", наповненням якого буде керувати майстер-реєстр "Реєстр фізичних осіб зареєстрованих в ЄСІКС".**

6. НЕФУНКЦІОНАЛЬНІ ВИМОГИ

Архітектура Системи та нефункціональні вимоги мають виключати технологічну залежність від конкретного постачальника хмарних або інфраструктурних сервісів.

Усі компоненти Системи повинні мати можливість розгортання в середовищі власної інфраструктури або інфраструктури будь-якого постачальника без зміни прикладної логіки.

Не допускається використання пропрієтарних 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;**
- **унеможливлюють або істотно ускладнюють міграцію системи до альтернативного інфраструктурного середовища.**

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

Механізми масштабування, відновлення та управління життєвим циклом повинні реалізовуватися на рівні оркестрації або інфраструктури, а не шляхом пропрієтарних сервісів постачальника.

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

Експлуатація Системи має забезпечуватися персоналом Адміністратора Системи 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 проектами 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.

Система повинна відповідати сучасним міжнародним стандартам інформаційної безпеки, 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.

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

Інформація в повідомленнях зовнішнім сторонам про помилки в компонентах Системи не має відображати технічні подробиці складу та версій компонентів.

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. **Система повинна мати функціонал для обмеження кількості запитів до системи з метою її захисту від перевантаження.**
4. **Система 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 Системи. Після виконання дій з усунення або мінімізації впливу виявлених вразливостей у Системі мають бути відсутні вразливості рівня high та вище.

Передбачити створення стандартних шаблонів безпечної конфігурації та готових образів для розгортання операційних систем, обладнання, програмного забезпечення, додаткових сервісів, необхідних для штатного функціонування Системи.

Платформа інфраструктури має забезпечувати логічну ізоляцію складових Системи від інших сервісів, що функціонують в межах інфраструктури.

В Системі для забезпечення роботи адміністраторів та користувачів із Системою формуються і використовуються типові рольові моделі кінцевих адміністраторів/користувачів Системи 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).

Система має забезпечити автентифікацію користувачів 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.

Система 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 Системі. Відповідальність за недопущення внесення такої інформації покладається на користувачів, які повинні бути належним чином проінструктовані.

Система 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 Системи.

6.3 Вимоги до ергономіки та технічної естетики

Кінцеві користувачі отримують доступ до Системи через вебсайт, як частини інтерфейсу Системи. Вебсайт надаватиме загальнодоступну інформацію та міститиме перехід до кабінету зареєстрованих користувачів. Для кожної з користувацьких груп автоматично компонується на підставі наданих ролей окремий інтерфейс кабінету користувача, який пристосований до відповідного максимального набору функцій. Необхідно передбачити універсальність інтерфейсів для різних функціоналів та закласти подальше розширення переліку доступних для користувачів функцій.

Система повинна надавати користувачеві гнучкі механізми персоналізації її інтерфейсу. 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.

Прототипи дизайну вебсайту — це схематичне зображення форм і окремих елементів сторінки. Пропорції елементів дизайну, розміри шрифтів і заголовків, відстані між елементами, дизайн елементів та їх розміщення є умовними та можуть відрізнятися в кінцевій реалізації Системи.

Мати можливість запуску і роботи вебінтерфейсу, використовуючи браузер Microsoft Edge, Safari або Google Chrome найсучаснішої версії на момент проведення випробувань Системи. При цьому усі сторінки вебсайту повинні бути відображені у тій же зручній формі на настільному комп'ютері та на мобільному пристрої користувача (планшет, ноутбук, смартфон), незалежно від типу пристрою (без використання окремої мобільної версії), тобто інтерфейс повинен бути адаптивний (ця технологія може бути застосована до певного функціоналу на рівні кожної підсистеми, що визначається в технічному завданні).

Вебкомпоненти Системи повинні бути доступні без необхідності встановлення додаткового програмного забезпечення (плагіни, розширення, десктопне ПЗ), крім програмного забезпечення, необхідного для активації можливості підписання КЕП.

6.4 Вимоги до захисту інформації

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

- або шляхом створення Системи 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 Системі.

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

Інфраструктура, на якій функціонуватиме Система, 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

Система 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 Системи повинна будуватися на уніфікованих принципах проєктування та реалізації програмних компонентів і мати єдиний архітектурний підхід в межах проєкту та наслідувати загальноприйняті на проєкті патерни поведінки.

Система та всі програмні компоненти повинні відповідати чинним міжнародним угодам, національним нормативно-правовим актах та стандартам у сфері IT.

Система 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 Системи повинна забезпечуватися стабільною роботою її компонентів, збереженням цілісності та доступності даних, а також мінімальною потребою у втручанні системного адміністратора для відновлення працездатності. Впроваджена Система повинна забезпечувати постійну доступність всіх сервісів в режимі 24x7, окрім випадків, коли у Системі виконуються планові профілактичні роботи

або відбувається оновлення програмного забезпечення, про що користувачі Системи заздалегідь поінформовані.

Відмовостійкість Системи 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.

Система 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 Системи у разі відмови або виходу з ладу будь-якого одного з програмно-апаратних компонентів;**
- **збереження інформації на момент відмови або виходу з ладу будь-якого з компонентів Системи незалежно від призначення з наступним відновленням після проведення ремонтних і відновлювальних робіт;**
- **резервування критично важливих компонентів і даних Системи, конфігурації та налаштувань;**
- **архівація даних та налаштувань Системи 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. Збереження даних має забезпечуватися у випадках:

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

Збереження інформації, що обробляється в складових Системи, повинно бути гарантоване у повному обсязі, втрата даних не допускається. Система 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 компонентів Системи з «холодних» копій у цілісному та працездатному вигляді;**
- **RTO (Recovery time objective, максимальний час відновлення працездатності усіх компонентів Системи за умови наявності серверної інфраструктури): не більше 2 годин;**
- **забезпечення доступності Системи 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 компоненти Системи повинні мати надлишковість за схемою щонайменше N+1 з метою технічного обслуговування та оновлення ПЗ окремих компонентів без перешкоджання роботі всієї Системи (тобто для кожного ключового компонента має бути щонайменше один резервний вузол, у разі відмови основного вузла система автоматично перемикається на резервний).

Система має забезпечувати спостереження (реєстрація, аудит подій тощо) за усіма операціями (подіями) та повний моніторинг функціонування системи, в тому числі резервування та відновлення.

Система має забезпечувати георозподілення між дата-центрами.

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 пропускною 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 кожної підсистеми будуть визначені у технічному завданні.

6.8 Вимоги до режимів функціонування засобу інформатизації

З метою забезпечення умов розробки та експлуатації Система 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 Системи. Розгортання PROD-середовища та його подальше адміністрування будуть виконуватися силами Адміністратора Системи. 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

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

Система 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.**

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

6.10. Вимоги до лінгвістичного забезпечення

Система 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 підсистем та вимог законодавства. Управління мовами та перекладами повинне здійснюватися через інтерфейс адміністратора.

6.11 Вимоги до потужності системи

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

Система 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 Системи 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, мережеві ресурси) під навантаженням.

Система має бути здатною обробити інформацію згідно очікуваного навантаження:

Користувачі

№	Показник	Опис / розріз	2023	2024	2025
1	Загальна кількість користувачів	Усі зареєстровані	ЕК 133 220 ВКЗ 33 877	ЕК 157 054 ВКЗ 38 413	ЕК 170 469 ВКЗ 59 303
2	Внутрішні користувачі (судді, помічники тощо)	К-сть	–	АСДС 23 000	АСДС 24 000
3	Зовнішні неавторизовані користувачі вебпортал (сеансів)	К-сть	6-12 місяці 22036749	37 164 155	41 030 966

4	Користувачі ЄДРСР З повним доступом	К-сть	10340	12 600	14 100

Основні сутності

№	Сутність	Одиниця	2023	2024	2025
1	Справи	К-сть створених	3 385 341	3 469 217	3 671 016
2	Провадження	К-сть створених	4 356 825	4 461 328	4 827 291
3	Судові рішення	К-сть створених	7 817 209	8 083 168	8 812 741
4	Виконавчі документи	К-сть створених	788 831	957 340	1 001 393
5	Нотифікації через ЕК	К-ть створених	800 000 000	950 000 000	1 100 000 000

Документи

№	Показник	Одиниця	2023	2024	2025
1	Документів	шт.	62 157 453	72 106 168	77 835 858
2	Файлів	шт.	39 825 839	91 685 911	180 910 079

Дані

Назва параметру	До 1 Кб	Від 1 Кб до 1 Мб	Від 1 Мб до 10 Мб	Від 10 Мб до 100 Мб	Від 100 Мб
Середній розмір прикріпленого файлу (В)	2 373,682664	851 766,8753	12 786 417,97	106 999 087,2	1 673 141 004
Відсоток від загальної кількості	0,01%	78,55%	17,76%	3,28%	0,40%

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

- **90% запитів повинні виконуватися протягом 1 сек.**
- **95% запитів повинні виконуватися протягом 2 сек.**
- **99% Користувачів повинні успішно ввійти в Систему з першої спроби.**
- **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 (Систему), створене в рамках надання послуг з розробки (включаючи вихідний код, документацію, бази даних, графічні елементи тощо), у повному обсязі переходять до Власника Системи з моменту підписання Акту приймання-передачі наданих послуг;**
- **Виконавець має гарантувати, що передана Система не порушує права інтелектуальної власності третіх осіб;**
- **У складі Системи 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 Системи використовувати Систему у власних цілях без виплати додаткових роялті та без обов'язкового розкриття власного коду Системи (якщо це не суперечить типу ліцензії);**
- **Виконавець зобов'язаний надати повний перелік усіх сторонніх бібліотек та компонентів, що використані в Системі, із зазначенням типу їх ліцензій;**
- **У разі необхідності використання у складі Системи комерційного ПЗ третіх осіб, Виконавець повинен:**
    - **Попередньо погодити із Власником Системи 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 Системи необхідні періодичні ліцензійні платежі (subscription), Виконавець зобов'язаний надати розрахунок вартості володіння (TCO) на період не менше 3 (трьох) років.**
- **Виконавець має передати Власнику Системи 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 Системи постачаються у вигляді ліцензійних сертифікатів та (за необхідності) ліцензійних ключів (файлів), що інсталюються разом із відповідним програмним забезпеченням у складі Системи;**
- **Ліцензії на програмне забезпечення, що використовується у складі Системи, повинні бути безстроковими та необмеженими у часі;**
- **Програмне забезпечення Системи, 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 Системи, повинні дозволяти після впровадження створювати декілька серверних інсталяцій (кількість обмежується за згодою сторін) для можливостей тестування, розробки та навчання. Програмне забезпечення СКБД, яке використовуватиметься у складі Системи, повинне передбачати безкоштовну версію СКБД, яку можна використовувати для тестування та навчання;**
- **Тип ліцензії повинен забезпечувати одночасну роботу всієї кількості користувачів Системи, яка дорівнює кількості придбаних ліцензій, на будь-якій кількості комп'ютерів або віртуальних машин;**
- **Ліцензійне програмне забезпечення, необхідне для впровадження та експлуатації Системи, поставляється у термін, достатній для початку надання послуг з впровадження Системи, її налаштування та введення в дію.**

6.13 [QA] 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 Системи на етапі формування технічного завдання. За вимогою Адміністратора Виконавець має проводити консультації щодо архітектури та розробки (орієнтовно до 2 годин на тиждень).

Власник Системи (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 Системи.

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.

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

6.14 [QA] Вимоги до міграції даних

Виконавець зобов'язаний забезпечити повне та коректне перенесення даних з усіх необхідних діючих систем (далі — Джерела даних): Електронний суд, ДЗ, ДСС, Кадри-веб, ЄДРСР, ВКЗ, що надаються Адміністратором Системи, до новостворюваної Системи. 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 Системи 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;**
- **Виконавець повинен провести міграцію та надати звіти про результати міграції, що підтверджують цілісність, повноту та коректність перенесених даних у новій Системі.**

Перед початком міграції історичних даних Адміністратор Системи має забезпечити Виконавцю доступ до баз даних, які використовуються у підсистемах ЄСІКС, 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), зокрема, але не виключно:

- **Інформація про фізичних осіб, задіяних в процесах ЄСІКС;**
- **Інформація про фізичних осіб як користувачів ЄСІКС;**
- **Інформація про юридичних осіб/фізичних осіб-підприємців, які є учасниками судових справ;**
- **Інформація про представників (адвокатів) фізичних осіб та/або юридичних осіб/фізичних осіб-підприємців;**
- **Інформація про інших осіб;**

- **Інформація про органи, що входять в систему судової влади України та інших органів;**
- **Довідники.**

7 ТЕХНОЛОГІЧНИЙ СТЕК

Технологічний стек Системи сформовано відповідно до концепції ЄСІКС з урахуванням принципів уніфікації, масштабованості та довгострокової експлуатаційної спроможності. При виборі технологій враховано їх поширеність на ринку, рівень зрілості, активність професійних спільнот, наявність документації та практик промислового використання, а також можливості Адміністратора Системи щодо подальшої підтримки, розвитку та супроводу системи 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. Аргументація повинна враховувати відповідність концепції ЄСІКС, вплив на безпеку, масштабованість, вартість володіння, складність супроводу, кадрову доступність, а також ризики подальшої експлуатації та розвитку системи Адміністратором Системи .

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

Система 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 системи 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.

7.1 Мови програмування, Фреймворки та бібліотеки

Стек програмування:

1. **Стек програмування для front-end частини — Vue.js, починаючи з v.3;**
2. **Стек програмування для back-end з аргументуванням вибору виконавця:**
   - **2.1. Python для роботи з даними, процесами, пов’язаними з аналітикою;**
   - **2.2. Java для роботи основних процесів, пов'язаних з ЄСІКС.**

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

7.2 Бази даних

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

Типи баз даних:

1. **Реляційні SQL - PostgreSQL;**
2. **Нереляційні NoSQL - MongoDB;**
3. **REST-сумісне об’єктне сховище даних з відкритим кодом.**

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

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

7.3 Інструменти інтеграції та API

Складові Системи повинні взаємодіяти між собою через стандартизовані API та/або подієві механізми.

Базовим механізмом синхронної взаємодії складових Системи є використання RESTful веб-сервісів 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.

Для інтеграції з наявними складовими Системи має бути забезпечена можливість роботи з протоколом SOAP (з використанням XML) та іншими форматами даних. Можливість трансформації даних між різними форматами має бути закладена.

Між складовими Системи має бути забезпечена можливість автоматизованої електронної інформаційної взаємодії та обміну даними як внутрішньо (в рамках Системи), так і зовнішньо.

7.4 Базова інфраструктура

7.4.1 Управління ключами шифрування та системними паролями

7.4.1.1 Загальний опис

Управління ключами та паролями — це централізоване захищене сховище для секретів Системи (паролів, сертифікатів, API-ключів). Модуль має забезпечувати повний життєвий цикл секретів: від генерації та зберігання до ротації та відкликання, мінімізуючи ризик витоку конфіденційних даних інфраструктури та підтримувати механізми масштабування та георозподілення.

7.4.1.2 Основні функціональні вимоги

1. **Модуль має забезпечувати зберігання даних з шифруванням відповідним до операції обробки даних (передачі, зберігання тощо).**
2. **Модуль має забезпечувати можливість автоматичної ротації паролів та ключів за розкладом або за подією.**
3. **Модуль має забезпечувати можливість випуску та автоматичного оновлення внутрішніх SSL/TLS-сертифікатів для забезпечення захищеного з'єднання між підсистемами (mTLS).**
4. **Модуль має надавати API для шифрування/дешифрування даних без передачі самого ключа шифрування складовим Системи.**
5. **Модуль має забезпечувати реалізацію алгоритмів розділення ключа доступу до самого сховища між кількома адміністраторами (наприклад, схема Шаміра), щоб ніхто одноосібно не мав повного контролю над Системою.**
6. **Доступ до сховища секретів має бути суворо обмежений на основі принципу мінімальних привілеїв.**

7.4.1.3 Вимоги до інтеграції та використання

1. **Модуль має підтримувати нативну автентифікацію для сервісів, розгорнутих у K8s. Інші складові Системи не повинні знати пароль від сховища секретів — вони мають використовувати свій Service Account для отримання доступу.**
2. **Виконавець має забезпечити механізм передачі секретів у функціональні складові Системи через змінні середовища або тимчасові файли безпосередньо в контейнери, щоб розробники інших складових Системи не писали складний код інтеграції.**
3. **Модуль має забезпечувати можливість гнучкого налаштування прав: наприклад, «Сервіс А» може тільки читати пароль від своєї бази даних, але не бачить секретів «Сервіс Б».**
4. **Фіксація кожної спроби доступу до будь-якого секрету (хто, коли і до якого саме ключа звертався).**

7.4.2 Кешування даних та оперативне зберігання сесій користувачів

7.4.2.1 Загальний опис

Кешування даних та оперативне зберігання сесій користувачів — це критичний компонент інфраструктури складових Системи, що має бути реалізований як розподілене сховище даних у пам’яті (In-memory data store). Модуль виконує роль високопродуктивного посередника між складовими Системи та основними базами даних. Модуль має підтримувати роботу в режимі кластера та георозподілення для забезпечення відмовостійкості та збереження кешованих даних при виході з ладу окремих вузлів.

Модуль має вирішувати три стратегічні завдання:

1. **Винесення стану сесій користувачів за межі складових Системи для їх горизонтального масштабування.**
2. **Збереження чернеток та контексту роботи користувача в умовах нестабільного енергопостачання та зв’язку з обмеженим часом життя, що буде визначено на етапі технічного завдання.**
3. **Прискорення роботи складових Системи шляхом кешування частих запитів та зниження навантаження на реляційні бази даних.**

7.4.2.2 Основні функціональні вимоги

1. **Забезпечувати механізм фонового автозбереження проміжних результатів роботи користувача.**
2. **Зберігати контекст роботи користувача, дозволяючи відновити процес з того самого місця після раптового розриву з'єднання або переавторизації.**
3. **Кешування нормативно-довідкової інформації (НДІ): оперативне зберігання результатів "важких" запитів до БД які працюють з даними, що часто зчитуються, але рідко змінюються.**
4. **Забезпечувати роботу механізмів запобігання одночасному редагуванню одного об'єкта (наприклад, судової справи або документа) декількома користувачами одночасно (якщо цей об'єкт не дозволено редагувати колективно).**
5. **Управління життєвим циклом тимчасових даних (TTL): модуль має автоматично видаляти застарілі сесії, чернетки та застарілі кеші на основі налаштованих термінів зберігання (Time-to-Live).**
6. **Спільний доступ до сесій (Shared Sessions): усі інстанси одного сервісу повинні мати однаковий доступ до даних сесії та кешу.**

7.4.2.3 Вимоги до інтеграції та використання s3

1. **Stateless-інтеграція: складові Системи не мають зберігати жодних даних про стан користувача та його сесії у власній оперативній пам'яті. Весь стан має передаватися до цього модуля через стандартизований API.**

2. **Стратегії кешування: модуль повинен підтримувати різні стратегії інвалідації кешу (наприклад, за часом або за подією зміни даних в основній БД), щоб гарантувати актуальність інформації для користувача.**
3. **Модуль має бути сумісним із протоколом In-memory рішень для забезпечення мінімальної затримки (latency) при доступі до даних.**
4. **Модуль має бути інтегрований із сервісом автентифікації для автоматичного анулювання тимчасових даних та сесійних ключів при завершенні сесії.**

7.4.3 Компонент «Управління репозиторієм файлового контенту та медіа-матеріалів (S3)»

7.4.3.1 Загальний опис

Управління репозиторієм файлового контенту та медіаматеріалів (S3) — компонент є засобом управління централізованим об'єктним сховищем, призначеним для надійного, масштабованого та захищеного зберігання об'єктного контенту (PDF-документи, аудіо/відео засідань, фотодокази та інше). На відміну від традиційних файлових систем, компонент використовує об'єктну модель доступу (S3 API), що дозволяє зберігати петабайти даних та забезпечувати високу швидкість доступу.

7.4.3.2 Основні функціональні вимоги

1. **S3-сумісність: Компонент має забезпечувати підтримку протоколу Amazon S3 API як галузевого стандарту для забезпечення Vendor-agnostic підходу (можливість використовувати MinIO, Ceph або хмарні рішення).**
2. **Компонент має забезпечувати автоматичне або налаштоване збереження попередніх версій об'єкта при його оновленні. Видалення об'єкта не має призводити до фізичного знищення даних без спеціальної команди адміністратора або спеціальних налаштувань.**
3. **Компонент має надавати можливість присвоювати кожному файлу користувацькі теги (наприклад, case_id, document_type, security_level), що дозволяє шукати та класифікувати файли без звернення до основної БД.**
4. **Компонент має надавати можливість налаштованого переміщення старих файлів у «холодне» сховище (архів) або їх видалення після завершення терміну зберігання відповідно до правил, встановлених у сервісі "Електронний архів" або налаштованих окремо, якщо це не електронний документ або документальна справа.**
5. **Компонент має забезпечувати підтримку завантаження великих файлів (відео засідань по 5–10 ГБ) частинами з можливістю відновлення завантаження після розриву зв'язку.**

7.4.3.3 Інструменти розробника та стандарти інтеграції

Виконавець має забезпечити, щоб інші команди розробників могли інтегруватися зі сховищем за мінімальний час, а саме:

1. **Надати бібліотеку/сервіс для генерації тимчасових посилань, що дозволяє фронтенду завантажувати файл напряму в S3, оминаючи бекенд-сервіси, що критично знижує навантаження на систему при масовому завантаженні документів.**
2. **Надати готові конфігурації та обгортки (Wrappers, SDK) для стандартних S3-клієнтів (Java, .NET, Python), які вже налаштовані на роботу з внутрішньою мережею Системи.**
3. **Надати інструментарій та його опис, завдяки яким реалізується механізм сповіщень та/або інтегруватися з наявними складовими Системи.**
4. **Розробити та задокументувати єдину політику формування шляхів (наприклад, court-id/year/case-number/file-uuid), щоб розробники різних підсистем не створювали хаос у сховищі.**

5. **Компонент має забезпечувати абстракційний шар доступу до об'єктного сховища, що дозволяє змінювати постачальника або тип S3-сумісного сховища без внесення змін до бізнес-логіки або прикладного коду складових Системи.**

7.4.3.4 Вимоги до безпеки та стійкості

1. **Модуль має забезпечувати обов'язковий криптографічний захист даних при передачі (із застосуванням TLS) та при зберіганні (із застосуванням стійких алгоритмів шифрування, не нижче AES-256).**
2. **Вимкнення або послаблення криптографічного захисту допускається виключно для інформації, що не належить до інформації з обмеженим доступом, та за наявності окремо задокументованого рішення власника засобу інформатизації, прийнятого в межах моделі загроз та СЗІ.**
3. **Модуль має підтримувати синхронну або асинхронну реплікацію даних між двома або більше територіально рознесеними дата-центрами.**
4. **Інтеграція з ICAP: будь-який файл, що потрапляє в S3, має автоматично проходити через чергу перевірки на віруси перед тим, як стати доступним для інших користувачів.**

7.4.4 Компонент "Логування" (Logging)

7.4.4.1 Загальний опис

Компонент "Логування" — централізоване сховище, призначене для агрегації логів з усіх шарів складових Системи (інфраструктура, БД, підсистеми, базові сервіси, прикладне ПЗ) про технічні події. Компонент є первинним джерелом даних для пошуку помилок та технічної діагностики.

7.4.4.2 Основні функціональні вимоги

1. **Компонент має забезпечити централізований збір даних у режимі реального часу з розподілених інфраструктурних вузлів та програмних компонентів через легкі агенти.**
2. **Компонент має зберігати всі події в узгодженому для всієї Системи форматі із використанням стандартних полів (Trace ID, Service Name, Severity Level тощо).**
3. **Компонент має забезпечувати передачу контексту запиту між складовими Системи для відтворення повного шляху транзакції та трасування.**
4. **Компонент має забезпечувати налаштування та оптимізацію під швидкий запис та пошук із терміном зберігання 30–90 днів (залежно від критичності сервісу).**
5. **Компонент повинен забезпечувати:**
   - 5.1. **збір логів сервісів, системних логів, логів безпеки та технічних логів інтеграції;**
   - 5.2. **логування помилок із фіксацією:**
     - 5.2.1. **унікального ідентифікатора транзакції;**
     - 5.2.2. **типу помилки;**
     - 5.2.3. **stack trace;**
     - 5.2.4. **рівня критичності.**
   - 5.3. **логування змін конфігурації системи;**
   - 5.4. **логування подій розгортання нових сервісів;**
   - 5.5. **синхронізацію часових позначок через NTP;**
   - 5.6. **можливість передачі логів до зовнішніх SIEM;**
   - 5.7. **сумісність з open-source системами збору та аналізу логів;**
   - 5.8. **конфігуровані політики зберігання логів;**
   - 5.9. **фіксацію змін налаштувань логування;**
   - 5.10. **централізоване агрегування логів усіх підсистем.**
6. **Вимоги до захисту:**
   - 6.1. **Компонент повинен забезпечувати:**
     - 6.1.1. **обмеження доступу до логів відповідно до ролей;**
     - 6.1.2. **захист логів від несанкціонованого редагування;**
     - 6.1.3. **маскування чутливих даних;**

6.1.4. контроль цілісності логів.

7.4.4.3 Вимоги до інтеграції

1. Компонент має забезпечувати використання відкритих стандартів для збору та передачі даних.
2. Компонент має забезпечувати автоматичне знеособлення персональних даних (наприклад, номерів телефонів чи РНОКПП) з логів до їх збереження.

7.4.5 Компонент “Моніторинг” (Monitoring)

7.4.5.1 Загальний опис

Компонент “Моніторинг” — аналітична надбудова, яка перетворює «сирі» дані (метрики та логи) у візуальні звіти та оперативні сповіщення. Компонент відповідає за контроль здоров’я системи (Health Checks), моніторинг та прогнозування навантаження.

7.4.5.2 Основні функціональні вимоги

1. Візуалізація: Компонент має забезпечити відображення в реальному часі ключових показників (CPU, RAM, Error Rate, Request Latency, кількість одночасних сесій, метрики складових Системи).
2. Компонент має забезпечити наявність незалежної від базового сервісу системи сповіщень (через SMS/Telegram/Email або інші канали) на основі порогових значень та аномалій (наприклад, раптове зростання 500-х помилок). Виконавець має забезпечити можливість відправки повідомлень у разі:
   2.1. Перевищення попередньо встановлених порогових значень;
   2.2. Перевищення заданого часу відгуку компонентів Системи;
   2.3. Наближення до граничного значення параметрів роботи компонентів Системи;
   2.4. Досягнення граничної пропускної здатності каналу;
   2.5. Виявлення критичних помилок, що блокують роботу;
   2.6. Непрацездатності компоненту ЄСІКС.
3. Компонент має здійснювати регулярну перевірку доступності публічних точок доступу (endpoints) та внутрішніх сервісів.
4. Компонент має забезпечувати можливість порівняння поточного навантаження з історичними даними (наприклад, навантаження під час масового подання звітів).
5. Компонент повинен дозволяти додавати та керувати бізнес-метриками та нотифікаціями, необхідними для виявлення потенційних проблем.

7.4.5.3 Вимоги до інтеграції та використання

1. Компонент має забезпечувати інтеграцію з компонентом «Логування» (для аналізу частоти помилок) та безпосередньо з платформою контейнеризації — для збору метрик.
2. Виконавець має забезпечити можливість для розробників інших складових Системи реалізувати та підключити стандартний endpoint /health для опитування системою моніторингу. Виконавець має розробити та надати специфікацію JSON-відповіді для endpoint-а /health, яку мають реалізувати всі інші розробники, щоб система моніторингу могла автоматично розуміти стан сервісу («Up», «Down» та інші).
3. Метрики “з коробки”: Виконавець має забезпечити готові шаблони (Library/Interceptors) для автоматичного збору базових метрик, як от:
   3.1. Час відповіді (Latency);
   3.2. Кількість помилок (Error rate);
   3.3. Кількість запитів (Throughput);
   3.4. Інші, що будуть визначені на етапі формування ТЗ.
4. Компонент має забезпечити можливість для розробників інших складових Системи самостійно створювати власні дашборди в системі моніторингу без залучення адміністратора системи.

7.4.6 Компонент “Черга повідомлень”

7.4.6.1 Загальний опис

Черга повідомлень — це інфраструктурний сервіс, призначений для забезпечення асинхронної комунікації між підсистемами ЄСІКС та зовнішніми інформаційними системами. Компонент 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.

7.4.6.2 Основні функціональні вимоги

Компонент повинен забезпечувати:

1. **Підтримку основних патернів обміну:**
   - **1.1. Публікація/Підписка — для розсилки подій декільком сервісам;**
   - **1.2. 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. **Механізми повторних спроб: автоматичне повторне відправлення повідомлення у разі тимчасової недоступності сервісу-отримувача за налаштованим алгоритмом.**
4. **Обробку помилок: переміщення повідомлень, які не вдалося обробити після визначеної кількості спроб, до спеціальної черги “недоставлених повідомлень” для подальшого аналізу та ручної обробки.**
5. **Горизонтальне масштабування: можливість динамічного збільшення кількості обробників для забезпечення високої пропускної здатності в пікові періоди навантаження.**
6. **Пріоритезацію повідомлень: можливість обробки критично важливих системних подій поза чергою або з вищим пріоритетом.**

7.4.6.3 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.**

7.4.6.4 Вимоги до інтеграції та безпеки

1. **Стандартизація протоколів: підтримка відкритих протоколів взаємодії (наприклад, AMQP 0.9.1, MQTT або Kafka Protocol).**
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 компонента “Моніторинг”.**
4. **Безпека та аудит:**
   - **4.1. Автентифікація підсистем при підключенні до брокера;**
   - **4.2. Шифрування трафіку між відправником, брокером та отримувачем;**
   - **4.3. Обмеження прав доступу — сервіс повинен мати доступ лише до визначених для нього черг та топіків;**
   - **4.4. Логування: фіксація фактів публікації та доставки повідомлень у компоненті “Логування” для можливості трасування бізнес-процесів.**

7.4.7 Компонент “Сервіс аудиту” (Audit)

7.4.7.1 Загальний опис

Сервіс аудиту — централізований компонент Системи, призначений для фіксації, збереження та відображення юридично значущих подій та дій користувачів і адміністраторів, а також змін даних та станів бізнес-об’єктів.

Компонент забезпечує формування доказової бази щодо дій у Системі для цілей внутрішнього контролю, інформаційної безпеки, службових перевірок, розслідувань інцидентів та забезпечення регуляторної відповідності.

7.4.7.2 Основні функціональні вимоги

Компонент повинен забезпечувати:

1. **Аудит дій користувачів і адміністраторів. Сервіс повинен забезпечити фіксацію:**
   - **1.1. входу до Системи (логін);**
   - **1.2. виходу із Системи (логаут);**
   - **1.3. неуспішних спроб входу;**
   - **1.4. створення, блокування користувачів;**
   - **1.5. змін ролей та прав доступу;**
   - **1.6. змін налаштувань безпеки;**
   - **1.7. виконання дій, що потребують підтвердження за допомогою КЕП;**
   - **1.8. операцій експорту та імпорту даних;**
   - **1.9. пошукових запитів (у випадках, визначених політикою безпеки).**
2. **Аудит операцій над бізнес-об’єктами. Сервіс повинен забезпечити фіксацію:**
   - **2.1. створення, перегляду, зміни та видалення об’єктів (документів, сутностей, записів);**
   - **2.2. змін статусів та станів документів;**
   - **2.3. версіонування змін із збереженням попередніх значень;**
   - **2.4. операцій архівування, відновлення, видалення або спроб доступу до архіву;**
   - **2.5. операцій автоматичного або ручного розподілу документів;**
   - **2.6. операцій інформаційної взаємодії, що мають юридичне або безпекове значення.**
3. **Представлення інформації запису, що містить:**
   - **3.1. дату та час події (синхронізовані через NTP);**
   - **3.2. унікальний ідентифікатор події;**
   - **3.3. ідентифікатор користувача;**
   - **3.4. роль користувача на момент виконання дії;**
   - **3.5. IP-адресу та/або ідентифікатор сесії;**
   - **3.6. тип дії;**
   - **3.7. об’єкт дії (тип та ідентифікатор);**
   - **3.8. результат виконання (успішно/неуспішно);**
   - **3.9. додаткові атрибути контексту (за потреби).**
4. **Незмінність та зберігання записів:**
   - **4.1. неможливість редагування або видалення записів аудиту користувачами та адміністраторами;**
   - **4.2. контроль цілісності записів (із застосуванням механізмів хешування або аналогічних методів);**
   - **4.3. довгострокове або безстрокове зберігання записів відповідно до політики зберігання даних;**
   - **4.4. розмежування доступу до перегляду аудиту відповідно до ролей.**

7.4.7.3 Вимоги до надання та використання даних аудиту

Компонент повинен забезпечувати можливість використання даних іншими сервісами та підсистемами ЄСІКС, а саме:

1. **забезпечувати отримання історії дій користувача;**
2. **забезпечувати отримання історії змін конкретного об’єкта;**

3. **забезпечувати фільтрацію записів за:**
   - 3.1. **періодом;**
   - 3.2. **типом дії;**
   - 3.3. **користувачем;**
   - 3.4. **об'єктом;**
   - 3.5. **результатом виконання.**
4. **підтримувати пагінацію та сортування результатів;**
5. **забезпечувати відображення аудиту в обліковій картці користувача або в консолі адміністратора;**
6. **забезпечувати експорт записів аудиту у форматі CSV;**
7. **забезпечувати експорт у форматі JSON/CEF для інтеграційних потреб;**
8. **забезпечувати контроль доступу до API на основі ролей;**
9. **унеможливлювати зміну або видалення записів через API.**

7.4.7.4 Вимоги до інтеграції

Компонент повинен забезпечувати:

1. **інтеграцію з компонентом управління доступом (IAM) для отримання ідентифікаційних атрибутів користувача;**
2. **інтеграцію з прикладними підсистемами через стандартизований механізм передачі подій аудиту;**
3. **використання уніфікованого формату даних (JSON) для внутрішньої взаємодії;**
4. **можливість передачі подій безпеки до зовнішніх SIEM-систем у стандартизованих форматах (наприклад, CEF або еквівалент);**
5. **ізоляцію сховища аудиту від прямого доступу прикладних адміністраторів;**
6. **синхронізацію часових позначок через NTP для забезпечення коректної кореляції подій;**
7. **можливість масштабування відповідно до обсягу подій.**

8 ВИМОГИ ДО СУПРОВОДУ ТА ОБСЛУГОВУВАННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ

Рівень деталізації вимог — користувацький сценарій до групи функціональності Системи 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 Системи.

Інфраструктура NON-PROD для розробки буде виділена Адміністратором Системи:

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 Системи.

8.1 Вимоги до гарантійної підтримки

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

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

1. **Усунути всі виявлені недоліки складових Системи, які не відповідають вимогам технічного завдання та функціональних вимог в терміни, визначені в SLA, що є додатком до договору;**
2. **Оновлювати документацію, коли виникає потреба через зміни, викликані відмінностями у порівнянні зі станом на момент поставки складових Системи;**
3. **Виконувати оновлення та/або відновлення складових Системи, 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 Системи 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 модулю 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 Системи.

Конкретна спеціалізована форма, в якій мають бути представлені ті чи інші навчальні матеріали про певний аспект роботи Системи 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 Системи. Окрім зазначеного, навчальні матеріали можуть бути також у вигляді сформованого курса лекцій в спеціалізованій навчальній підсистемі, що буде розгорнута Адміністратором Системи, у вигляді відео-курсів, у вигляді автоматизованих тестів з можливістю налаштувати перелік питань та спосіб надання відповідей тощо.

8.3 Вимоги до документації

Система повинна мати таку документацію:

1. **Інструкція користувача Системи (за наявними ролями). Інструкція користувача повинна містити покрокові описи дій користувачів по всіх операціях з візуальним відображенням (скріншоти інтерфейсу).**
2. **Інструкція адміністратора Системи:**
   - **2.1. Інструкція для системи 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 документу 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 Системи, 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 Системи;**
   - **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 Системи із зазначенням компонентів, їх взаємодії, середовищ розгортання, зовнішніх інтеграцій, потоків даних та залежностей між сервісами.**
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. [QA] Вимоги до проведення випробувань

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

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 із Адміністратором Системи, з подальшим повторним тестуванням.

9.1.1 Функціональне тестування

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

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

Результати функціонального тестування оформлюються протоколом випробувань, який підписується представниками Адміністратора Системи 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 в частині фактично реалізованих взаємодій між складовими Системи, а також із зовнішніми державними інформаційно-комунікаційними системами і реєстрами.

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 Системи від несанкціонованого доступу, зловживань правами доступу, витоків інформації та інших загроз інформаційній безпеці.

Безпекові випробування повинні охоплювати перевірку механізмів автентифікації та авторизації користувачів, управління сесіями, розмежування прав доступу, захисту персональних та службових даних, а також стійкості складових Системи до типових мережевих 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 Системи до повторного тестування. Складові Системи не можуть бути прийняті Адміністратором Системи 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 Системи стабільно функціонувати при визначених цими технічними вимогами прогнозованих параметрах інтенсивності роботи, визначення її пропускної здатності, часу відгуку та стійкості до пікових навантажень.

Випробування повинні охоплювати перевірку роботи Системи 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 Системи нефункціональним вимогам та рекомендації щодо оптимізації або масштабування.

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

9.2 Вимоги до передачі результатів виконаних робіт

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

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

Орієнтовні терміни виконання робіт від 5 до 8 місяців з моменту підписання договору.

Крім того, Виконавець у складі пропозиції повинен надати опис підходу до подальшого доопрацювання та розвитку функціоналу Системи 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 Системи 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 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 Системи 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 Системи 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 Системи здійснюється на безоплатній основі. Вартість майнових прав інтелектуальної власності (у тому числі виключних) на Програмне забезпечення включена у вартість Договору на створення Підсистеми.

9.3 Вимоги до патентної чистоти

9.3.1. Вимоги до програмного забезпечення, яке розробляється Виконавцем

На момент передання Системи Виконавець зобов’язаний врегулювати всі правовідносини з авторами та третіми особами, залученими ним до створення Системи, та забезпечити набуття від них майнових прав інтелектуальної власності на Систему 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 Системи.