

# ТЕХНІЧНІ ВИМОГИ

**МОДЕРНІЗАЦІЯ ДЕРЖАВНОЇ  
ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ  
СИСТЕМИ ТА ВЕБ-ПОРТАЛУ  
ДЕРЖЛІКСЛУЖБИ В ЧАСТИНІ  
СТВОРЕННЯ «ЕЛЕКТРОННОЇ СИСТЕМИ  
ОН-ЛАЙН ПОДАЧІ ТА  
ВІДСЛІДКОВУВАННЯ ЗАЯВ НА  
ОТРИМАННЯ ДОЗВІЛЬНИХ  
ДОКУМЕНТІВ, ЩО НАДАЮТЬСЯ  
ДЕРЖЛІКСЛУЖБОЮ ТА ЇЇ  
ТЕРИТОРІАЛЬНИМИ ОРГАНАМИ»**

## Зміст

Розділ 1. ЗАГАЛЬНІ ВІДОМОСТІ.....	3
1.1. Повне найменування системи та її умовне позначення.....	3
1.2. Відомості про джерела та порядок фінансування .....	3
1.3. Перелік нормативно-правових актів, на підставі яких створюється система.....	3
1.4. Визначення, позначення та скорочення.....	4
1.4.1. Поняття та терміни .....	4
1.4.2. Скорочення.....	4
Розділ 2. ПРИЗНАЧЕННЯ ТА МЕТА СТВОРЕННЯ СИСТЕМИ .....	5
2.1. Призначення системи .....	5
2.2. Мета створення системи .....	6
Розділ 3. ХАРАКТЕРИСТИКА ОБ'ЄКТІВ АВТОМАТИЗАЦІЇ .....	7
Розділ 4. ЗАГАЛЬНИЙ ОПИС ІСНУЮЧОЇ СТРУКТУРИ СИСТЕМИ .....	7
Розділ 5. ВИМОГИ ДО СИСТЕМИ .....	7
5.1. Вимоги до Системи в цілому.....	8
5.1.1. Вимоги до структури та функціонування системи.....	8
5.1.2. Вимоги до технологічної платформи ЕСОВПЛЗ-ДСЛЗ.....	10
5.1.3. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами системи.....	11
5.1.4. Вимоги до режимів функціонування системи .....	12
5.1.5. Вимоги до журналювання в системі .....	12
5.1.6. Перспективи розвитку та модернізація системи.....	12
5.1.7. Вимоги до ергономіки та технічної естетики .....	12
5.1.8. Вимоги до захисту інформації від несанкціонованого доступу.....	13
5.1.9. Вимоги до забезпечення збереження інформації у випадку аварійних ситуацій.....	17
5.2. Вимоги до функцій (задач), що виконуються ЕСОВПЛЗ-ДСЛЗ .....	17
Розділ 6. ВИМОГИ ДО РОЗРОБКИ ТА ПЕРЕДАЧІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ .....	17
6.1. Вимоги до розробника програмного забезпечення .....	17
6.2. Вимоги до передачі програмного забезпечення .....	17
5.3. Отримувач програмного забезпечення .....	18

## **Розділ 1. ЗАГАЛЬНІ ВІДОМОСТІ**

### **1.1. Повне найменування системи та її умовне позначення**

**Повне найменування системи:** модернізація державної інформаційно-аналітичної системи та веб-порталу Держлікслужби в частині створення модулю "Електронна система он-лайн подачі та відслідковування заяв на отримання дозвільних документів, що надаються Держлікслужбою та її територіальними органами".

**Коротке найменування системи (умовне позначення):** ЕСОПВЛЗ-ДСЛЗ.

### **1.2. Відомості про джерела та порядок фінансування**

Розробка системи фінансується Міжнародною благодійною організацією «Фонд Східна Європа» в рамках виконання проекту міжнародної технічної допомоги «Прозорість та підзвітність у державному управлінні та послугах (TAPAS)».

### **1.3. Перелік нормативно-правових актів, на підставі яких створюється система**

Закон України від 04.04.1996 № 123/96-ВР «Про лікарські засоби»;

Закон України від 06.09.2012 року № 5203-17 «Про адміністративні послуги»;

Закон України від 02.03.2015 № 222-VIII «Про ліцензування видів господарської діяльності»;

Закон України від 05.04.2007 № 877-V «Про основні засади державного нагляду (контролю) у сфері господарської діяльності»;

Закон України від 19.11.1992 № 2801-XII «Основи законодавства України про охорону здоров'я»;

Постанова Кабінету Міністрів України від 30.11.2016 № 929 Про затвердження Ліцензійних умов провадження господарської діяльності з виробництва лікарських засобів, оптової та роздрібною торгівлі лікарськими засобами, імпорту лікарських засобів (крім активних фармацевтичних інгредієнтів);

Постанова Кабінету Міністрів України від 10.09.2008 № 843 «Про затвердження критерію, за яким оцінюється ступінь ризику від провадження діяльності у сфері охорони здоров'я для безпеки життя і здоров'я населення та визначається періодичність здійснення планових заходів державного нагляду (контролю)»

Постанова Кабінету Міністрів України від 14.09.2005 № 902 "Про затвердження Порядку здійснення державного контролю якості лікарських засобів, що ввозяться в Україну";

Порядок контролю за додержанням Ліцензійних умов провадження господарської діяльності з виробництва лікарських засобів, оптової, роздрібною торгівлі лікарськими засобами, які затверджені наказом МОЗ України від 31.10.2011 № 724 та зареєстровані в Міністерстві юстиції України 07.12.2011 за № 1421/20159;

Наказ МОЗ України від 15.05.2006 N 275 «Про затвердження Інструкції із санітарно-протиепідемічного режиму аптечних закладів»;

Наказ МОЗ України від 06.07.2012 № 498 «Про затвердження Переліку товарів, які мають право придбавати та продавати аптечні заклади та їх структурні підрозділи»;

Наказ МОЗ України від 11.07.2012 № 513 Про затвердження Порядку перевірки перед видачею ліцензії на провадження господарської діяльності з виробництва лікарських засобів, оптової, роздрібною торгівлі лікарськими Засобами;

Наказ МОЗ України від 17.10.2012 № 812 «Про затвердження Правил виробництва (виготовлення) та контролю якості лікарських засобів в аптеках»;

Наказ Міністерства Охорони Здоров'я від 29.10.2014 № 698 "Про затвердження Порядку здійснення контролю за відповідністю імунобіологічних препаратів, що застосовуються в медичній практиці, вимогам державних і міжнародних стандартів";

Наказ МОЗ України від 19.07.2005 № 360 «Про затвердження Правил виписування рецептів та вимог-замовлень на лікарські засоби і виробу медичного призначення, Порядку відпуску лікарських засобів і виробів медичного призначення з аптек та їх структурних підрозділів, Інструкції про порядок зберігання, обліку та знищення рецептурних бланків та вимог-замовлень»;

Наказ МОЗ України від 18.05.2015 № 242 "Про затвердження Правил утилізації та знищення лікарських засобів";

Наказ МОЗ України 29.09.2014 № 677 «Про затвердження Порядку контролю якості лікарських засобів під час оптової та роздрібною торгівлі»;

Наказ МОЗ України від 16.02.2009 №95 Настанова Лікарські засоби. Належна практика дистрибуції. СТ-Н МОЗУ 42-5.0:20014";

Наказ МОЗ України від 16.02.2009 №95 Настанова 42-5.1:2011 «Лікарські засоби. Належна практика зберігання»;

Наказ Міністерства охорони здоров'я України від 27.12.2012 № 1130 «Про затвердження Порядку проведення підтвердження відповідності умов виробництва лікарських засобів вимогам належної виробничої практики»;

Наказ Міністерства охорони здоров'я України від 07.12.2012 № 1008 «Про затвердження Порядку сертифікації якості лікарських засобів для міжнародної торгівлі та підтвердження для активних фармацевтичних інгредієнтів, що експортуються».

ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення.

ГОСТ 34.201-89. Інформаційна технологія. Комплекс стандартів на автоматизовані системи. Види, комплектність та позначення документів при створенні автоматизованих систем.

## **1.4. Визначення, позначення та скорочення**

### **1.4.1. Поняття та терміни**

Поняття та терміни вживаються у значеннях, визначених нормативними документами переліченими у розділі 1.3 цих Технічних вимог.

### **1.4.2. Скорочення**

АРМ	Автоматизоване робоче місце
АС	Автоматизована система

БД	База даних
Держлікслужба	Державна служба України з лікарських засобів та контролю за наркотиками
ДДХ	Документ дозвільного характеру
ЕЦП	Електронний цифровий підпис
ІТС	Інформаційно-телекомунікаційна система
ЛЗ	Лікарський засіб
ЛУ	Ліцензійні умови провадження господарської діяльності
МВ	Вироби медичного призначення та медична техніка
НСД	Несанкціонований доступ
ПЗ	Програмне забезпечення
СГД	Суб'єкт господарської діяльності - зареєстрована в установленому законодавством порядку юридична особа незалежно від її організаційно-правової форми та форми власності, яка провадить господарську діяльність, крім органів державної влади та органів місцевого самоврядування, а також фізична особа - суб'єкт підприємницької діяльності
СУБД	Система керування базою даних
ТЗ	Технічне завдання

## Розділ 2. ПРИЗНАЧЕННЯ ТА МЕТА СТВОРЕННЯ СИСТЕМИ

### 2.1. Призначення системи

Модернізація державної інформаційно-аналітичної системи та веб-порталу Держлікслужби в частині створення модулю "Електронна система он-лайн подачі та відслідковування ліцензійних заяв та ліцензійної документації Держлікслужби України" призначена для оптимізації процесу взаємодії ліцензіатів з Держлікслужбою протягом усього процесу розгляду ліцензійних заяв та заяв на видачу висновку про якість ввезеного (Постанова Кабінету Міністрів України від 14.09.2005 №902) шляхом автоматизації процесу подачі, розгляду, зберігання та пошуку ліцензійної та іншої дозвільної документації. Також система повинна забезпечувати каталогізацію даних про ліцензіатів та наданої ліцензійної документації в електронній формі з використанням сучасних інформаційно-комунікаційних технологій.

ЕСОПВЛЗ-ДСЛЗ має надавати можливість:

- отримання заявником вичерпної інформації щодо процесу ліцензування, або процесу отримання висновку про якість ввезеного (перелік та склад необхідних документів, термінів їх розгляду тощо);
- формування заявником заяви через інтерактивну форму веб-інтерфейсу на офіційному веб-порталі Держлікслужби для суб'єктів господарювання;
- відправлення заявником заяви та супровідної документації, засвідчених електронним цифровим підписом та електронною печаткою суб'єкта господарської діяльності - юридичної особи або фізичної особи-підприємця до

Держлікслужби або її територіальних органів (відповідно до чинного Законодавства у даній галузі);

- отримання заявником інформації щодо поточного стану опрацювання заяви та супровідної документації від моменту подання заяви до моменту прийняття рішення Держлікслужбою або її територіальним органом;
- централізованої реєстрації заяв та супровідної документації з валідацією цифрового підпису заявника ЕСОПВЛЗ-ДСЛЗ;
- зберігання історії та статистики щодо прийнятих та оброблених пакетів документів;
- своєчасне отримання інформації щодо прийнятих рішень по направленим електронним заявам або необхідності надання додаткових підтверджуючих документів для прийняття рішення.

## **2.2. Мета створення системи**

Основною метою створення ЕСОПВЛЗ-ДСЛЗ є реалізація процесів надання пілотних адміністративних послуг Держлікслужбою та її територіальними органами (документів дозвільного характеру) в електронній формі суб'єктам господарської діяльності (заявникам), а саме:

- подання заявником документів для отримання пілотних послуг в електронній формі з використанням електронного цифрового підпису (далі - ЕЦП) та направленою шифрування;
- перевірка, реєстрація та опрацювання відповідальними працівниками Держлікслужби та/або територіальних органів, поданих заявником документів в електронній формі;
- видача результату надання пілотних адміністративних послуг у спосіб визначений заявником (особисто, повідомлення в електронній формі);
- надання заявникам електронних інформаційних сервісів, що супроводжують процес надання пілотних адміністративних послуг: повідомлення про успішну перевірку пакету документів та про реєстрацію електронного документу щодо розгляду заяви (позитивне рішення або відмову у реєстрації чи неприйняття до розгляду), повідомлення про результат адміністративної послуги;
- зберігання дозвільних документів у електронній формі в особистих електронних кабінетах заявників.

Створення та впровадження ЕСОПВЛЗ-ДСЛЗ забезпечить підвищення ефективності, доступності та прозорості надання адміністративних послуг Держлікслужбою та її територіальними органами через запровадження додаткового каналу отримання цих послуг в електронній формі.

Впровадження ЕСОПВЛЗ-ДСЛЗ сприятиме зменшенню корупційних загроз у процесі надання адміністративних послуг, підвищенню довіри до органів влади з боку громадян та суб'єктів господарської діяльності та якості й ефективності роботи Держлікслужби та її територіальних органів.

### **Розділ 3. ХАРАКТЕРИСТИКА ОБ'ЄКТІВ АВТОМАТИЗАЦІЇ**

Об'єктом автоматизації є центральний орган виконавчої влади – Держлікслужба, її територіальні структурні підрозділи, що задіяні в процесі видачі ліцензій та дозвільних документів на провадження діяльності з лікарськими засобами.

У рамках створення ЕСОПВЛЗ-ДСЛЗ проводиться автоматизація процесів надання пілотного переліку адміністративних послуг (документів дозвільного характеру) в електронній формі.

Користувачами ЕСОПВЛЗ-ДСЛЗ є:

- суб'єкти господарської діяльності;
- державні службовці – співробітники Держлікслужби та її територіальних органів, співробітники територіальних та уповноважених лабораторій.

Предметом автоматизації є адміністративні процеси, пов'язані з видачою документів дозвільного характеру для суб'єктів господарської діяльності у сфері оптової та роздрібною торгівлі, виробництва лікарських засобів в умовах аптеки/промислового виробництва/імпорту лікарських засобів, а також з видачою дозвільних документів на імпорті лікарські засоби, що ввозяться на територію України.

### **Розділ 4. ЗАГАЛЬНИЙ ОПИС ІСНУЮЧОЇ СТРУКТУРИ СИСТЕМИ**

Існуюча Державна інформаційно-аналітична система контролю якості лікарських засобів і медичної продукції складається з таких підсистем (модулів):

- Ліцензування торгівлі ЛЗ
  - Модуль «Ліцензування торгівлі ЛЗ»;
  - Модуль «Перевірки СГД щодо дотримання ЛУ з торгівлі ЛЗ»;
- Ліцензування та сертифікація виробництва ЛЗ
  - Модуль «Ліцензування виробництва ЛЗ»;
  - Модуль «Перевірки СГД щодо дотримання ЛУ з виробництва ЛЗ»;
  - Модуль «Сертифікація виробництва ЛЗ»;
  - Модуль «Сертифікація ЛЗ для міжнародної торгівлі»;
- Ліцензування імпорту ЛЗ
  - Модуль «Ліцензування імпорту ЛЗ»;
- Державний контроль якості ЛЗ
  - Модуль «Державний контроль якості ЛЗ»;
  - Модуль «Перевірки СГД щодо якості ЛЗ»;
  - Модуль «Державний контроль ЛЗ, які ввозяться в Україну»;
  - Модуль «Централізовані реєстри»;
  - Модуль «Контроль знищення ЛЗ»;
  - Модуль «Облік справ про адміністративні правопорушення».
- Державний контроль безпеки МВ
  - Модуль «Контроль безпеки МВ».

### **Розділ 5. ВИМОГИ ДО СИСТЕМИ**

## 5.1. Вимоги до Системи в цілому

### 5.1.1. Вимоги до структури та функціонування системи

В рамках створення ЕСОПВЛЗ-ДСЛЗ повинні бути розроблені наступні ключових підсистем (рис. 1):

- підсистеми подачі заявок;
- підсистеми обробки заявок;
- підсистеми зберігання дозвільних документів;
- модуль взаємодії з функціонуючими модулями Державної інформаційно-аналітичної системи Держлікслужби;
- підсистеми адміністрування та захисту інформації;
- підсистеми оцінки якості сервісу надання електронних послуг.

Підсистема подачі заявок забезпечує:

- інтеграцію ЕСОПВЛЗ-ДСЛЗ з Веб-порталом Держлікслужби для суб'єктів господарювання;
- доступ до інформації про адміністративні послуги (документи дозвільного характеру);
- надання для заповнення електронних форм, необхідних для отримання адміністративних послуг (документів дозвільного характеру);
- можливість зберігання наперед заповнених шаблонів-форм електронних заяв користувачів;
- можливість роздрукування заповнених електронних форм та подальшого додавання сканованих (фотографованих) підписаних власноручним підписом заяв;
- можливість подання суб'єктами звернення заявок за допомогою засобів телекомунікаційного зв'язку, зокрема з використанням механізмів електронного цифрового підпису та направленою шифрування заявок відкритим ключом ЕСОПВЛЗ-ДСЛЗ.

Підсистема обробки заявок забезпечує:

- забезпечення передачі заявок користувачів на надійне зберігання до підсистеми зберігання дозвільних документів;
- забезпечення передачі заявок користувачів та отримання рішень щодо них через модуль взаємодії з функціонуючими модулями Державної інформаційно-аналітичної системи Держлікслужби «Лабораторний комплекс контролю якості ЛЗ та МП» ;
- перевірка, реєстрація та опрацювання відповідальними працівниками Держлікслужби або її територіальних органів поданих заявником документів в електронній формі;



- можливість надання заявникам повідомлень, підписаних електронними цифровими підписами відповідальних осіб Держлікслужби або її територіальних органів, про стан та результат обробки заявки за допомогою засобів телекомунікаційного зв'язку.

Підсистема зберігання дозвільних документів забезпечує:

- зберігання електронних копій Заявок та комплектів сканованих документів заявників на отримання/зміни/скасування ліцензії;
- зберігання електронних копій Ліцензій на провадження господарської діяльності з оптово/роздрібною торгівлі/виробництва лікарських засобів в умовах аптеки, промислового виробництва, імпорту лікарських засобів;
- зберігання електронних копій Заяв та комплектів сканованих документів заявників на отримання висновку про якість ввезених лікарських засобів;
- зберігання електронних копій висновків про якість ввезених лікарських засобів (Постанова Кабінету Міністрів України від 14.09.2005 №902);
- зберігання шаблонів наперед заповнених електронних заявок;
- надання доступу до електронних копій дозвільних документів.

Модуль взаємодії з функціонуючими модулями Державної інформаційно-аналітичної системи Держлікслужби «Лабораторний комплекс контролю якості ЛЗ та МП»:

- передача електронних копій Заявок та комплектів сканованих документів заявників на отримання/зміни/скасування ліцензії;
- отримання результатів розгляду Заявок з інформаційно-аналітичної системи Держлікслужби «Лабораторний комплекс контролю якості ЛЗ та МП» (модулі «Ліцензування виробництва», «Ліцензування торгівлі», «Ліцензування імпорту»);
- передача електронних копій Заявок та комплектів сканованих документів заявників на отримання висновку про якість ввезених ЛЗ;
- отримання результатів розгляду Заявок (з деталізацією по кожному лікарському засобу у заявці окремо) з інформаційно-аналітичної системи Держлікслужби «Лабораторний комплекс контролю якості ЛЗ та МП» (модуль «Державний контроль якості ЛЗ при ввезенні»);
- Внесення змін у відповідні модулі інформаційно-аналітичної системи Держлікслужби «Лабораторний комплекс контролю якості ЛЗ та МП» з метою приведення даних та бізнес-процесів, що автоматизуються Системою, до відповідних оновлень/ редакцій нормативно-правових документів галузі, які регламентують дані процеси.

Підсистема адміністрування та захисту інформації забезпечує:

- цілісність, доступність та автентичність розміщеної в ЕСОПВЛЗ-ДСЛЗ відкритої публічної інформації;

- конфіденційність, цілісність, доступність та автентичність заявок користувачів;
- конфіденційність, цілісність та доступність технологічної інформації ЕСОПВЛЗ-ДСЛЗ;
- реалізацію правил розмежування доступу;
- управління користувачами системи (введення, модифікація, вилучення відомостей);
- дотримання політики інформаційної безпеки;
- спостержність за роботою всіх компонентів ЕСОПВЛЗ-ДСЛЗ;
- керування налаштуваннями роботи системи в цілому.

Підсистема оцінки якості сервісу надання електронних послуг забезпечує:

- створення та зміна форм оцінки якості та доступності послуг;
- збір та аналіз інформації про якість та доступність послуг;
- зберігання інформації про оцінки якості та доступності послуг.

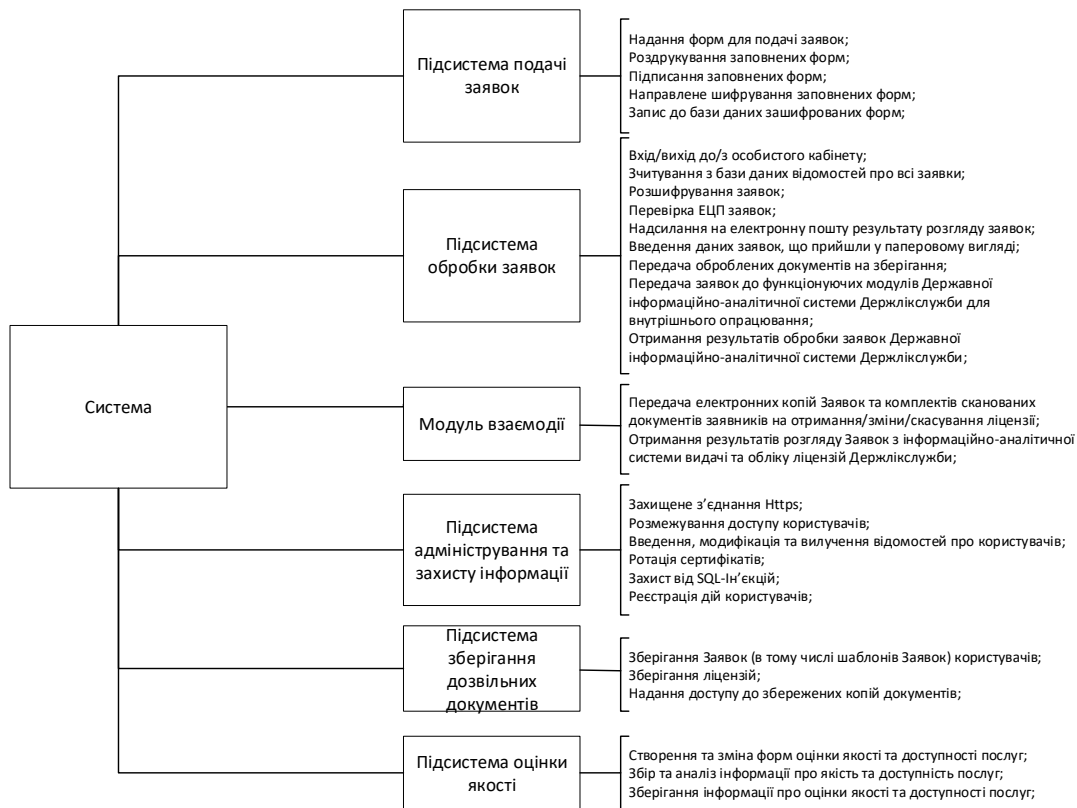


Рис. 1 – Створювані підсистеми ЕСОПВЛЗ-ДСЛЗ

### 5.1.2. Вимоги до технологічної платформи ЕСОПВЛЗ-ДСЛЗ

ЕСОПВЛЗ-ДСЛЗ повинна будуватись на програмній платформі, яка базується на веб-сервісах і використовує всі переваги сервісно-орієнтованої архітектури. Архітектура

додатку буде спроектована на основі підходу DDD (Domain-driven design), що використовується для розробки складних систем із тривалим життєвим циклом. При реалізації архітектури клієнтської частини повинні використовуватись архітектурні шаблони MVC, WEB-API та The Clean Architecture.

Розробка і тестування нової функціональності повинна проводитись із використанням методології TDD (Test-driven development). Використовувана платформа повинна містити інтегрований програмний інструмент з наявністю IDE для розробників, проектувальників і дизайнерів, який забезпечує повний цикл робіт зі створення додатків на основі платформи, а також містить інструментарій для створення складних екранних форм.

Використовувана платформа повинна містити готові шаблони проектування (моделі) організаційної структури організації, адміністрування, забезпечення безпеки, управління контентом, нотифікації, версійності, підтримки історичності і т.д. Клієнтський додаток платформи повинен бути кросплатформним, тобто може працювати на різних клієнтських операційних системах, таких як Windows, Linux, Unix, Mac OS, а також різних мобільних додатках для Android/iOS. Програмна платформа, на якій повинна бути побудовано ЕСОПВЛЗ-ДСЛЗ, повинна забезпечувати високий рівень інтеграції розроблених додатків з іншими системами за допомогою REST API, а також повинна підтримувати технологію єдиного входу (SSO). Програмна платформа повинна забезпечувати високий рівень швидкодії розроблених на ній веб-додатків за рахунок балансування навантаження, кластеризації та близького до лінійного масштабування.

Загальне рішення, яке будуватиметься на описаній вище програмній платформі (сервер застосувань), повинно забезпечувати роботу під керуванням операційної системи Linux. Інтерфейсні форми та функціонал для користувачів ЕСОПВЛЗ-ДСЛЗ повинні бути реалізовані за допомогою сучасних JS фреймворків та REST API. Бекенд бізнес логіки повинен реалізовуватись з використанням платформи .Net Core та мови програмування C#, реляційної СУБД PostgreSQL (або іншої реляційної СКБД з відкритим серцевим кодом).

ЕСОПВЛЗ-ДСЛЗ повинен бути розроблено з урахуванням забезпечення одночасної роботи щонайменше 1000 користувачів.

Веб-інтерфейс ЕСОПВЛЗ-ДСЛЗ повинен будуватись з врахуванням вимог до захисту інформації та забезпечуватиме шифрування трафіку між клієнтською та серверною частинами. Дані, що будуть вноситися шляхом Веб-інтерфейсу (на клієнті), матимуть можливість щодо засвідчення за допомогою ЕЦП (у відповідності до стандартів ДСТУ 4145-2002 та інтерфейсів SSP1).

### **5.1.3. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами системи**

Передача інформації між компонентами системи має виконуватись стандартними протоколами на рівні програмного забезпечення або на рівні платформи (системи керування базами даних, веб-серверів, тощо).

#### **5.1.4. Вимоги до режимів функціонування системи**

ЕСОПВЛЗ-ДСЛЗ повинна забезпечувати функціонування в режимі 24/7 (24 години на добу 7 днів на тиждень) без необхідності зупинки роботи ЕСОПВЛЗ-ДСЛЗ для проведення планового регламентного технічного обслуговування. ЕСОПВЛЗ-ДСЛЗ повинна бути адаптована для розгортання на декількох серверах для забезпечення надлишковості та мати функціонал балансування навантаження при розгортанні на декількох серверах.

#### **5.1.5. Вимоги до журналювання в системі**

Діагностування системи повинна забезпечуватись протоколюванням роботи компонентів ЕСОПВЛЗ-ДСЛЗ, як на рівні платформи (системи керування базами даних, веб-серверу, операційних систем, тощо), так і на рівні комп'ютерної програми (log-файли пошукових запитів, log-файли помилок).

#### **5.1.6. Перспективи розвитку та модернізація системи**

При розробці ЕСОПВЛЗ-ДСЛЗ передбачена можливість її подальшої модернізації та масштабування при мінімальних затратах часу по наступним напрямкам:

- додавання нових джерел інформації для пошуку відомостей (нових видів документів);
- додавання електронної ідентифікації запитувачів;
- прискорення роботи системи шляхом нарощування обчислювальних потужностей у разі збільшення навантаження.

ЕСОПВЛЗ-ДСЛЗ повинна бути розроблена таким чином, щоб забезпечити можливість оперативного внесення змін до класифікаторів та довідників, що використовуються в ній та зміни перевірок обов'язковості полів внесення даних.

#### **5.1.7. Вимоги до ергономіки та технічної естетики**

Інтерфейс системи повинен бути зручним та інтуїтивно зрозумілим користувачам. Форми внесення інформації повинні мати підказки щодо обов'язковості заповнення полів та щодо формату їх заповнення. Інтерфейс системи повинен бути орієнтований на використання клавіатури та маніпулятора «миша» (з можливістю використання тільки клавіатури, для пришвидшення введення інформації) з мінімізацією кількості дій для виконання простих операцій.

Взаємодія користувача з системою повинна виконуватись українською мовою, за винятком системних повідомлень, що не підлягають перекладу.

Форми внесення інформації повинні забезпечувати зменшення вірогідності помилок користувача при роботі з системою.

Інтерфейс повинен мати адаптацію для використання людьми з вадами зору відповідно до міжнародних рекомендацій.

При введенні інформації повинна здійснюватися перевірка коректності даних з використанням масок вводу (кількість знаків, відсутність невірних символів, надлишкові пробіли, тощо) та логічних умов.

Стилі, шрифти та кольори інтерфейсу веб-порталу повинні використовувати сучасні каскадні таблиці стилів (CSS), що використовуються на даний час при створенні сучасних веб-порталів.

Всі Веб-сторінки, елементи інтерфейсу повинні коректно відкриватись в будь-яких веб-браузерах, що на поточний момент використовуються користувачами (Edge, Google Chrome, FireFox, Opera, Safari, Internet Explorer тощо).

Кольорове оформлення інтерфейсу повинне бути виконане в єдиному строгому стилі.

Елементи інтерфейсу (кнопки, посилання) повинні мати назви, що дозволяють користувачеві однозначно інтерпретувати виконувани ними дії.

Використання кнопок як елементів керування повинне супроводжуватися повним набором візуальних ефектів, характерних для даного типу інтерфейсу (натискання/відпускання кнопки тощо).

Сигналізація про помилки або помилкові дії повинна супроводжуватися підказкою про подальші дії.

Інтерфейс системи має бути адаптований до використання на мобільних пристроях.

### **5.1.8. Вимоги до захисту інформації від несанкціонованого доступу**

Для забезпечення захисту інформації в системі відповідно вимогам законодавства України, вимагається побудова комплексної системи захисту інформації.

Питання створення комплексної системи захисту інформації на ЕСОПВЛЗ-ДСЛЗ цими технічними вимогами не передбачається.

В той же час, до ЕСОПВЛЗ-ДСЛЗ висуваються наступні вимоги із забезпечення безпеки інформації, які будуть враховані при подальшій побудові комплексної системи захисту інформації, а саме:

1. Забезпечення цілісності загальнодоступної інформації веб-сайту вимагає застосування технологій, що забезпечують реалізацію контрольованого і санкціонованого доступу до інформації та заборону неконтрольованої й несанкціонованої її модифікації, що повинно вирішуватися на рівні операційної системи сервера, системи управління баз даних та розроблюваного програмного забезпечення.

2. Задля забезпечення автентичності веб-сайт повинен працювати за протоколом https.

3. Компоненти ЕСОПВЛЗ-ДСЛЗ повинні бути здатним здійснювати первинну ідентифікацію будь-яких користувачів (незарєєстрованих та зарєєстрованих) за IP-адресою.

4. Повинна здійснюватися фільтрація на мережевому рівні, фільтрація пакетів службових повідомлень, фільтрація з урахуванням вхідного та вихідного інтерфейсу. За допомогою апаратних та/або програмних (pf, ipfw, iptables) міжмережєвих екранів забезпечити фільтрацію вхідних інформаційних потоків за принципом «заборонено все, що не дозволено», а також обмежити доступність зі сторони мережі Інтернет всіх портів, окрім тих, які необхідні для функціонування серверу застосувань.

5. Повинні бути встановлені мінімальні привілеї для користувачів мережі Інтернет при доступі до файлів та папок (директорій) серверу застосувань, обмеживши їх правом «тільки читання»; уникнути можливості перегляду лістингу директорій та файлів серверу застосувань зі сторони мережі Інтернет (наприклад, за допомогою конфігурування серверу застосувань, у тому числі файлів .htaccess).

6. Привілеї для користувачів ЕСОПВЛЗ-ДСЛЗ при доступі до файлів та папок (директорій) серверу застосувань повинні виставлятися за критерієм мінімально необхідних.

7. Повноваження користувачів повинні вестися на всіх необхідних для коректної роботи ЕСОПВЛЗ-ДСЛЗ рівнях, зокрема: операційної системи, системи управління базами даних, фреймворку тощо.

8. У ЕСОПВЛЗ-ДСЛЗ для управління правами доступу повинен бути реалізований механізм профілів і ролей.

9. Неприпустимо виникнення ситуації, при якій існує можливість отримати доступ до компоненту або функції ЕСОПВЛЗ-ДСЛЗ або Державної інформаційно-аналітичної системи Держлікслужби, оминувши авторизацію. У разі, якщо користувачем не пред'явлено персональні ідентифікатори, або вони не відповідають жодному з облікових записів, користувач повинен розглядатися як анонімний і доступ до кабінетної системи ЕСОПВЛЗ-ДСЛЗ або інших модулів Державної інформаційно-аналітичної системи Держлікслужби повинен бути заборонений.

10. Користувачам повинна бути реалізована форма реєстрації/входу виключно із використанням модулю автентифікації користувачів за ЕЦП або пари логін/пароль.

11. Форма реєстрації/входу в Особистий кабінет ЕСОПВЛЗ-ДСЛЗ повинна унеможливити автоматичне запам'ятання пароля до секретного ключа користувача веб-браузером.

12. Не допускається зберігання паролів в тексті процедур або функцій.

13. Процес реєстрації користувача веб-сайту повинен ініціювати виключно адміністратор безпеки.

14. Авторизація забезпечується модулем автентифікації та потребує накладання електронного цифрового підпису користувачем на генеровану сервером послідовність символів та його перевірки на стороні сервера.

15. Веб-сайт повинен забезпечувати здійснення ротації сертифікатів користувачів.

Ротація сертифікатів користувачів має здійснюватися виключно в ручному режимі адміністратором системи.

16. Контроль цілісності основних файлів ЕСОПВЛЗ-ДСЛЗ повинен здійснюватися на рівні операційної системи та системи управління базами даних.

17. Електронні кабінети веб-сайту повинні передбачати автоматичний вихід користувача з системи, якщо користувач не виконував жодних дій протягом 15 хвилин.

18. З метою безпеки всі файли, що відносяться до системи, повинні зберігатися в спеціальній структурі каталогів на рівні операційної системи і бути захищені.

19. Повинні бути заблоковані несанкціоновані завантаження файлових об'єктів на сервер застосувань. Користувачам дозволено завантажувати тільки документи, необхідні

для надання адміністративних послуг. Файли повинні завантажуватись до спеціально призначеної для цього директорії, запуск сценаріїв та скриптів з якої повинен бути заборонений.

20. Веб-сервер повинен відповідати на підключення тільки на TCP-порти 443 та 34789 (протоколи HTTPS та SSH відповідно).

21. Основні сценарії роботи веб-сайту не повинні мати доступу на запис до власних файлів.

22. Всі дані та параметри, одержувані серверною частиною системи через її веб-інтерфейси, повинні перевірятися на відповідність типам, розмірам, допустимим діапазнам значень.

23. Перевірка параметрів на відповідність повинна здійснюватися як на клієнтській стороні (наприклад, за допомогою вбудованих в веб-сторінки сценаріїв), так і на серверній стороні. При цьому перевірка на серверній стороні є основною і повинна забезпечувати гарантоване запобігання несанкціонованого доступу або збоїв системи в результаті відправки значень параметрів, невідповідних за типом, складом або розміром. Перевірка на клієнтській стороні є допоміжною і повинна забезпечувати захист від випадкових помилок добросовісного користувача, виключаючи відправку помилкових даних на серверну сторону.

24. Система повинна контролювати одержувану інформацію на предмет відсутності шкідливого для неї або інших користувачів системи програмного коду і керуючих послідовностей. Зокрема, повинна запобігати можливості впровадження в тіло повідомлень, призначених для публічного перегляду, якого-небудь шкідливого коду. Механізм, що забезпечує недопущення шкідливих компонентів, повинен діяти не за принципом виключення даних, відповідних деяким зразками або значенням, а за принципом виключення всіх даних, які не відповідають дозволеним значенням або зразкам. При цьому слід проводити перетворення службових символів в безпечний код, що забезпечує їхнє відображення на стороні клієнта.

25. Система повинна контролювати валідність ЕЦП використовуваних користувачами, а також співставляти відповідність ЕЦП користувачів, за якими вони авторизуються, ЕЦП, які накладаються на відповідні електронні заявки та вкладені додаткові електронні матеріали цих користувачів, у разі не відповідності ЕЦП – заявки та матеріали не повинні реєструватись та обробляться підсистемою обробки заявок ЕСОПВЛЗ-ДСЛЗ.

26. Доступ до Веб-сайту адміністраторів системи повинен здійснюватися лише з визначеного діапазону IP-адрес.

27. При розробці системи повинні бути визначені можливі типи помилок і механізми обробки аварійних ситуацій. При виникненні помилок або аварійних ситуацій, система повинна видавати користувачам повідомлення про це, не вказуючи при цьому жодних додаткових даних (наприклад, налагоджувальної інформації, дамів пам'яті тощо). Повідомлення про помилку не повинно містити інформації про архітектуру і внутрішню структуру системи.

28. Розроблене прикладне програмне забезпечення ЕСОПВЛЗ-ДСЛЗ повинно вміти перехоплювати всі виключення. Невідоме виключення повинне повертати загальний код помилки.

29. В ЕСОПВЛЗ-ДСЛЗ повинно бути забезпечено реєстрацію всіх подій, які мають безпосереднє відношення до безпеки і зберігати їх в окремо виділеній від веб-порталу бази даних. До них відносяться наступні класи подій:

- вхід/вихід або намагання входу/виходу в/із системи користувачами будь-яких категорій;

- реєстрація та видалення або намагання реєстрації та видалення користувачів будь-якої категорії в системі;

- створення користувачем будь-якої категорії твердих копій та виведення їх на друкуючі пристрої.

Веб-сайт повинен надавати можливість визначення переліку реєстраційних подій виключно адміністратору системи.

Реєстрація всіх подій, що мають безпосереднє відношення до безпеки, здійснюється в журналі реєстрації, який повинен містити інформацію стосовно дати, часу, місця, типу і наслідків зареєстрованої події (успішність/неуспішність), ім'я (IP-адресу) та/або ідентифікатор причетного до цієї події користувача. Реєстраційна інформація повинна бути достатньою для однозначної ідентифікації користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

30. Забороняється використовувати не сертифіковані згідно законодавства України в галузі криптографічного захисту інформації засоби накладання та перевірки ЕЦП.

31. Певні типи помилок повинні реєструватися в журналах збоїв. Склад реєстрованих помилок повинен бути визначений на стадії технічного проектування.

32. Доступ веб-сайту до СУБД повинен здійснюватися з обліковим записом з мінімальними правами.

33. Перед запуском веб-сайту здійснити перевірку вихідних кодів на предмет наявності вразливостей, що виникають при недостатній та/або некоректній фільтрації (обробці) вхідних даних (атаки типу JS-, PHP-, SQL-ін'єкції, XSS та інші).

34. Зовнішній інтерфейс Веб-порталу (відкритий доступ без автентифікації) повинен віддавати запитувану інформацію у спосіб, що не спричиняє великого навантаження на Веб-сервер, веб-сторінки повинні генеруватися швидко або бути статичними. Це дозволить знизити рівень навантаження на Веб-сервер при здійсненні мережових атак типу відмови в обслуговуванні.

35. HTML-сторінки, які передаються користувачу, повинні містити гіперпосилання тільки на офіційні веб-сайти органів державної влади у домені gov.ua.

36. Всі сценарії JavaScript, які виконуються на стороні користувача, повинні знаходитись на сервері застосувань. Забороняється використовувати сценарії, які розміщені на сторонніх веб-ресурсах.

37. Основний обліковий запис СУБД повинен бути захищений складним паролем.

38. Основний обліковий запис СУБД повинен бути перейменований.

39. Повинен бути заблокований анонімний доступ до бази даних (використовуючи обліковий запис nobody).

40. Процеси СУБД повинні виконуватися під унікальним UID/GID, невживаних ніяким іншим системним процесом.

41. Логічна структура бази даних повинна проектуватися з урахуванням реалізації функції СУБД з розмежування доступу до даних.

42. Повинні бути видалені всі типові бази даних і таблиці.

43. Всі паролі, що розміщуються у СУБД повинні зберігатися у зашифрованому вигляді.

44. Персональні дані, заяви суб'єктів звернення та відповіді на них повинні зберігатися у полях таблиць баз даних у зашифрованому вигляді.



45. На сторінці веб-сайту ЕСОПВЛЗ-ДСЛЗ із запрошенням про авторизацію повинна бути розміщена «Інструкція (настанова) з безпечної роботи з веб-порталом».

ЕСОПВЛЗ-ДСЛЗ повинна передбачати можливість резервного копіювання та відновлення системних та користувацьких даних.

### **5.1.9. Вимоги до забезпечення збереження інформації у випадку аварійних ситуацій**

Забезпечення збереження інформації у випадку аварійних ситуацій повинно передбачатись архітектурою системи. Система повинна передбачати обов'язкове створення резервних копій баз даних, файлів налаштувань, тощо. Відновлення інформації у випадку аварій повинно виконуватись за допомогою наперед передбачених сценаріїв адміністратором системи за мінімально можливий термін.

### **5.2. Вимоги до функцій (задач), що виконуються ЕСОПВЛЗ-ДСЛЗ**

ЕСОПВЛЗ-ДСЛЗ повинна реалізовувати надання юридичним особам пілотних електронних адміністративних послуг в електронній формі, а саме:

- подання заявником документів для отримання пілотних послуг в електронній формі з використанням ЕЦП та направленою шифрування;
- перевірка, реєстрація та опрацювання відповідальними працівниками Держлікслужби або територіальних органів Держлікслужби поданих заявником документів в електронній формі;
- видача результату надання пілотних адміністративних послуг у спосіб визначений заявником (особисто, повідомлення в електронній формі);
- надання заявникам електронних інформаційних сервісів, що супроводжують процес надання пілотних адміністративних послуг: повідомлення про успішну перевірку та про реєстрацію електронного документу/відмову у реєстрації; повідомлення про результат адміністративної послуги.

## **Розділ 6. ВИМОГИ ДО РОЗРОБКИ ТА ПЕРЕДАЧІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ**

### **6.1. Вимоги до розробника програмного забезпечення**

Розробник програмного забезпечення повинен надати підтвердження реалізації веб-систем схожої складності.

Проект повинен включати розробку технічного завдання, програмного забезпечення, встановлення його на серверах бенефіціара, налаштування та впровадження його в експлуатацію.

### **6.2. Вимоги до передачі програмного забезпечення**

При передачі програмного забезпечення мають бути передані:

- Невиключні майнові права на розроблюване програмне забезпечення;

- Вихідні коди програмного забезпечення в електронному вигляді;
- Інсталяційний пакет програмного забезпечення в електронному вигляді;
- Інструкція по інсталяції та розгортанню програмного забезпечення;
- Інструкція адміністратора програмного забезпечення;
- Інструкція користувача програмного забезпечення;
- Технічне завдання на програмне забезпечення;
- Загальний опис програмного забезпечення;
- Програма та методика випробувань програмного забезпечення;

### **5.3. Отримувач програмного забезпечення**

Кінцевим бенефіціаром та користувачем програмного забезпечення є Держлікслужба.