

ТЕХНІЧНІ ВИМОГИ

на послуги зі створення комп'ютерної програми для модернізації Єдиного державного вебпорталу електронних послуг з метою розширення функціоналу системи онлайн моніторингу та оцінки якості послуг

Зміст

1 ЗАГАЛЬНІ ПОЛОЖЕННЯ	5
1.1 Підстава для розроблення технічних вимог.....	5
1.2. Найменування засобу інформатизації	5
1.3. Мета створення засобу інформатизації	5
1.4 Терміни та скорочення.....	6
2. ОБГРУНТУВАННЯ ПОТРЕБИ	7
2.1 Опис потреби Бенефіціара	7
2.2 Призначення модернізації.....	8
2.3 Найменування сторін	8
2.4 Нормативно–законодавча база	9
2.5. Опис робочих процесів (бізнес-процесів).	10
3. ОПИС ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ОБ’ЄКТІВ ІНФОРМАТИЗАЦІЇ	11
4. ВИМОГИ ДО ЗАСОБУ ІНФОРМАТИЗАЦІЇ	11
4.1. Вимоги до загальної побудови та складу засобу інформатизації.	11
4.2. Вимоги до функцій (завдань), що виконуються засобом інформатизації.	13
4.2.1 Зміни рольової моделі	13
4.2.1.1 Делегування доступів та ієрархія ролей (RBAC)	13
4.2.1.2 Машина станів електронного звіту (State Machine)	14
4.2.1.3 Версійність та збереження історії змін звіту	15
4.2.2. Зміни у довідниках	15
4.2.2.1 Довідники адміністративних послуг	15
4.2.2.2 Адресні довідники та геокодування.....	16
4.2.2.3 Дані про чисельність населення та автоматична категоризація ЦНАП	16
4.2.3. Конфігурація звітності	16
4.2.3.1 Функціональні вимоги до Конфігуратора	16
4.2.3.2 Архітектурні обмеження збереження даних	17
4.2.3.3 Юридична значущість та електронний підпис	17
4.2.3.4 Експорт даних	17
4.2.4. Профілі	17
4.2.4.1 Відомості про ЦНАП	18
4.2.4.2 Територіальні підрозділи та ВРМ	19
4.2.4.3 Відомості про СНАП.....	19
4.2.5. Реєстр ЦНАП	20
4.2.5.1 Механізм версійності та оновлення даних.....	20
4.2.5.2 Склад атрибутів Реєстру	20
4.2.6. Експорт реєстру ЦНАП.....	21
4.2.6.1 Формати експорту	21
4.2.6.2 Обмеження доступу та маскування даних (White-list підхід)	21
4.2.7. Звітність для побудови рейтингу	21

4.2.7.1 Вимоги до форми звіту «Показники відповідності офлайн фронт-офісу»	22
4.2.7.2 Вимоги до форми звіту «Показники відповідності онлайн фронт-офісу».....	22
4.2.7.3 Вимоги до форми звіту «Показники ефективності надання адміністративних послуг».....	23
4.2.7.4 Вимоги до модернізації доступу та агрегації (RBAC).....	23
4.2.8. Додаткова звітність	23
4.2.8.1 Вимоги до форми «Звіт за наявними інформаційними системами».....	24
4.2.8.2 Вимоги до форми «Звіт за працівниками»	24
4.2.8.3 Правила доступу, агрегації та редагування додаткової звітності (RBAC)	25
4.2.8.4 Вимоги до форми «Звіт за послугами».....	25
4.2.9. Валідація звітності.....	25
4.2.10. Контроль термінів подачі звітності	26
4.2.11. Модифікація реєстру ЦНАП	26
4.2.12 Розробка API для інтеграції з Платформою центрів Дії.....	27
4.2.13. Розробка API для імпорту відомостей до Системи онлайн-моніторингу.....	30
4.2.14. Розробка API для експорту відомостей щодо показників ЦНАП.....	30
4.2.15. Створення статичного звіту з переліком послуг, що надаються у ЦНАП.....	30
4.2.15.1 Архітектура та інтеграція	30
4.2.15.2 Валідація та Інтерфейс (UI)	31
4.2.16. Функціонал подачі заяви на підключення до Системи онлайн-моніторингу (Онбординг)	31
4.2.17. Розробка функціоналу відкритих даних.....	31
4.2.18. Функціонал збору фінансової звітності	32
4.2.18.1 Інтеграція з Конфігуратором звітів	32
4.2.18.2 Структура фінансових показників	32
4.2.18.3 Аналітика та Валідація.....	32
4.2.19. Функціонал семантичного аналізу місцевих послуг.....	33
4.2.20. Функціонал збору та аналізу повідомлень про надмірні документарні вимоги ...	33
4.2.21. Функціонал збору фотопідтверджень показників статичного моніторингу	36
4.2.21.1 Завантаження та обробка медіафайлів	36
4.2.21.2 Модуль перевірки (модерації) медіаданих	37
4.2.21.3 Динамічне управління показниками моніторингу	37
4.2.22. Функціонал аналітичної візуалізації та формування презентаційних матеріалів.	37
4.2.22.1 Візуалізація показників	38
4.2.22.2 Порівняльна аналітика	38
4.2.22.3 Інтерактивні дашборди	38
4.2.22.4 Експорт аналітичних матеріалів.....	38
4.2.22.5 Формування презентацій за шаблонами.....	39
4.2.22.6 API доступ до агрегованих даних моніторингу	39
4.2.22.7 Агрегування даних для аналітики.....	39
4.2.22.8 Версійність показників моніторингу	39

4.3. Вимоги до персоналу, що забезпечує функціонування та експлуатацію засобу інформатизації.	40
4.4. Вимоги до режимів функціонування засобу інформатизації.	40
4.5. Вимоги до надійності роботи та збереження інформації.	41
4.5.1. Управління змінами (Change Request, CR)	42
4.5.2. Порядок міграції даних	42
4.6. Вимоги до захисту інформації та кіберзахисту.	42
4.7. Вимоги до продуктивності.	43
4.8. Вимоги до інтерфейсу користувача та зручності використання.....	43
5. ВИМОГИ ДО СУПРОВОДУ ТА ОБСЛУГОВУВАННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ	45
5.1. Вимоги до гарантійної підтримки.....	45
5.2. Вимоги до навчання користувачів (за потреби);	46
5.3. Вимоги до документації.....	46
6. ВИМОГИ ДО ПРИЙМАННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ	47
6.1 Вимоги до проведення випробувань.....	47
6.1.1. Функціональне тестування	47
6.1.2. Навантажувальне тестування	47
6.1.3. Тестування на проникнення (Pentest)	47
6.1.4. Приймальне тестування (UAT)	48
6.2. Вимоги до передачі результатів виконаних робіт та/або наданих послуг.	48
6.3 Порядок приймання.....	48
7. ВИМОГИ ДО ВИКОНАВЦЯ	49
8. ОРІЄНТОВНИЙ КАЛЕНДАРНИЙ ПЛАН РОЗРОБКИ СИСТЕМИ ОНЛАЙН-МОНІТОРИНГУ	50

1 ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1 Підстава для розроблення технічних вимог

Технічні вимоги зі створення комп'ютерної програми для модернізації Єдиного державного вебпорталу електронних послуг з метою розширення функціоналу системи онлайн-моніторингу та оцінки якості розроблені в ініціативному порядку для запровадження системи моніторингу якості надання послуг суб'єктами надання адміністративних послуг (далі — СНАП) за показниками якості відповідно до Порядку проведення моніторингу якості надання адміністративних послуг та оприлюднення інформації про результати моніторингу якості надання адміністративних послуг, затвердженого постановою Кабінету Міністрів України від 11.08.2021 № 864.

1.2. Найменування засобу інформатизації

Повна назва – Комп'ютерна програма (модуль Єдиного державного вебпорталу електронних послуг) «Система онлайн-моніторингу та оцінки якості послуг».

Скорочена назва – КП «Система онлайн-моніторингу та оцінки якості послуг», «Система онлайн-моніторингу».

1.3. Мета створення засобу інформатизації

Головною метою створення комп'ютерної програми для модернізації Системи онлайн-моніторингу є розширення її функціональних можливостей для забезпечення проведення моніторингу якості надання адміністративних послуг, збору, обробки, перевірки, аналізу та візуалізації відповідних даних, а також інтеграційної взаємодії з іншими інформаційними системами, зокрема:

- запровадження моніторингу якості надання послуг суб'єктами надання адміністративних послуг (далі — СНАП) за показниками якості відповідно до «Порядку проведення моніторингу якості надання адміністративних послуг та оприлюднення інформації про результати моніторингу якості надання адміністративних послуг», затвердженому Постановою КМУ від 11.08.2021 №864;

- забезпечення можливості збору, обробки, перевірки та аналізу даних за встановленими показниками й у порядку проведення моніторингу якості надання адміністративних послуг;

- створення механізму динамічного управління структурою статичних даних та звітів шляхом розробки та впровадження програмного продукту з використанням нереляційних типів даних (формат JSONB) для забезпечення гнучкого управління структурою звітів без необхідності зміни фізичної схеми бази даних, із збереженням транзакційної цілісності та контролю на рівні PostgreSQL;

- реалізація можливості підключення до Системи онлайн-моніторингу інформаційних систем, реєстрів та баз даних суб'єктів, визначених їх держателями, з метою проведення автоматизованого моніторингу замовлених послуг;

- забезпечення інтеграції Системи онлайн-моніторингу з електронним кабінетом Порталу Дія, Національною вебплатформою центрів надання адміністративних послуг та Реєстром адміністративних послуг шляхом розробки стандартизованих RESTful API;

- запровадження функціоналу фінансової звітності для збору, обробки та аналізу даних щодо витрат і доходів ЦНАП із можливістю перехресної звірки;

- забезпечення візуалізації показників у дашбордах;

- перехід до ризик-орієнтованого підходу (СУІБ) в управлінні інформаційною безпекою з урахуванням вимог чинного законодавства України щодо захисту інформації в інформаційно-комунікаційних системах та, у випадках, передбачених законодавством, забезпечення створення та/або модернізації авторизованої системи з безпеки інформації.

У частині функціоналу, запровадження або застосування якого потребує внесення змін до нормативно-правових актів, використання відповідних компонентів Системи онлайн-моніторингу в межах обов'язкового моніторингу здійснюється після набрання чинності такими змінами.

1.4 Терміни та скорочення

Поняття або скорочення	Пояснення
ЗІ	засіб інформатизації
Система онлайн-моніторингу	Комп'ютерна програма (модуль) Єдиного державного вебпорталу електронних послуг, яка призначена для збору та обробки оціночних даних, розміщення результатів моніторингу, а також ведення профілів центрів надання адміністративних послуг
ЦНАП	центр надання адміністративних послуг
СНАП	суб'єкт надання адміністративних послуг
ТП	територіальний підрозділ
ВРМ	віддалене робоче місце
ОДА	обласна державна адміністрація
ОВА	обласна військова адміністрація
ЦОВВ	центральний орган виконавчої влади
ОМС	орган місцевого самоврядування
КЕП	кваліфікований електронний підпис
КП	комп'ютерна програма
УЕП	удосконалений електронний підпис
ПД	персональні дані
ЄДР	Єдиний державний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань
ЄДДР	Єдиний державний демографічний реєстр
ДЗК	Державний земельний кадастр
ДРАЦС	Державний реєстр актів цивільного стану громадян
ЄІССС	Єдина інформаційна система соціальної сфери
ЄДЕССБ	Єдина державна електронна система у сфері будівництва

Поняття або скорочення	Пояснення
КАТОТТГ	Кодифікатор адміністративно-територіальних одиниць та територій територіальних громад
КОАТУУ	Класифікатор об'єктів адміністративно-територіального устрою України
СЕД	система електронного документообігу
ТЕО	техніко-економічне обґрунтування
СБІ	система з безпеки інформації
СУІБ	система управління інформаційною безпекою
IDF	унікальний ідентифікатор об'єкта в Системі онлайн-моніторингу
API	прикладний програмний інтерфейс
RBAC	управління доступом на основі ролей
SLA	угода про рівень послуг
UAT	приймальне тестування за участю користувача
CR	запит на зміну
RPO	цільовий показник відновлення даних
RTO	цільовий час відновлення працездатності
SAST	статичний аналіз коду на вразливості
DAST	динамічний аналіз застосунку на вразливості
NLP	обробка природної мови
CI/CD	безперервна інтеграція та безперервне розгортання
Git	розподілена система контролю версій
DDL	команди визначення структури бази даних

2. ОБґРУНТУВАННЯ ПОТРЕБИ

2.1 Опис потреби Бенефіціара

Очікуваними результатами модернізації є удосконалення існуючого функціоналу Єдиного державного вебпорталу електронних послуг, зокрема:

- вдосконалення функціоналу звітності статичного моніторингу;
- запровадження та вдосконалення функціоналу онлайн-моніторингу якості послуг для всіх суб'єктів надання адміністративних послуг;

- опублікування та динамічне оновлення результатів моніторингу та інших показників функціонування ЦНАП на Національній вебплатформі центрів надання послуг;
- впровадження спеціалізованих пошукових рушіїв та/або інтеграцію бібліотек обробки природної мови (NLP) для аналізу подібності місцевих послуг та їхнього об'єднання;
- розробка власної або інтеграція до Системи онлайн-моніторингу інших існуючих систем оцінки рівня задоволеності суб'єктів звернення;
- розробка універсального та безпечного інтерфейсу, що дозволить ЦНАП (ТП та ВРМ), СНАП та ЦОВВ завантажувати фотографії відповідно до визначених показників;
- модернізація існуючого профілю та Реєстру ЦНАП у частині доповнення та деталізації відомостей про доступність, безбар'єрність і облаштування ЦНАП, ТП та ВРМ відповідно до показників статичного моніторингу та вимог законодавства щодо доступності для маломобільних груп населення;
- розробка функціоналу для можливості побудови презентаційних матеріалів, за усіма обраними показниками моніторингу;
- розробка функціоналу для порівняння показників між будь-якими ЦНАП (ТП та ВРМ), СНАП та ЦОВВ з метою оцінки їхньої ефективності (із застосуванням актуального Кодифікатора КАТОТТГ);
- розробка та впровадження функціоналу для автоматичного порівняння актуальних оціночних даних показників з аналогічними за попередній звітний період;
- запровадження додаткового аналітичного функціоналу для збору, семантичного аналізу, класифікації та опрацювання повідомлень Операторів ЦНАП про надмірні, необґрунтовані, застарілі або дублюючі документарні вимоги у процесах надання адміністративних послуг з метою їх подальшого аналізу, скерування відповідальним органам та підготовки управлінських пропозицій.

Критеріями досягнення мети модернізації визначено такі принципи:

Відповідність законодавству України (зокрема дотримання стандартів інженерії вимог ДСТУ ISO/IEC/IEEE 29148:2025 та Обов'язкових вимог КМУ №205).

Гнучкість та масштабованість архітектури.

Максимальне використання конфігураторів та конструкторів у рамках Системи онлайн-моніторингу.

Вебдоступність та інклюзивність на рівні глибинної семантичної верстки HTML згідно з ДСТУ EN 301 549:2022.

Виконавець зобов'язаний сформулювати технічне завдання, експлуатаційну, звітну та іншу супровідну документацію відповідно до вимог цього документа. Склад та вимоги до переданої документації визначаються у розділах 5.3 та 6.2 цього документа.

2.2 Призначення модернізації

Призначенням комп'ютерної програми «Система онлайн-моніторингу та оцінки якості послуг» (далі – Система онлайн-моніторингу), яка є модулем Єдиного державного вебпорталу електронних послуг, є створення функціональних можливостей для забезпечення збору, обробки, перевірки, аналізу та оприлюднення результатів моніторингу якості надання адміністративних послуг відповідно до законодавства України.

У межах модернізації повинно бути забезпечено розвиток функціоналу Єдиного державного вебпорталу електронних послуг, необхідного для ведення профілів суб'єктів моніторингу, формування та подання звітності, обробки оціночних даних, візуалізації показників, інтеграційної взаємодії з іншими інформаційними ресурсами та виконання інших функцій, визначених цими Технічними вимогами.

2.3 Найменування сторін

Замовник — визначається Міністерством цифрової трансформації України.
Бенефіціар/Реципієнт — Міністерство цифрової трансформації України.
Технічний адміністратор — Державне підприємство “ДІА”.
Виконавець — визначається замовником послуг.

2.4 Нормативно–законодавча база

Система онлайн-моніторингу, повинна розроблятися з урахуванням вимог чинних нормативно–правових документів, а саме:

- Конституція України;
- Закон України “Про електронну ідентифікацію та електронні довірчі послуги”;
- Закон України “Про інформацію”;
- Закон України “Про електронні документи та електронний документообіг”;
- Закон України “Про доступ до публічної інформації”;
- Закон України “Про захист персональних даних”;
- Закон України “Про захист інформації в інформаційно–комунікаційних системах”;
- Закон України “Про звернення громадян”;
- Закону України “Про адміністративні послуги”;
- Закон України “Про внесення змін до деяких законодавчих актів України щодо оптимізації мережі та функціонування центрів надання адміністративних послуг та удосконалення доступу до адміністративних послуг, які надаються в електронній формі”;
- Указ Президента України від 04.09.2019 № 647 “Про деякі заходи із забезпечення надання якісних публічних послуг”;
- Постанова Кабінету Міністрів України від 18.09.2019 № 856 “Питання Міністерства цифрової трансформації”;
- Постанова Кабінету Міністрів України від 04.12.2019 № 1137 “Питання Єдиного державного вебпорталу електронних послуг та Єдиного державного порталу адміністративних послуг”;
- Постанова Кабінету Міністрів України від 11.08.2021 № 864 “Питання організації моніторингу якості надання адміністративних послуг”;
- Постанова Кабінету Міністрів України від 03.02.2021 № 72 “Про Національну веб–платформу центрів надання адміністративних послуг”;
- Наказ Міністерства цифрової трансформації України від 11.11.2021 № 145 “Щодо питання забезпечення моніторингу якості надання адміністративних послуг”;
- Наказ Міністерства цифрової трансформації України від 10.12.2021 року № 173, “Про затвердження Основних вимог до якості обслуговування суб’єктів звернення”;
- Наказ Міністерства цифрової трансформації України від 11.11.2021 № 146 “Деякі питання передачі відомостей із системи онлайн–моніторингу та оцінки якості послуг Єдиного державного вебпорталу електронних послуг до Національної веб–платформи центрів надання адміністративних послуг (Платформи Центрів Дія);
- Наказ Міністерства цифрової трансформації від 16.11.2021 № 148 “Про затвердження Змін до Порядку обробки та захисту персональних даних, володільцем яких є Міністерство цифрової трансформації України”;
- Наказ Міністерства цифрової трансформації України від 04.08.2021 № 104 “Повідомлення суб’єктів персональних даних про обробку персональних даних на Національній веб–платформі центрів надання адміністративних послуг (Платформі Центрів Дія)”;
- Постанова Кабінету Міністрів України від 21.02.2025 № 205 “Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації”.

Даний перелік нормативно–правових актів не є вичерпним. Виконавець зобов’язаний забезпечити виконання вимог чинного законодавства України, що стосуються мети, призначення та функціонування Системи, у тому числі у разі оновлення/зміни відповідних нормативно–правових актів.

Технічні вимоги цього документа є обов’язковими для виконання у межах предмета закупівлі та застосовуються як технічна специфікація (вимоги Замовника до результату робіт). Уточнення допускаються виключно як деталізація (без зменшення обсягу та без погіршення характеристик/функціональності) та здійснюються лише у порядку управління змінами (Change Request, CR), визначеному цим документом.

2.5. Опис робочих процесів (бізнес-процесів).

У ході виконання робіт Виконавець повинен проаналізувати та оформити звіт за результатами аналізу робочих процесів (бізнес-процесів), який має бути погоджений із Бенефіціаром.

У межах модернізації Системи онлайн-моніторингу підлягають автоматизації, модернізації або функціональному доопрацюванню такі основні робочі процеси (бізнес-процеси):

- управління користувачами, ролями та правами доступу відповідно до рольової моделі Системи онлайн-моніторингу;
- ведення та оновлення профілів ЦНАП, ТП, ВРМ та СНАП;
- формування, подання, перевірка, повернення на доопрацювання, погодження та опублікування звітності;
- динамічне налаштування структури звітів, показників, форм та правил валідації через Конфігуратор;
- ведення Реєстру ЦНАП та оновлення його атрибутів на підставі даних профілів і затвердженої звітності;
- внесення та аналіз інформації про місцеві послуги, включаючи виявлення подібних або дублюючих записів;
- збір, обробка та аналіз фінансової звітності ЦНАП;
- збір, перевірка та модерація фотопідтверджень показників статичного моніторингу;
- збір, семантичний аналіз, маршрутизація та опрацювання повідомлень Операторів ЦНАП про надмірні документарні вимоги;
- інтеграційний обмін даними з іншими інформаційними системами, реєстрами та платформами через API;
- формування аналітичних дашбордів, звітів, презентаційних матеріалів, відкритих даних та експортів.

Для кожного з визначених робочих процесів Виконавець у межах підготовки технічного завдання повинен здійснити деталізацію, що включає щонайменше:

- учасників процесу та їх ролі;
- вхідні дані та джерела їх отримання;
- основну послідовність дій;
- статуси, переходи між статусами та умови їх зміни;
- вихідні дані або результат процесу;
- виняткові ситуації та сценарії повернення на доопрацювання;
- вимоги до журналювання, аудиту та збереження історії змін;
- точки інтеграційної взаємодії з іншими системами, у разі наявності.

За результатами аналізу робочих процесів Виконавець повинен підготувати опис бізнес-процесів у складі технічного завдання, який підлягає погодженню з Бенефіціаром. Деталізація бізнес-процесів не повинна зменшувати обсяг функціональних вимог, визначених цими Технічними вимогами, або погіршувати характеристики Системи онлайн-моніторингу.

3. ОПИС ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ОБ'ЄКТІВ ІНФОРМАТИЗАЦІЇ

Об'єктом інформатизації є комп'ютерна програма (модуль) Єдиного державного вебпорталу електронних послуг. Його головне завдання в результаті модернізації – забезпечувати збір, обробку, валідацію та візуалізацію показників моніторингу якості надання адміністративних послуг, а також формування різноманітної звітності й аналітичних матеріалів.

Модернізована система має підтримувати чітку взаємодію різних груп користувачів: від операторів Мінцифри, які здійснюють центральне адміністрування, до відповідальних осіб ЦНАП, їхніх територіальних підрозділів (ТП), віддалених робочих місць (ВРМ), СНАП та обласних військових адміністрацій (ОВА). Ця розгалужена мережа користувачів відповідатиме за подання та перевірку звітності, а також завантаження підтверджувальних матеріалів на базі відповідної рольової моделі.

Під час своєї роботи оновлена Система онлайн-моніторингу має оперувати різноманітними типами даних. Це довідники й реєстри (зокрема, ЦНАП, СНАП, переліки послуг та показників), безпосередні звітні дані, протоколи валідації, службові записи аудиту, а також медіафайли, наприклад, фотографії для підтвердження виконання показників. Оскільки ці масиви можуть містити персональні дані (ПІБ або контактні номери відповідальних осіб), їхня обробка повинна суворо відповідати законодавству України про захист персональних даних.

Для забезпечення стабільного, своєчасного та автоматизованого обміну даними Систему онлайн-моніторингу необхідно інтегрувати з іншими компонентами цифрової екосистеми. Серед обов'язкових взаємодій – підсистеми автентифікації та електронного кабінету (ID.GOV.UA), Платформа центрів Дія, спеціалізовані інформаційні системи автоматизації роботи ЦНАП (зокрема, ІС «Вулик» та аналогічні рішення), а також інші державні інформаційні системи та реєстри в межах затверджених регламентів інформаційної взаємодії. Крім того, оновлена Система онлайн-моніторингу має надавати власні API для зручного імпорту й експорту даних (в тому числі для безшовної передачі звітних даних із систем рівня «Вулик»), а також для формування наборів відкритих даних.

Технічне функціонування та життєвий цикл Системи онлайн-моніторингу повинні забезпечуватися щонайменше у трьох середовищах: розробки, тестування та промислової (продуктивної) експлуатації. Процес розгортання має реалізовуватися у контейнеризованому вигляді (за допомогою Docker) з використанням існуючої серверної інфраструктури або обчислювальних потужностей технічного адміністратора.

4. ВИМОГИ ДО ЗАСОБУ ІНФОРМАТИЗАЦІЇ

4.1. Вимоги до загальної побудови та складу засобу інформатизації.

Розробка КП Система онлайн-моніторингу (включаючи прикладний рівень, рівень доступу до даних та інтеграційні інтерфейси) повинна здійснюватися без порушення працездатності існуючих функцій та без втрати сумісності з наявною архітектурою розгортання. Рішення повинні забезпечувати продуктивність, інформаційну безпеку та горизонтальну/вертикальну масштабованість.

Мова програмування та бекенд-фреймворк:

Основною мовою залишається Python.

Фреймворк: Django (для серверної логіки та веброботи).

Умова: Допускається оновлення мінорних версій фреймворків у межах версій з довгостроковою підтримкою виробника, за умови забезпечення сумісності, безперервності та стабільності функціонування КП Система онлайн-моніторингу.

Зміна базового технологічного стеку фронтенду допускається виключно за умови погодження відповідного Запиту на зміну (Change Request, CR) у встановленому порядку.

Бази даних та архітектура збереження:

PostgreSQL залишається основною системою керування реляційними базами даних.

Архітектурне обмеження для Конфігуратора звітності: Зберігання динамічних структур звітів повинно реалізовуватися виключно з використанням нереляційних типів даних PostgreSQL, зокрема формату JSONB. Структура кожного звіту (метадані) повинна зберігатися у вигляді JSON Schema. Застосування патерну EAV (Entity–Attribute–Value) або динамічної генерації DDL–запитів (ALTER TABLE) для створення нових таблиць/стовпців під кожен новий звіт суворо забороняється.

Технології пошуку та семантичного аналізу (NLP):

Для забезпечення аналізу інформації про місцеві послуги та визначення їхньої подібності, архітектура повинна передбачати використання спеціалізованих повнотекстових пошукових рушіїв (наприклад, Elasticsearch або OpenSearch) та/або інтеграцію бібліотек обробки природної мови (NLP). Алгоритми мають враховувати морфологію української мови та синонімічні ряди.

Система обробки задач (Message Broker / Task Queue):

Celery для асинхронної обробки завдань та планування.

Redis як брокер повідомлень для воркерів та підсистема кешування.

Деплоймент, Інфраструктура та Оркестрація (DevOps):

Docker:

Усі програмні компоненти Системи онлайн-моніторингу (включаючи прикладний рівень (backend), інтерфейс користувача (frontend), інтеграційні інтерфейси (API) та допоміжні сервіси), що створюються або модифікуються в межах цієї модернізації, повинні бути контейнеризовані.

Середовища:

Для середовищ dev та test забезпечується можливість відтворюваного локального розгортання програмного забезпечення Системи онлайн-моніторингу, що створюється або змінюється в межах модернізації. Конфігурація повинна дозволяти повне розгортання залежностей, сервісів та баз даних, необхідних для коректної роботи компонентів.

Програмне забезпечення Системи онлайн-моніторингу повинно підтримувати розгортання у промисловому середовищі (prod) на базі Kubernetes–кластера, що надається або визначається Замовником чи уповноваженим технічним адміністратором.

Stateful–компоненти:

Stateful–компоненти (зокрема PostgreSQL, Redis, а також підсистеми резервного копіювання) можуть розгортатися як частина Kubernetes–кластера із використанням механізмів persistent storage або як окремі керовані (managed) сервіси Замовника. Остаточна модель розгортання визначається технічним адміністратором Замовника.

Сумісність:

Виконавець зобов'язаний забезпечити сумісність нових та змінених компонентів програмного забезпечення Системи онлайн-моніторингу з обраною Замовником моделлю розгортання та інфраструктурними стандартами. Несумісність із середовищем продакшн–розгортання не допускається та є підставою для неприймання результатів робіт.

Зони відповідальності:

Виконавець постачає Helm–чарти або Kustomize–маніфести, базові налаштування Horizontal Pod Autoscaler (HPA), ліміти та запити ресурсів, а також повну інструкцію з розгортання та оновлення системи.

Інфраструктура розгортання (Kubernetes–кластер, container registry, система управління секретами) визначається Замовником або технічним адміністратором окремо. Виконавець зобов'язаний забезпечити сумісність програмного забезпечення Системи з такою інфраструктурою.

Система контролю версій та CI/CD:

Використання Git (переважно GitLab) для спільної розробки. Налаштування автоматизованих pipeline для безперервної інтеграції, тестування (DevSecOps) та розгортання.

Моніторинг та Логування (Observability):

Метрики: Експорт метрик (HTTP latency/p95, error rate, queue depth, DB connections) у форматі, сумісному з Prometheus (через /metrics endpoint).

Логи: Структуроване логування у форматі JSON із наскрізним ідентифікатором запиту (request_id). Усі чутливі та персональні дані повинні обов'язково маскуватися перед відправкою до системи централізованого збору логів (напр., стек ELK).

Алерти: Налаштування критичних сценаріїв сповіщень (зростання помилок 5xx, падіння API) для систем Zabbix або Prometheus. Вибір кінцевого інструменту визначається технічним адміністратором Замовника.

Заходи безпеки:

Оновлення та перевірка управління сесіями, обробка автентифікації. Жорстке кодування (hardcoding) токенів, паролів або API-ключів у вихідному коді забороняється.

Уніфікація та інтероперабельність:

- приведення до єдиних підходів ідентифікаторів, довідників та форматів даних (JSON UTF-8 для API, уніфіковані коди/ID);
- забезпечення версіонування API та зворотної сумісності існуючих контрактів при їхній модифікації;
- усі нові та оновлені інтеграційні контракти мають бути обов'язково задокументовані за допомогою специфікації OpenAPI (Swagger) версії 3.0+.

4.2. Вимоги до функцій (завдань), що виконуються засобом інформатизації.

4.2.1 Зміни рольової моделі

У рамках модернізації Системи онлайн-моніторингу існуюча рольова модель має бути приведена до децентралізованої ієрархії управління доступами (RBAC). Термінологія ролей уніфікується: використання термінів «адміністратор» та «оператор» як синонімів не допускається, базовим терміном є «Оператор».

4.2.1.1 Делегування доступів та ієрархія ролей (RBAC)

Система онлайн-моніторингу повинна підтримувати 5 базових ролей із наступним розподілом прав:

Оператор Мінцифри:

- *Управління користувачами:* Реєструє, верифікує та керує обліковими записами виключно Операторів ОДА (ОВА) та ЦОВВ;
- *Робота зі звітами:* Має право перегляду всіх звітів. Має право повернути на доопрацювання будь-який поданий звіт (ЦНАП, СНАП, ЦОВВ, ОДА);
- *Робота з повідомленнями про надмірні документарні вимоги:* переглядає результати семантичного аналізу повідомлень, підтверджує або змінює попередню класифікацію, присвоює статуси, визначає відповідальний ЦОВВ або СНАП та скеровує повідомлення на опрацювання;
- *Експорт:* Має доступ до експорту загальної агрегованої статистики (з обов'язковим сортуванням XLSX-файлів за полем «Назва органу, що утворив центр»).

Оператор ОДА (ОВА):

- *Управління користувачами:* Реєструє та керує обліковими записами Операторів ЦНАП виключно в межах своєї області (регіону).

- Робота зі звітами: Перевіряє, погоджує або повертає на доопрацювання звіти підпорядкованих ЦНАП.

Оператор ЦОВВ:

- Управління користувачами: Підтверджує реєстрацію та керує обліковими записами Операторів СНАП у своїй сфері;
- Робота зі звітами: Перевіряє, погоджує або повертає звіти підпорядкованих СНАП. Доступ обмежується виключно послугами, щодо яких ЦОВВ формує державну політику (на основі Реєстру адмінпослуг);
- Опрацювання скерованих повідомлень: розглядає повідомлення про надмірні документарні вимоги, скеровані Оператором Мінцифри, та надає позицію, пояснення, нормативне обґрунтування або пропозиції щодо усунення відповідної вимоги в межах компетенції.

Оператор ЦНАП:

- Управління користувачами: Управляє профілем свого головного центру та самостійно створює/керує підпорядкованими ТП та ВРМ;
- Робота зі звітами: Створює, редагує та направляє звіти (включаючи звіти за ТП та ВРМ);
- Подання повідомлень: подає первинні повідомлення про надмірні, необґрунтовані, застарілі або дублюючі документарні вимоги, що виникають у процесах надання адміністративних послуг через відповідний ЦНАП, ТП або ВРМ.

Оператор СНАП:

- Управління користувачами: Управляє виключно профілем своєї організації;
- Робота зі звітами: Створює, редагує та направляє власні звіти;
- Опрацювання скерованих повідомлень: розглядає повідомлення про надмірні документарні вимоги, скеровані Оператором Мінцифри, та надає позицію, пояснення, нормативне обґрунтування або пропозиції щодо усунення відповідної вимоги в межах компетенції.

Вхід до системи для всіх ролей здійснюється виключно за допомогою інтегрованої системи ID.GOV.UA (КЕП/УЕП).

4.2.1.2 Машина станів електронного звіту (State Machine)

Для усунення конфліктів погодження (deadlocks) Системою онлайн-моніторингу має бути впроваджений жорсткий життєвий цикл звітів із такими статусами:

1. **Чернетка (Draft):** Звіт редагується Оператором ЦНАП/СНАП. Доступний для читання/запису лише автору.
2. **На перевірці (Pending Review):** Після накладання КЕП звіт переходить до Оператора ОДА (для ЦНАП) або ЦОВВ (для СНАП). Для автора звіт переходить у режим read-only.
3. **Повернуто на доопрацювання (Returned):** Оператор ОДА/ЦОВВ/Мінцифри повертає звіт. Система онлайн-моніторингу вимагає обов'язкового введення коментаря (причини). Звіт повертається автору зі створенням нової версії.
4. **Погоджено локально (Approved Locally):** Оператор ОДА або ЦОВВ затвердив звіт. Дані стають доступними для агрегації на рівні Мінцифри.
5. **Опубліковано (Published / Locked):** Фінальний статус. Звіт заблокований для будь-яких змін (immutable state). Дані передаються у відкриті реєстри, на дашборди та Платформу центрів Дія. Після переходу у статус Published звіт є незмінним на рівні його змісту. Повторна передача або технічна реплікація даних у разі збоїв інтеграцій не вважається зміною звіту та не впливає на його версію.

4.2.1.3 Версійність та збереження історії змін звіту

Будь-яка зміна поданого звіту здійснюється виключно шляхом створення нової версії звіту з присвоєнням унікального `version_id`. Система онлайн-моніторингу повинна забезпечувати повну історичність змін із можливістю перегляду попередніх версій у режимі `read-only`.

Збереження історії: Система онлайн-моніторингу повинна зберігати всі попередні версії звітів із фіксацією дати, часу, автора змін та коментаря щодо причини повернення.

При повторній подачі доопрацьованого звіту Система онлайн-моніторингу повинна автоматично генерувати загальний агрегований звіт із врахуванням уточнених показників.

4.2.2. Зміни у довідниках

Для забезпечення формування коректної звітності Система онлайн-моніторингу повинна передбачати модернізацію існуючих та створення нових довідників на основі даних Реєстру адміністративних послуг.

4.2.2.1 Довідники адміністративних послуг

Довідники повинні містити структуровану інформацію: тематична група, категорія, назва послуги з ідентифікатором (із забезпеченням можливості множинного вибору послуг).

Каталог місцевих сервісів (локальних послуг): Система онлайн-моніторингу повинна передбачати можливість внесення Оператором ЦНАП **інформації про локальні сервіси/послуги органів місцевого самоврядування**, що відсутні у Реєстрі адміністративних послуг, **виключно для цілей моніторингу, аналітики та класифікації**.

Структура запису в репозиторії місцевих послуг має містити: область; населений пункт; назву ЦНАП; IDF ЦНАП; назву послуги; тематичну групу; категорію; коротку інформацію про послугу.

Інформація про обрані послуги повинна відображатися у звіті «Адміністративні послуги» та у профілі відповідного ЦНАП, ТП або ВРМ.

Внесення записів до репозиторію місцевих послуг здійснюється виключно для цілей моніторингу та аналітики. Таке внесення не є створенням або затвердженням нової адміністративної послуги та не змінює Реєстр адміністративних послуг.

IDF ЦНАП є незмінним (`immutable`) технічним ідентифікатором, що присвоюється об'єкту під час його створення у Системі онлайн-моніторингу та використовується для інтеграційної взаємодії із зовнішніми системами. Зміна IDF не допускається протягом усього життєвого циклу об'єкта.

Аналіз подібності (Дедуплікація): Для реалізації функціоналу визначення подібності та об'єднання місцевих послуг, архітектура Системи повинна передбачати використання повнотекстових пошукових рушіїв (наприклад, `Elasticsearch`) та/або алгоритмів обробки природної мови (`NLP`).

Процес об'єднання ідентичних послуг має здійснюватися виключно після підтвердження Оператором Мінцифри або ЦОВВ. Система онлайн-моніторингу повинна забезпечувати збереження повної історії змін (видалення, об'єднання) із фіксацією дати, часу та ідентифікатора користувача, який вносив правки.

4.2.2.2 Адресні довідники та геокодування

Модернізація адресних довідників Системи онлайн-моніторингу має бути здійснена з обов'язковим переходом на актуальний Кодифікатор адміністративно-територіальних одиниць та територій територіальних громад (КАТОТТГ). Використання застарілого класифікатора КОАТУУ в нових та модифікованих модулях забороняється. Для історичних даних має бути передбачена таблиця відповідності (мапінгу).

4.2.2.3 Дані про чисельність населення та автоматична категоризація ЦНАП

Система онлайн-моніторингу повинна передбачати інтеграцію з даними Держстату через API для автоматичного оновлення довідника чисельності населення територіальних громад.

У разі недоступності API Держстату, має бути передбачена можливість ручного внесення даних адміністратором (із позначкою «override» та фіксацією автора змін).

На основі даних про чисельність населення територіальної громади Система онлайн-моніторингу повинна автоматично визначати категорію фронт-офісу для каталогів ЦНАП та СНАП:

- 1 категорія — 100 тис. осіб і більше;
- 2 категорія — від 50 до 100 тис. осіб;
- 3 категорія — від 20 до 50 тис. осіб;
- 4 категорія — від 10 до 20 тис. осіб;
- 5 категорія — від 5 до 10 тис. осіб;
- 6 категорія — менше 5 тис. осіб.

4.2.3. Конфігурація звітності

Для динамічного управління структурою статичних звітів у Системі онлайн-моніторингу має бути реалізований модуль «Конфігуратор звітів».

4.2.3.1 Функціональні вимоги до Конфігуратора

Модуль повинен забезпечувати користувачу з роллю «Оператор Мінцифри» можливості: створювати нові екземпляри або версії існуючих звітів; редагувати структуру звіту та вкладок; додавати/видаляти питання; налаштовувати контроль доступу; публікувати нові версії звітів із системою автоматичного сповіщення користувачів.

Конфігуратор повинен забезпечувати можливість налаштування показників доступності, безбар'єрності та облаштування ЦНАП, ТП та ВРМ, зокрема визначення групи показника, типу даних, одиниці вимірювання, нормативного або рекомендованого значення, правила попередньої автоматичної валідації, обов'язковості заповнення, необхідності фотопідтвердження та посилання на відповідне нормативне джерело або погоджену Замовником структуру показників.

Структура таких показників не повинна бути жорстко закодована у програмному коді Системи онлайн-моніторингу. Додавання, редагування, деактивація показників, зміна типів даних, правил валідації, нормативних або рекомендованих значень та ознаки необхідності фотопідтвердження повинні здійснюватися через Конфігуратор без необхідності внесення змін до програмного коду.

Зміни, внесені в конфігураторі, повинні автоматично відображатися в шаблонах форм, модулях валідації (недопущення подачі застарілих версій) та модулях експорту. Поля,

створені у попередніх звітних періодах, повинні зберігати свої значення та бути доступними для вивантаження.

4.2.3.2 Архітектурні обмеження збереження даних

Зберігання динамічних структур звітів, створених через Конфігуратор, повинно реалізовуватися виключно з використанням нереляційних типів даних СУБД PostgreSQL (формат JSONB).

Застосування патерну EAV (Entity-Attribute-Value) або динамічної генерації DDL-запитів (ALTER TABLE) для створення нових таблиць або стовпців під кожен новий звіт суворо забороняється через ризики порушення цілісності бази даних.

4.2.3.3 Юридична значущість та електронний підпис

Завершуючи роботу з формою, Оператор засвідчує звіт за допомогою кваліфікованого електронного підпису (КЕП) або удосконаленого електронного підпису (УЕП).

Оскільки форма звіту є динамічною, Система онлайн-моніторингу повинна передбачати механізм детермінованої серіалізації: перед накладанням підпису має автоматично генеруватися незмінна візуальна форма звіту (у форматі PDF/A) або стандартизований JSON-документ. Підпис накладається саме на згенерований файл (хеш файлу), який зберігається Системою онлайн-моніторингу у незмінному вигляді разом з оригінальними метаданими.

4.2.3.4 Експорт даних

Для усіх форм звітності повинна бути реалізована можливість експорту в уніфікованих машиночитаних форматах: XLSX (Office Open XML) та JSON (UTF-8) із версіюванням схеми.

4.2.4. Профілі

В особистому кабінеті Оператора ЦНАП Система онлайн-моніторингу повинна передбачати розділ «Профіль ЦНАП», що складається з двох вкладок: «Відомості про ЦНАП» та «Відомості про ТП та ВРМ». В особистому кабінеті Оператора СНАП передбачається розділ «Профіль СНАП» із вкладкою «Відомості про СНАП».

Профіль ЦНАП, ТП та ВРМ повинен забезпечувати відображення та оновлення відомостей про доступність, безбар'єрність та облаштування відповідного об'єкта у складі атрибутів Реєстру, визначених у пункті 4.2.5.2 цього документа.

Усі поля профілів, що містять контактні дані керівників та відповідальних осіб (ПІБ, контактний номер телефону, персоналізований робочий e-mail), класифікуються як **персональні дані**. Їхня обробка має суворо відповідати вимогам законодавства про захист персональних даних. Система онлайн-моніторингу повинна забезпечувати:

1. **Обмеження доступу:** перегляд цих полів дозволяється виключно авторизованим користувачам з відповідними правами (наприклад, Оператор ОДА, Оператор ЦОВВ, Оператор Мінцифри).

2. **Маскування:** ці дані не підлягають вивантаженню у відкриті дані (data.gov.ua). У разі публічного експорту реєстру або надання доступу через відкриті API, зазначені поля повинні бути повністю виключені або криптографічно замасковані.

4.2.4.1 Відомості про ЦНАП

Система онлайн-моніторингу повинна забезпечувати збір та збереження наступних груп атрибутів (з обов'язковою валідацією на стороні клієнта та сервера):

Основні відомості:

Унікальний ідентифікатор (IDF) (Обов'язкове): Поле недоступне для редагування Оператором ЦНАП; зазначається при створенні запису Оператором ОДА або Мінцифри. Реалізується через пошук із валідацією для існуючих ЦНАП.

Назва (найменування) центру та Скорочена назва (Обов'язкові).

Наявність пов'язаного підрозділу (ТП, ВРМ) та його IDF: Забезпечення зв'язку Parent–Child у базі даних.

Тип ЦНАП (Обов'язкове): Вибір із переліку (ЦНАП, ТП, ВРМ СТ, ВРМ МЦ, ВРМ МА, староста).

Код ЄДРПОУ: Текстове поле з валідацією на ціле число (8 цифр).

Перелік послуг ЦНАП (Обов'язкове): Вибір із Реєстру адміністративних послуг (тематична група, категорія, назва) із можливістю множинного вибору та функціоналом додавання місцевих послуг.

Орган, що утворив ЦНАП, та Тип органу (Обов'язкові): Вибір із переліку (міська рада, селищна рада тощо) та текстова назва ОМС.

Кількість населення громади (Обов'язкове): Значення підтягується через зв'язок із довідником Держстату.

Статус центру (Обов'язкове) та Дати: Вибір із переліку (Діючий, Закритий, Функціонує під час воєнного стану). Поле «Дата закриття центру» стає обов'язковим виключно за умови зміни статусу на «Закритий».

Адреса центру та Геопозиціонування:

- **Класифікатор КАТОТТГ:** Усі ієрархічні списки адрес (Область, Район, Територіальна громада, Населений пункт, Район у місті) повинні формуватися виключно на базі актуального Кодифікатора КАТОТТГ. Використання застарілого КОАТУУ заборонено;
- **Вулиця, Номер будинку, Індекс (Обов'язкові):** Поля з підтримкою пошуку (search/filter list).
- **Координати (Широта, Довгота) (Обов'язкові):** * Система онлайн-моніторингу повинна зберігати координати у системі WGS84 (EPSG:4326) як масив [longitude, latitude]. Валідація значень: longitude $\$in\$ [-180;180]$, latitude $\$in\$ [-90;90]$.
- **Механізм геокодування:** Автоматичне визначення координат виконується через інтеграцію з сертифікованим провайдером геоданих. У разі недоступності API або неможливості автоматичного визначення, Система онлайн-моніторингу повинна переводити запис у статус «Потребує ручного геопозиціонування» (fallback), надаючи Оператору ЦНАП інтерфейс для вибору точки на інтерактивній мапі вручну.

Контактні дані та Стан приміщення:

Час прийому (Обов'язкове): Внесення даних по днях тижня з валідацією формату часу (ГГ:ХВ – ГГ:ХВ);

Контакти для суб'єктів звернення (Обов'язкові): Телефон (із жорсткою валідацією формату +38XXXXXXXXXX), E-mail (стандартна перевірка формату адреси), Адреса вебсайту;

Контактні дані керівника та відповідального за звітність (Обов'язкові): ПІБ, Телефон, Персоналізований робочий e-mail. Ці дані обробляються з урахуванням вимог до персональних даних (див. вище);

Відомості щодо площі (м²) та наявності місць: Числові значення для загальної площі відкритої частини, секторів прийому, інформування, очікування, обслуговування;

Стан приміщення: Вибір одного варіанту (належний стан, зруйноване, пошкоджене та придатне, пошкоджене та непридатне);

Тип розміщення ЦНАП: вибір одного варіанта: окрема будівля; інтегрований офіс / розміщення у приміщенні іншої установи;

Наявність укріття: вибір одного варіанта: так; ні. У разі наявності укріття Система повинна передбачати можливість зазначення його розташування: у будівлі ЦНАП; на прилеглій території; інше найближче доступне укріття;

Інформаційні системи та зворотний зв'язок: Множинний вибір впроваджених інформаційних систем (Вулик, e-ЦНАП, SMART Monitor тощо) та систем електронного документообігу (АСКОД, Megapolis.DocNet тощо). Позначки (Так/Ні) щодо підключення до системи онлайн-моніторингу, наявності QR-коду та смс-розсилок.

4.2.4.2 Територіальні підрозділи та ВРМ

Вкладка «ТП та ВРМ» повинна містити реєстр підрозділів поточного ЦНАП (стовпці: Унікальний ідентифікатор, Тип, Назва, Статус) із функціями додавання, перегляду та редагування.

При створенні нового запису Система онлайн-моніторингу повинна жорстко фіксувати реляційний зв'язок між головним ЦНАП та його структурним підрозділом (ТП) або віддаленим робочим місцем (ВРМ).

Набір реквізитів для ТП та ВРМ є ідентичним до профілю головного ЦНАП (Основні відомості, Адреса за КАТОТТГ, Координати WGS84, Контакти, Площа), з урахуванням динамічної обов'язковості полів залежно від типу підрозділу (наприклад, поля площі та координат є обов'язковими для ТП та ВРМ СТ, але можуть бути необов'язковими для інших типів).

Оператор ЦНАП наділяється правами управління власними ТП та ВРМ, включно з можливістю переведення діючого підрозділу у статус «Закритий».

4.2.4.3 Відомості про СНАП

При створенні нового запису СНАП, Оператор заповнює такі групи полів:

Основні відомості: Код ЄДРПОУ, Повна назва, Скорочена назва, Формат надання послуг (онлайн/офлайн), ЦОВВ, якому підзвітний суб'єкт, Статус СНАП (Діючий, Закритий, Воєнний стан), Дата відкриття/закриття.

Адреса СНАП: Для офлайн СНАП адреса вказується з використанням ієрархічного довідника КАТОТТГ (Область, Район, Громада, Населений пункт, Вулиця, Будинок, Індекс). Для онлайн СНАП вказується посилання (URL).

Перелік послуг СНАП: Вибір із Реєстру адміністративних послуг із можливістю внесення місцевих послуг.

Обслуговування: Щорічна кількість суб'єктів звернення, що обслуговує фронт-офіс (через зв'язок із довідником кількості населення громади).

Контактні дані: Час прийому, адреса вебсайту, контактний номер телефону та e-mail для консультацій суб'єктів звернення.

Персональні дані керівництва: ПІБ, Телефон, Персоналізований робочий e-mail керівника СНАП та уповноваженої особи з питань моніторингу. Ці поля обробляються із застосуванням політик маскування ПД.

4.2.5. Реєстр ЦНАП

Реєстр ЦНАП є агрегованою базою даних, що містить актуальну інформацію про мережу ЦНАП на основі відомостей із профілів та останньої затвердженої звітності.

4.2.5.1 Механізм версійності та оновлення даних

З метою забезпечення аудиту та доступу до історичних даних (вимога до версійності), архітектура Реєстру повинна реалізовувати наступний механізм:

Зберігання даних: Реєстр зберігається як актуальний стан (поточний знімок / snapshot) та журнал усіх подій/змін (event log).

Тригери оновлення: Версія запису в Реєстрі інкрементується автоматично у випадках:

1. Створення нового запису ЦНАП.
2. Редагування полів у профілі ЦНАП, що відображаються в Реєстрі.
3. Перехід нової версії звіту (яка містить поля, що входять до Реєстру) у статус «Опубліковано».

Журнал змін (Event Log): Для кожної зміни Система онлайн-моніторингу повинна фіксувати: timestamp (дату і час), actor_role та actor_id (хто вніс зміну), field_name (назву зміненого реквізиту), old_value (старе значення), new_value (нове значення) та source (джерело: профіль або звіт).

4.2.5.2 Склад атрибутів Реєстру

Реєстр ЦНАП формується з наступних груп реквізитів (згідно з даними профілів та звітів «Показники відповідності офлайн фронт-офісу»):

Службові ідентифікатори: Внутрішній ідентифікатор у системі, IDF головного ЦНАП (для підрозділів), дата створення та дата останньої модифікації запису.

Дані профілю: IDF, Назва, Скорочена назва, Тип ЦНАП, Орган (та тип органу), що утворив ЦНАП, Кількість населення, Статус, Дата відкриття/закриття, використання позначення «Центр Дії», Форма утворення.

Адреса та Контакти: Область, Район, Громада, Населений пункт, Район у місті, Вулиця, Будинок, Індекс (за класифікатором КАТОТТГ); Широта та Довгота (EPSG:4326); вебсайт, контактний телефон та загальна електронна пошта для консультацій.

Показники доступності та облаштування (зі звітів): відомості про стан доступності, безбар'єрності та облаштування ЦНАП, ТП та ВРМ, що формуються з урахуванням показників статичного моніторингу, вимог законодавства щодо доступності для маломобільних груп населення та погодженої Замовником структури показників.

Для таких показників Система онлайн-моніторингу повинна забезпечувати можливість зазначення:

- статусу відповідності;
- опису виявленого бар'єра;
- коментаря відповідальної особи;
- ознаки необхідності фотопідтвердження;
- посилання на відповідне нормативне джерело або погоджену Замовником структуру показників;
- результату попередньої автоматичної валідації.

Автоматична валідація таких показників використовується як технічний механізм попереднього виявлення можливих невідповідностей або бар'єрів. Остаточний статус показника та висновок щодо наявності бар'єра визначаються уповноваженим користувачем

Системи онлайн-моніторингу з урахуванням внесених даних, фотопідтверджень та результатів обстеження.

Система онлайн-моніторингу повинна забезпечувати збереження історії зміни відомостей про доступність, безбар'єрність та облаштування, включаючи дату внесення або оновлення даних, користувача, який вніс зміни, попереднє та актуальне значення показника, а також результати перевірки або модерації фотопідтверджень.

Відомості про доступність, безбар'єрність та облаштування повинні використовуватися для:

- відображення актуального стану доступності у профілі та Реєстрі ЦНАП, ТП або ВРМ;
- формування аналітичних дашбордів за показниками доступності;
- порівняння стану доступності між ЦНАП, ТП та ВРМ;
- підготовки агрегованих звітів щодо наявності бар'єрів та потреби в їх усуненні;
- формування наборів відкритих даних у частині, що не містить персональних даних та інформації з обмеженим доступом.

Послуги: Перелік послуг, що надаються у ЦНАП.

4.2.6. Експорт реєстру ЦНАП

Система онлайн-моніторингу повинна забезпечувати механізми вивантаження даних Реєстру ЦНАП для публічного доступу та інтеграції із зовнішніми інформаційними ресурсами.

4.2.6.1 Формати експорту

Експорт табличних даних через вебінтерфейс публічного розділу порталу має здійснюватися у форматі **XLSX** (Office Open XML).

Машиночитаний експорт та доступ через API має надаватися у форматі **JSON (UTF-8)** із фіксованою та версійованою схемою (наприклад, включення атрибута `schema_version`).

4.2.6.2 Обмеження доступу та маскування даних (White-list підхід)

Для запобігання витоку інформації з обмеженим доступом, розробка функціоналу експорту та публічного API повинна підпорядковуватися наступним правилам:

Білий список полів: Публічне API та модулі експорту надають доступ *виключно* до заздалегідь визначеного «білого списку» (white-list) полів Реєстру ЦНАП.

Заборона експорту ПД: Будь-які атрибути, що містять персональні дані (наприклад, ПІБ, прямі контактні номери телефонів та персоналізовані e-mail керівників або адміністраторів), повинні бути жорстко виключені з публічного експорту та відповідей публічного API. Формулювання вимог на кшталт «усі можливі публічні дані» не допускається.

Доступ до історичних даних: Публічне API повинно підтримувати запити на отримання стану Реєстру на певну дату (наприклад, параметризація запиту **GET /registry/cnap/{idf}?as_of=<timestamp>**).

4.2.7. Звітність для побудови рейтингу

У рамках модернізації підсистеми звітності **необхідно забезпечити** можливість збору, валідації та агрегації даних для проведення статичного, динамічного моніторингу та оцінки рівня задоволеності суб'єктів звернення. Для розрахунку рейтингів якості надання

адміністративних послуг Система онлайн-моніторингу **повинна підтримувати** роздільний збір показників залежно від типу фронт-офісу (онлайн/офлайн).

Усі наведені нижче форми звітів **мають бути реалізовані** за допомогою підсистеми «Конфігуратор звітів» (див. п. 4.2.3).

4.2.7.1 Вимоги до форми звіту «Показники відповідності офлайн фронт-офісу»

Має бути передбачена можливість подання даного звіту Операторами ЦНАП (в т.ч. за ТП та ВРМ) та офлайн СНАП у розрізі конкретного фронт-офісу та звітного періоду. Структура звіту **повинна містити** наступні атрибути (усі поля повинні мати логічний тип даних «Так/Ні», якщо не зазначено інше):

Блок «Облаштування»:

- Необхідно реалізувати поля для фіксації наявності: автоматизованої системи керування чергою; місця для бланків заяв; сервісу оплати (POS-термінал, ПТКС, відділення банку); супутніх послуг (вільний Wi-Fi, оплата комуналки, правова допомога, місця для самообслуговування).
- Повинна фіксуватися можливість попереднього запису: телефоном, особисто, через вебсайт, чат-бот.
- Повинні фіксуватися канали зворотного зв'язку (книга відгуків, скринька, онлайн-опитування) та інформування (стенд, термінал, вебсайт, телефон, картки, зразки заповнення).

Блок «Доступність»:

- Необхідно реалізувати поля для оцінки інфраструктури: наявність зупинок (до 250 м), безоплатної стоянки (загальної та для осіб з інвалідністю), безперешкодного доступу, пандусу/підйомача, санітарної кімнати (в т.ч. обладнаної для осіб з інвалідністю), місць для колясок, ігрового простору, необхідної кількості працівників.
- Повинні фіксуватися засоби орієнтування: шрифт Брайля, технічні рішення для осіб з порушенням слуху, залучення перекладача жестової мови.

Блок «Рівень обслуговування»:

- Необхідно реалізувати поля: розподіл за принципом прийому/видачі, наявність сектору прийому.
- Повинні фіксуватися канали консультацій (телефон, онлайн, e-mail, чат-бот) та способи інформування про хід розгляду (телефон, смс, чат-бот, онлайн).

Блок «Організаційне забезпечення»:

- Мають бути поля щодо доступу до національних електронних ресурсів, наявності СЕД, наявності ІС для автоматизації послуг та проведення заходів з підвищення кваліфікації.

4.2.7.2 Вимоги до форми звіту «Показники відповідності онлайн фронт-офісу»

Для онлайн СНАП **має бути налаштований** окремий шаблон звіту. Структура звіту **повинна містити** атрибути (тип полів: «Так/Ні»):

Блок «Облаштування»: Наявність ≥ 3 варіантів авторизації, двофакторної автентифікації, розширеного пошуку послуг, адаптації сайту (ПК/смартфон/планшет), зворотного зв'язку (телефон/e-mail/чат-бот), онлайн-опитування, сервісу онлайн-оплати, комплексної системи захисту інформації.

Блок «Доступність»: Доступність повної інформації, інклюзивність сайту (для осіб з інвалідністю), наявність підказок, збереження ходу заповнення форми, можливість отримати послугу в автоматичному режимі.

Блок «Рівень обслуговування»: Розділ FAQ, служба підтримки (зв'язок до 30 хв), підвищення кваліфікації. Показники автоматизації (складання заяви, підвантаження документів із реєстрів, автоматична перевірка повноти/помилки). Вибір способу інформування, перегляд історії дій, точний опис помилок/відмов.

4.2.7.3 Вимоги до форми звіту «Показники ефективності надання адміністративних послуг»

Має бути реалізована можливість регулярного подання даного звіту Операторами СНАП та ЦНАП. Дані щодо переліку послуг **повинні автоматично заповнюватися** з профілів ЦНАП та СНАП.

Тіло звіту **повинне містити** наступні атрибути:

Своєчасність надання (%): **має розраховуватися** Системою або вводиться (числове значення);

Кількісні показники (числові значення): Послуг надано в строк; Послуг надано з порушенням строку;

Результативність (%): **має розраховуватися** Системою або вводиться (числове значення);

Кількісні показники результатів (числові значення):

- Успішно наданих послуг (рішення про задоволення заяви);
- Наданих відмов.

Загальні показники (числові значення):

- Загальна кількість наданих послуг (без супутніх);
- Кількість наданих послуг за звітний квартал (без накопичення).

4.2.7.4 Вимоги до модернізації доступу та агрегації (RBAC)

У рамках доопрацювання рольової моделі під час роботи зі звітами **повинні бути реалізовані** наступні права доступу:

Оператор ОДА: повинен мати можливість відслідковувати всі подані ЦНАП звіти, переглядати агреговану статистику за своєю областю та вносити зміни до звітів ЦНАП.

Оператор ЦОВВ: повинен мати можливість відслідковувати подані СНАП звіти, переглядати агреговану статистику (на основі атрибута «ЦОВВ, якому підзвітний суб'єкт») та вносити зміни до звітів СНАП.

Оператор Мінцифри: повинен мати можливість відслідковувати всі подані звіти (ЦНАП, СНАП, ЦОВВ) у розрізі послуги/території/ролі/періоду/джерела даних.

Механізм сповіщень: У разі внесення змін до звітів Оператором ОДА або ЦОВВ, Система онлайн-моніторингу **повинна забезпечувати** автоматичне відображення відповідного сповіщення у кабінеті користувача, чий звіт було відредаговано.

4.2.8. Додаткова звітність

У рамках виконання робіт **необхідно передбачити** можливість збору додаткових даних, що характеризують функціонування мережі ЦНАП (кадрове забезпечення, інтеграція з реєстрами та наявність обладнання). Усі наведені нижче форми звітів **мають бути налаштовані** як базові шаблони за допомогою модуля «Конфігуратор звітів».

4.2.8.1 Вимоги до форми «Звіт за наявними інформаційними системами»

Має бути реалізована можливість регулярного подання даного звіту Операторами ЦНАП (у тому числі за підпорядковані ТП та ВРМ) у розрізі конкретного фронт-офісу та звітного періоду.

Структура звіту **повинна містити** наступні групи атрибутів:

1. Інформація про підключення до державних реєстрів та інформаційних ресурсів:

Необхідно реалізувати обов'язкові поля з логічним типом даних (Boolean: Так/Ні) щодо наявності підключення робочих місць адміністраторів до:

- ЄДР (юридичних осіб, ФОП та громадських формувань);
- Єдиної інформаційної системи соціальної сфери (ЄІССС);
- Електронного кабінету ЦНАП на вебпорталі ПФУ;
- Державного реєстру речових прав на нерухоме майно;
- Єдиного державного демографічного реєстру (ЄДДР);
- Державного земельного кадастру (ДЗК);
- Державного реєстру актів цивільного стану (ДРАЦС);
- Реєстру територіальної громади (через програмні засоби на сайті ДМС);
- Реєстру територіальної громади (засобами власної відомчої ІС);
- Реєстру пошкодженого та знищеного майна;
- Єдиної державної електронної системи у сфері будівництва (ЄДЕССБ);
- Інтегрованої ІС «Соціальна громада»;
- Єдиної інформаційної системи МВС;
- Реєстру застрахованих осіб;
- Єдиного державного вебпорталу електронних послуг (Портал Дія).

2. Деталізація відомчих систем:

Має бути передбачене текстове поле (String, необов'язкове) «Назва відомчої інформаційної системи реєстру територіальної громади (найменування розробника)», яке стає активним у разі вибору відповідного варіанту в попередньому блоці.

3. Додаткові відомості (Обладнання):

Необхідно реалізувати поля з числовим типом даних (Integer, цілі числа ≥ 0) для фіксації кількості:

- наявних станцій паспортного обладнання;
- станцій, підключених до ЄДДР;
- принтерів SwiftPro для видачі посвідчень водія та реєстрації ТЗ;
- станцій, підключених до ЄДР ТЗ.

4.2.8.2 Вимоги до форми «Звіт за працівниками»

Має бути реалізована можливість регулярного подання даного звіту Операторами ЦНАП (у тому числі за підпорядковані ТП та ВРМ).

Структура звіту **повинна передбачати** збір наступних показників (усі поля є обов'язковими для заповнення):

Загальна кількість працівників: Поля з числовим типом даних (Integer) «Всього за штатним розписом» та «Всього фактично».

Відомості щодо фактично працюючих співробітників ЦНАП: Поля (Integer) для фіксації кількості призначених адміністраторів та призначених державних реєстраторів.

Відомості щодо інших працівників, розміщених у центрі: Поля (Integer) для фіксації кількості: державних реєстраторів бізнесу; державних реєстраторів прав на нерухоме майно; державних кадастрових реєстраторів; працівників територіального органу МВС; спеціалістів з питань соціального захисту; спеціалістів з питань пенсійного забезпечення.

Фінансові показники: Поле з числовим типом даних (Numeric/Float) для вводу значення «Середньомісячна заробітна плата адміністратора».

4.2.8.3 Правила доступу, агрегації та редагування додаткової звітності (RBAC)

Під час опрацювання додаткової звітності Система онлайн-моніторингу **повинна забезпечувати** наступну матрицю доступів:

Оператор ОДА: повинен мати права на перегляд усіх звітів ЦНАП своєї області, перегляд агрегованої статистики та внесення змін до таких звітів. **Обов'язкова вимога:** у разі внесення змін до звіту Оператором ОДА, Система онлайн-моніторингу повинна застосовувати механізм версійності (збереження Audit Trail) та автоматично генерувати сповіщення в кабінеті користувача, чий звіт було відредаговано.

Оператор ОМС (Органу місцевого самоврядування): повинен мати права виключно на читання (Read-only) усіх поданих ЦНАП звітів у межах своєї адміністративно-територіальної одиниці (громади).

Оператор Мінцифри: повинен мати наскрізні права на перегляд та агрегацію всіх поданих звітів у розрізі територій, періодів та джерел даних.

4.2.8.4 Вимоги до форми «Звіт за послугами»

Має бути реалізована можливість регулярного подання даного звіту Операторами ЦНАП (в т.ч. за ТП та ВРМ) та Операторами СНАП у розрізі конкретного фронт-офісу.

Структура звіту **повинна містити** наступні обов'язкові атрибути (усі поля мають числовий формат даних Integer, ≥ 0):

- **Загальна кількість адміністративних послуг, запроваджених через центр:** Дане поле **повинно заповнюватися автоматично** (Pre-fill) на основі інформації з Профілю установи (без можливості ручного редагування).
- **Послуги за суб'єктами надання:** Поля для вводу кількості послуг обласної державної адміністрації та міської/селищної/сільської ради.
- **Послуги за Переліком №523:** Дане поле **повинно розраховуватися автоматично** Системою на основі даних з довідника (Реєстру) адміністративних послуг, обраних у Профілі.
- **Кількісні показники за назвами послуг:** Динамічний перелік полів для вводу кількості наданих послуг, який **повинен автоматично генеруватися** відповідно до переліку послуг, обраного Оператором у Профілі установи.

4.2.9. Валідація звітності

Для мінімізації ризику помилок під час внесення звітних даних, підсистема звітності **повинна відповідати** наступним вимогам до валідації та користувацького інтерфейсу:

- **Порівняння історичних даних (Diffing):** Під час заповнення форм звітів Система онлайн-моніторингу **повинна автоматично** проводити порівняння введених актуальних показників із показниками за попередній аналогічний звітний період. У разі виявлення відхилень Система онлайн-моніторингу **повинна привертати увагу** користувача (наприклад, шляхом зміни кольору комірки чи тексту на попереджувальний, або за допомогою відображення спеціального інформаційного повідомлення/модального вікна).

- **Валідація в режимі реального часу (Real-time validation):** Перевірка введених даних має відбуватися динамічно (на льоту) безпосередньо під час заповнення відповідних форм.
- **Контроль форматів:** Система онлайн-моніторингу повинна жорстко перевіряти правильність введених даних на відповідність заданим правилам (числові обмеження, неможливість введення від'ємних значень, перевірка формату дат, електронних адрес тощо).

4.2.10. Контроль термінів подачі звітності

Для забезпечення своєчасності подачі звітів суб'єктами надання послуг та центрами надання послуг, а також їх своєчасного погодження ОДА та ЦОВВ, у Системі онлайн-моніторингу **необхідно впровадити** автоматизовану підсистему сповіщень (на базі планувальника завдань).

- **Автоматичні нагадування до дедлайну:** Якщо за 7 календарних днів до встановленого дедлайну звіт ще не був поданий або погоджений, Система онлайн-моніторингу має **автоматично генерувати та відправляти** нагадування в особисті кабінети користувачів відповідних організацій. Додатково це нагадування **повинно автоматично надсилатися** на контактну електронну адресу, зазначену у профілі організації.
- **Ескалація затримок погодження:** При виникненні затримки у погодженні вже поданого звіту, Система онлайн-моніторингу **повинна автоматично надсилати** відповідне сповіщення про цю затримку Операторам ОДА та ЦОВВ.

4.2.11. Модифікація реєстру ЦНАП

У рамках модернізації **необхідно забезпечити** механізм динамічного оновлення Реєстру ЦНАП відразу після отримання (затвердження) нових версій звітів.

- **Геопозиціонування:** У структурі Реєстру, окрім існуючих даних, **слід передбачити** додаткові атрибути для запису геокоординат ЦНАП: широти та довготи (у форматі WGS84). Ці поля **повинні бути доступні** для ручного редагування виключно користувачу з роллю «Оператор (Адміністратор) Мінцифри».
- **Автоматичне геокодування:** При первинному заповненні Реєстру Система онлайн-моніторингу **повинна забезпечувати** автоматичний запис геокоординат на основі введеної текстової адреси ЦНАП (через інтеграцію з геоінформаційними сервісами, наприклад, Google Geocoding API).
- **Журнал змін (Audit Trail):** Форма детального перегляду інформації про конкретний ЦНАП **повинна містити** додаткову вкладку або розділ «Історія змін», що буде надійно зберігати інформацію про всі модифікації профілю даного ЦНАП. У цьому розділі для кожної зміни **мають обов'язково відображатися:**
 - Дата та час кожної зміни;
 - Найменування реквізиту (поля), що було змінено;
 - Значення реквізиту до зміни (старі значення);
 - Значення реквізиту після зміни (нове значення).
- **Синхронізація зі звітами:** Дані у розділі історії змін **мають автоматично доповнюватися** кожного разу, коли надходить нова затверджена версія звіту. Система онлайн-моніторингу **повинна порівнювати** новий звіт із попереднім

за кожним параметром та автоматично фіксувати (логувати) всі виявлені зміни до Реєстру.

4.2.12 Розробка API для інтеграції з Платформою центрів Дії

Необхідно забезпечити автоматичну передачу із системи онлайн-моніторингу Порталу Дія до Платформи Центрів Дія наступних даних:

- Оціночні дані щодо ЦНАП:
- Дані про ЦНАП, територіальні підрозділи та віддалені робочі місця.
- Інформація для модулів інтерактивної карти ЦНАП <https://center.diiia.gov.ua/mapa-centriv-so-pracuut-pid-cas-vijni-2>.
- Дані для попереднього запису громадян та дистанційного навчання через Платформу Центрів Дія.
- Звітність про моніторинг якості послуг:
- Узагальнена звітність Мінцифри про якість послуг для публікації на Платформі Центрів Дія.
- Дані для інформаційної панелі (дашборду) відповідно до Порядку проведення моніторингу, затвердженого постановою КМУ № 864 від 11.08.2021.
- Інформація про рейтинг. Рейтингові дані суб'єктів та центрів надання адміністративних послуг.

Відомості, що мають бути передані систематично та в автоматичному режимі до Платформи Центрів Дія для функціонування інтерактивної карти ЦНАП в рамках інформаційної взаємодії відповідно до Таблиці 1:

Таблиця 1
Структура даних для інтерактивної карти ЦНАП

№	Назва поля (атрибут)	Опис
1	IDF	Унікальний ідентифікатор
2	ADMIN_1	Область
3	ADMIN_2	Район
4	ADMIN_3	Громада
5	type_NP	Тип населеного пункту
6	name_NP	Назва населеного пункту
7	mother_unit	Батьківський ЦНАП
8	title	Назва у форматі JSON
9	full_name	Назва
10	name	Скорочена назва

№	Назва поля (атрибут)	Опис
11	coordinates	array geometry [x,y]
12	status	Статус
13	type	Тип ЦНАП (ЦНАП, ТП, ВРМ, Дія.Центр)
14	adress	Населений пункт, вулиця, номер будинку
15	web	Адреса вебсайту центру або спеціалізованої вебсторінки центру на сайті органу, що утворив центр
16	bus_100	Наявність зупинок громадського транспорту в радіусі 2500 м. (так/ні)
17	free_parking	Наявність безоплатної стоянки автотранспорту (так/ні)
18	free_entry	Вільний (безперешкодний) доступ до приміщення
19	timetable	Час прийому суб'єктів звернень (з год:хв – до год:хв в розрізі днів)
20	contrast_step	Наявність маркування сходового маршу (перша та остання сходинка промарковані контрастною фарбою)
21	audio_entrance	Вхід до будівлі облаштований аудіопоказчиком (звуковим маячком–сигналізатором)
22	highcontrast_sign	Вхід до будівлі облаштований інформаційною табличкою, виконаною збільшеним шрифтом та у контрастному співвідношенні кольору шрифту відносно фону таблички
23	highvisibility_labe	Інформаційні таблички у приміщенні (напрямки руху, номери робочих місць, назви секторів) виконані збільшеним шрифтом та у контрастному співвідношенні кольору шрифту відносно фону таблички
24	serv_list	Перелік доступних послуг
25	contact	Забезпечення можливості надання суб'єктам звернень за допомогою засобів телекомунікації (телефон, електронна пошта)
26	tel_consul	Консультування телефоном (так/ні)
27	onl_consul	Онлайн–консультування (так/ні)

№	Назва поля (атрибут)	Опис
28	e_registr	Здійснення попереднього запису на прийом (так/ні)
29	bank_branch	Наявність у ЦНАП відділення банку (так/ні)
30	pay_card	Оплата послуг банківською картою (так/ні)
31	pay_terminal	Оплата послуг через платіжний термінал
32	add_serv	Додаткові послуги:
33	free_wifi	Вільний WI-FI (так/ні)
34	self_serv	Місця для самообслуговування (так/ні)
35	sanit_room	Наявність санітарної кімнати у центрі (так/ні)
36	disability	Забезпечення умов для перебування та обслуговування в центрі осіб з інвалідністю та інших маломобільних груп населення (так/ні)
37	pandus	Пандус та сходи з поручнями (так/ні)
38	dis_sanit	Обладнана санітарна кімната (так/ні)
39	braille_ma	Матеріали надруковані шрифтом Брайля (так/ні)
40	deaf_serv	Обслуговування осіб з порушенням слуху (так/ні)
41	pram_place	Місце для тимчасового розміщення дитячих колясок (так/ні)
42	kids_room	Наявність дитячої кімнати/дитячого куточка
43	diia_help	Надання консультацій щодо користування мобільним додатком Дія та Порталом Дія (так/ні)
44	feedback	Посилання на форму зворотнього зв'язку

Необхідно систематично та автоматично передавати до системи попереднього запису через Платформу Центрів Дія наступну інформацію:

Оціночні та додаткові дані про:

- Основні ЦНАП.
- Територіальні підрозділи ЦНАП.
- Віддалені та пересувні робочі місця адміністраторів.

Додаткові специфікації щодо обсягу необхідних даних будуть надані під час етапу розробки.

Необхідно забезпечити автоматизований обмін відомостями, згаданими в пункті 1, через прикладні програмні інтерфейси. Обмін відбувається між Порталом Дія, Платформою

Центрів Дія та системою запису до ЦНАП. При цьому слід використовувати засоби технічного та криптографічного захисту, відповідно до вимог законодавства про захист інформації.

4.2.13. Розробка API для імпорту відомостей до Системи онлайн-моніторингу

Модифікувати API динамічного моніторингу, додавши ідентифікатори для СНАП на основі provider, code, provider type

Для методу GET – запит на отримання даних, доопрацювати harvester (планувальник) та у кабінеті адміністратора запровадити інтерфейс з налаштуваннями розкладу звернень по API, до систем, підключених за таким методом.

Для методу POST – запит на додавання даних до системи, доопрацювати API репозиторія динамічного моніторингу для можливості підключення нових та конфігурації параметрів діючих он-лайн систем в кабінеті адміністратора.

Розробити та надати API для обміну даними між Системою онлайн-моніторингу та інформаційними системами ЦНАП, СНАП та ЦОВВ, з метою автоматичного оновлення інформації по показникам моніторингу.

Доопрацювати систему динамічного моніторингу з питання створення релевантних зв'язків між даними репозиторію наданих послуг з реєстрами ЦНАП та адміністративних послуг, модулями звітності та оцінки якості, а також довідниками. Передбачити версійність, та варіативність інформації.

В рамках взаємодії з ЦНАП в частині динамічного моніторингу, розробити API для імпорту та регулярного оновлення відомостей про перелік послуг, що надаються кожним конкретним ЦНАПом ТП та ВРМ, СНАП. Унікальні ідентифікатори послуг визначені у реєстрі.

Забезпечити підтримку роботи сервера Slave та доступу до нього з правами читання аналітичних систем та інших сторонніх систем даними репозиторію наданих послуг, реєстрів ЦНАП та адміністративних послуг, модулями звітності та оцінки якості, а також довідниками.

Розмістити документацію щодо використання API у розділі «Інформація для розробників».

4.2.14. Розробка API для експорту відомостей щодо показників ЦНАП

Розробити набір API для експорту відомостей щодо будь-яких показників ЦНАП, СНАП та послуг, які в них надаються, в тому числі публічне API для вивантаження в машиночитаному форматі всіх можливих публічних даних.

4.2.15. Створення статичного звіту з переліком послуг, що надаються у ЦНАП

У Системі онлайн-моніторингу має бути розроблена окрема форма статичного звіту, що містить вичерпний перелік послуг, які фактично надаються кожним конкретним ЦНАП.

4.2.15.1 Архітектура та інтеграція

- **Маппінг ідентифікаторів:** Звіт повинен будуватися на основі жорсткого реляційного зв'язку (маппінгу) унікального ідентифікатора ЦНАП (id ЦНАП) та унікального ідентифікатора адміністративної послуги (id послуги).

- **Джерело даних:** Для забезпечення консистентності даних, ід послуги повинен синхронізуватися (інтегруватися) з еталонним довідником програмного засобу «Гід з державних послуг» (Реєстром адміністративних послуг).
- **API звіту:** **Необхідно розробити** окремий API-ендпоінт для отримання даних цього маппінгу зовнішніми системами.

4.2.15.2 Валідація та Інтерфейс (UI)

- **Контроль цілісності:** Під час формування маппінгу Система онлайн-моніторингу **повинна перевіряти** наявність обов'язкових полів, правильність формату ID та забезпечувати унікальність комбінації id ЦНАП – id послуги (уникнення дублікатів).
- **UI/UX:** Інтерфейс користувача **повинен містити** функціонал швидкого пошуку та фільтрації за id ЦНАП або id послуги.
- **Експорт:** **Має бути реалізована** функція вивантаження результатів звіту у табличних форматах (CSV, XLSX).

4.2.16. Функціонал подачі заяви на підключення до Системи онлайн-моніторингу (Онбординг)

Для забезпечення безпечного та автоматизованого процесу надання доступу новим суб'єктам, Система онлайн-моніторингу **повинна містити** модуль електронного онбордингу.

- **Аутентифікація:** Вхід до форми подачі заяви **повинен здійснюватися виключно** з використанням сервісу ID.GOV.UA (за допомогою Кваліфікованого або Удосконаленого електронного підпису – КЕП/УЕП).
- **Електронна форма:** Після успішної аутентифікації користувачу **має відкриватися** електронна форма заяви на підключення. Дані про підписанта (ПІБ, РНОКПП/ЄДРПОУ організації) **повинні підтягуватися автоматично** з сертифіката ключа.
- **Життєвий цикл заяви:** 1. Автоматична первинна валідація введених даних Системою. 2. Передача заяви до кабінету Оператора Мінцифри для ручної верифікації та підтвердження повноважень. 3. Після підтвердження – автоматичне створення облікового запису з відповідною рольовою моделлю та надсилання сповіщення користувачу.

4.2.17. Розробка функціоналу відкритих даних

Для виконання вимог Закону України «Про доступ до публічної інформації» та Постанови КМУ № 835 від 21.10.2015 р., у Системі онлайн-моніторингу **необхідно реалізувати** підсистему формування та оприлюднення наборів відкритих даних на основі інформації з баз даних/реєстрів ІКС.

- **Знеособлення (Анонімізація) даних:** Перед формуванням публічних наборів Система онлайн-моніторингу **повинна автоматично** вилучати або криптографічно маскувати будь-яку інформацію з обмеженим доступом та персональні дані (наприклад, контактні номери телефонів, ПІБ керівників, персональні e-mail адреси), дотримуючись політики «білого списку» атрибутів.

- **Формати файлів:** Набори відкритих даних мають генеруватися у структурованих машиночитаних форматах (пріоритетно JSON, CSV), визначених п. 9 Постанови КМУ № 835.
- **Автоматизація оприлюднення:** Створені набори повинні регулярно оновлюватися за розкладом (cron). Вивантаження на Єдиний державний вебпортал відкритих даних (data.gov.ua) має здійснюватися автоматично через використання відкритого API. У разі неможливості прямої API-інтеграції, повинен бути реалізований механізм генерації статичних файлів в адміністративній панелі Оператора Мінцифри для їх подальшого завантаження.

4.2.18. Функціонал збору фінансової звітності

Підсистема звітності повинна бути розширена функціоналом для збору та аналізу фінансових показників діяльності ЦНАП.

4.2.18.1 Інтеграція з Конфігуратором звітів

- Форми фінансової звітності не повинні бути жорстко закодовані (hardcoded). Оператор Мінцифри повинен мати можливість створювати нові або редагувати існуючі шаблони фінансових звітів виключно через модуль «Конфігуратор звітів» (додавати нові статті витрат/доходів).

4.2.18.2 Структура фінансових показників

Система онлайн-моніторингу повинна підтримувати збір наступних базових груп даних (усі фінансові поля повинні мати числовий тип даних Decimal або Float для підтримки копійок):

- Загальний бюджет ЦНАП.
- Витрати на оплату праці.
- Витрати на утримання приміщення (включно з комунальними послугами).
- Витрати на технічне та програмне забезпечення.
- Доходи від надання платних адміністративних послуг.
- Інші кастомні статті (визначені через Конфігуратор).

4.2.18.3 Аналітика та Валідація

- **Валідація:** Система онлайн-моніторингу повинна здійснювати математичний контроль (наприклад, сума деталізованих витрат не може перевищувати загальний бюджет).
- **Порівняння:** Має бути реалізований автоматичний розрахунок відхилень (динаміки змін) фінансових показників порівняно з попередніми звітними періодами.
- **Експорт та Дашборди:** Агреговані фінансові дані повинні бути інтегровані у загальну підсистему дашбордів (див. п. 4.2.22) для візуалізації ефективності оптимізації витрат, а також доступні для вивантаження через API.

4.2.19. Функціонал семантичного аналізу місцевих послуг

З метою аналізу переліку послуг, що фактично надаються у центрах надання адміністративних послуг, у тому числі місцевих послуг, Система онлайн-моніторингу повинна забезпечувати функціонал семантичного аналізу та виявлення подібності між назвами й описами послуг.

Функціонал повинен забезпечувати:

- аналіз текстових описів послуг;
- визначення ступеня семантичної подібності між послугами;
- виявлення потенційних дублювань або схожих формулювань;
- групування подібних послуг;
- формування рекомендацій щодо уніфікації назв та описів;
- формування рекомендацій щодо зіставлення місцевих послуг із наявними ідентифікаторами послуг для подальшого використання у Гіді державних послуг.

Для реалізації зазначеного функціоналу архітектура Системи онлайн-моніторингу може передбачати використання повнотекстових пошукових рушіїв та інструментів обробки природної мови з урахуванням морфології української мови.

Результати семантичного аналізу повинні відображатися в інтерфейсі Системи онлайн-моніторингу як рекомендації та підлягати обов'язковому розгляду та підтвердженню користувачем з роллю «Оператор Мінцифри».

Присвоєння або підтвердження ідентифікатора послуги здійснюється виключно після прийняття рішення Оператором Мінцифри. Автоматичне присвоєння ідентифікатора без підтвердження уповноваженим користувачем не допускається.

Розроблені механізми семантичного аналізу можуть також використовуватися для виявлення подібних або дублюючих повідомлень про надмірні документарні вимоги відповідно до пункту 4.2.20 цього документа.

4.2.20. Функціонал збору та аналізу повідомлень про надмірні документарні вимоги

В рамках створення КП Система онлайн-моніторингу має бути реалізований додатковий аналітичний функціонал для збору, систематизації, попередньої класифікації та опрацювання повідомлень про надмірні, необґрунтовані, застарілі або дублюючі документарні вимоги, що виникають у процесах надання адміністративних послуг та можуть створювати додаткове навантаження на суб'єктів звернення або адміністраторів ЦНАП.

Зазначений функціонал реалізується як аналітичний модуль Системи онлайн-моніторингу та не є створенням окремого державного реєстру.

Метою функціоналу є виявлення типових або системних випадків витребування документів, довідок, копій, паперових підтверджень або іншої інформації, якщо такі вимоги можуть бути надмірними, необґрунтованими, застарілими, дублюючими або такими, що потребують додаткового аналізу з боку Мінцифри та/або відповідального суб'єкта владних повноважень.

Подання первинного повідомлення

Система онлайн-моніторингу повинна забезпечувати можливість подання первинних повідомлень про надмірні, необґрунтовані, застарілі або дублюючі документарні вимоги виключно Операторами ЦНАП у межах відповідного центру надання адміністративних послуг, його територіальних підрозділів або віддалених робочих місць.

Оператори ЦОВВ та Оператори СНАП не є суб'єктами первинного подання таких повідомлень у межах цього модуля. Їхня роль полягає в опрацюванні повідомлень, скерованих

Оператором Мінцифри, наданні позиції, пояснень, нормативного обґрунтування або пропозицій щодо усунення відповідної документарної вимоги в межах компетенції.

Оператор Мінцифри не є суб'єктом первинного подання повідомлень. Роль Оператора Мінцифри полягає у первинному опрацюванні повідомлення після семантичного аналізу, підтвердженні або зміні попередньої класифікації, присвоєнні статусу, визначенні відповідального ЦОВВ або СНАП та скеруванні повідомлення на опрацювання.

Повідомлення про надмірну документарну вимогу повинно містити щонайменше такі відомості:

- найменування ЦНАП, ТП або ВРМ, від імені якого подається повідомлення;
- назву адміністративної послуги або групи послуг, у межах яких виникає відповідна вимога;
- найменування ЦОВВ, СНАП або іншого суб'єкта, з діяльністю або вимогами якого пов'язане повідомлення, якщо така інформація відома Оператору ЦНАП;
- опис документарної вимоги, яка вважається надмірною, необґрунтованою, застарілою або дублюючою;
- джерело виникнення такої вимоги, якщо воно відоме Оператору ЦНАП;
- опис впливу такої вимоги на процес надання адміністративної послуги або на суб'єкта звернення;
- інформацію про повторюваність випадку, якщо вона відома Оператору ЦНАП;
- можливість додавання файлів, скан-копій, фотографій або інших підтверджувальних матеріалів;
- коментар Оператора ЦНАП;
- дату подання повідомлення;
- статус опрацювання повідомлення.

Семантичний аналіз повідомлення

Після подання повідомлення Оператором ЦНАП Система онлайн-моніторингу повинна здійснювати його попередній автоматизований та/або семантичний аналіз з метою:

- виявлення можливих дублікатів або подібних повідомлень;
- групування типових випадків за послугами, ЦНАП, регіонами, СНАП або ЦОВВ;
- попереднього визначення категорії повідомлення;
- попереднього визначення ймовірного відповідального ЦОВВ, СНАП або іншого суб'єкта, до компетенції якого може належати відповідна документарна вимога;
- формування аналітичної підказки для Оператора Мінцифри.

Попередня класифікація повідомлення може здійснюватися за такими категоріями:

- можливо застаріла документарна вимога;
- можливо необґрунтована документарна вимога;
- можливо надмірна документарна вимога;
- дублююча або подібна вимога;
- вимога, що потребує додаткового аналізу;
- повідомлення, що не належить до предмета опрацювання модуля.

Результати автоматизованого або семантичного аналізу мають попередній аналітичний характер і не є юридично значущим висновком щодо правомірності або неправомірності відповідної документарної вимоги.

Первинне опрацювання Оператором Мінцифри

За результатами семантичного аналізу повідомлення передається на первинне опрацювання Оператору Мінцифри.

Оператор Мінцифри повинен мати можливість:

- переглядати повідомлення та додані до нього матеріали;

- переглядати результати попереднього автоматизованого та семантичного аналізу;
- підтверджувати, змінювати або відхиляти попередню категорію повідомлення;
- об'єднувати дублюючі або подібні повідомлення в типовий випадок;
- визначати відповідальний ЦОВВ, СНАП або інший суб'єкт для подальшого опрацювання;
- присвоювати або змінювати статус повідомлення;
- додавати коментарі щодо результатів первинного опрацювання;
- скеровувати повідомлення на опрацювання відповідальному ЦОВВ або СНАП;
- повертати повідомлення Оператору ЦНАП для уточнення;
- відхиляти повідомлення, якщо воно не належить до предмета опрацювання модуля.

Опрацювання повідомлення відповідальним ЦОВВ або СНАП

Після скерування повідомлення Оператором Мінцифри відповідний Оператор ЦОВВ або Оператор СНАП повинен мати можливість переглянути повідомлення, додані матеріали, результати семантичного аналізу та коментар Оператора Мінцифри.

Оператор ЦОВВ або Оператор СНАП у межах своєї компетенції повинен мати можливість:

- надати позицію щодо відповідної документарної вимоги;
- зазначити нормативне або інше обґрунтування застосування такої вимоги, якщо воно наявне;
- підтвердити наявність проблеми та запропонувати спосіб її усунення;
- зазначити, що вимога не застосовується відповідним суб'єктом або не належить до його компетенції;
- запропонувати перенаправлення повідомлення іншому відповідальному суб'єкту;
- додати підтверджувальні матеріали або пояснення;
- подати відповідь на розгляд Оператора Мінцифри.

Фіналізація статусу повідомлення

Після отримання позиції відповідального ЦОВВ або СНАП Оператор Мінцифри здійснює фінальне опрацювання повідомлення та присвоює йому відповідний статус.

Система онлайн-моніторингу повинна передбачати щонайменше такі статуси опрацювання повідомлення:

- подано;
- на семантичному аналізі;
- потребує уточнення від ЦНАП;
- на первинному опрацюванні Мінцифри;
- скеровано відповідальному ЦОВВ/СНАП;
- на опрацюванні відповідального ЦОВВ/СНАП;
- отримано позицію відповідального ЦОВВ/СНАП;
- підтверджено як типову або системну проблему;
- потребує нормативного або організаційного врегулювання;
- враховано в аналітичних матеріалах;
- відхилено;
- закрито.

Для кожного повідомлення Система онлайн-моніторингу повинна забезпечувати збереження історії зміни статусів, коментарів, результатів попереднього аналізу, скерувань, відповідей відповідальних органів, рішень Оператора Мінцифри та дати відповідних дій.

Аналітика та звітність

Модуль повинен забезпечувати формування аналітичних зведень за такими параметрами:

- кількість повідомлень у розрізі регіонів, громад, ЦНАП, ТП та ВРМ;
- кількість повідомлень у розрізі адміністративних послуг або груп послуг;
- кількість повідомлень у розрізі ЦОВВ, СНАП або інших суб'єктів, яким повідомлення скеровувалися на опрацювання;
- категорії документарних вимог;
- статуси опрацювання повідомлень;
- повторюваність або типовість повідомлень;
- кількість повідомлень, скерованих відповідальним ЦОВВ або СНАП;
- кількість повідомлень, щодо яких отримано позицію відповідального ЦОВВ або СНАП;
- кількість повідомлень, підтверджених як типові або системні проблеми;
- кількість повідомлень, врахованих у підготовлених аналітичних або управлінських матеріалах;
- динаміка повідомлень за звітними періодами.

Аналітичні дані модуля повинні бути доступні для відображення у дашбордах, експорту в машиночитаних форматах та використання під час підготовки управлінських, аналітичних або звітних матеріалів.

Обмеження автоматизованого аналізу

Модуль не повинен забезпечувати автоматичне ухвалення юридично значущих рішень щодо правомірності або неправомірності документарної вимоги.

Будь-які автоматично сформовані висновки, категорії, підказки або рекомендації мають попередній аналітичний характер і підлягають перевірці Оператором Мінцифри.

Функціонал модуля не замінює офіційні процедури перегляду нормативно-правових актів, скасування документарних вимог або внесення змін до порядків надання адміністративних послуг, але може використовуватися для підготовки відповідних аналітичних матеріалів, пропозицій або звернень до компетентних органів.

4.2.21. Функціонал збору фотопідтверджень показників статичного моніторингу

З метою забезпечення проведення моніторингу якості надання адміністративних послуг та підтвердження фактичного стану інфраструктури ЦНАП, ТП/ВРМ та СНАП модернізована Система онлайн-моніторингу повинна підтримувати можливість додавання медіафайлів (фотопідтверджень) як доказових матеріалів до відповідних показників моніторингу.

Фотопідтвердження можуть використовуватися, зокрема, для підтвердження показників доступності, безбар'єрності та облаштування ЦНАП, ТП та ВРМ, що відображаються у профілі та Реєстрі відповідного об'єкта відповідно до розділу 4.2.4 та пункту 4.2.5.2 цього документа.

Зазначений функціонал реалізується з метою підвищення достовірності та перевірюваності інформації, що подається суб'єктами моніторингу у межах проведення моніторингу якості надання адміністративних послуг

4.2.21.1 Завантаження та обробка медіафайлів

Система онлайн-моніторингу повинна забезпечувати можливість завантаження користувачами з ролями Оператор ЦНАП (ТП/ВРМ) та Оператор СНАП фотографій об'єктів інфраструктури або елементів організації надання адміністративних послуг, що підтверджують відповідність визначеним показникам моніторингу.

Завантажені медіафайли повинні автоматично прив'язуватися до:

- відповідного ідентифікатора установи (IDF);
- відповідного показника статичного моніторингу;
- відповідного звіту або профілю установи.

Система онлайн-моніторингу повинна забезпечувати збереження медіафайлів та їх відображення:

- у профілях відповідних установ;
- у формах звітності;
- у модулі перевірки (модерації) даних.

4.2.21.2 Модуль перевірки (модерації) медіаданих

У Системі онлайн-моніторингу повинен бути реалізований функціонал перевірки (модерації) медіафайлів, завантажених користувачами.

Користувачі з роллю Оператор Мінцифри повинні мати можливість:

- переглядати завантажені фотографії;
- підтверджувати або відхиляти їх як доказ виконання відповідного показника;
- додавати коментарі щодо результатів перевірки;
- переглядати історію завантаження та модерації медіаданих.

4.2.21.3 Динамічне управління показниками моніторингу

Перелік показників статичного моніторингу не повинен бути жорстко закодований у програмному коді Системи онлайн-моніторингу.

Оператор Мінцифри повинен мати можливість через адміністративну панель Системи онлайн-моніторингу:

- додавати нові показники моніторингу;
- редагувати або деактивувати існуючі показники;
- визначати необхідність завантаження фотопідтверджень для відповідного показника.

Функціонал фотопідтверджень повинен застосовуватися лише до тих показників, для яких це передбачено налаштуваннями Системи онлайн-моніторингу та підтверджено Оператором Мінцифри.

Усі зміни повинні автоматично застосовуватися у Системі онлайн-моніторингу без необхідності внесення змін до програмного коду.

4.2.22. Функціонал аналітичної візуалізації та формування презентаційних матеріалів

З метою забезпечення керівництва та аналітиків оперативною інформацією за результатами моніторингу якості надання адміністративних послуг модернізована Система онлайн-моніторингу повинна забезпечувати можливість автоматичного формування візуальних, аналітичних та презентаційних матеріалів на основі агрегованих показників моніторингу.

Функціонал повинен забезпечувати побудову графіків, діаграм, таблиць та інших візуальних елементів для аналізу показників моніторингу, а також формування презентаційних матеріалів для подальшого використання у звітності, аналітичних матеріалах та управлінських рішеннях.

4.2.22.1 Візуалізація показників

Система онлайн-моніторингу повинна підтримувати автоматичну генерацію та відображення різних типів графіків та діаграм на основі обраних користувачем наборів даних (dataset), зокрема:

- лінійних графіків;
- стовпчастих діаграм;
- секторних (кругових) діаграм;
- пелюсткових (radar) діаграм;
- табличних представлень агрегованих даних.

Система онлайн-моніторингу повинна забезпечувати можливість налаштування параметрів візуалізації, зокрема:

- кольорової палітри;
- підписів осей;
- відображення значень на графіках;
- розташування легенди.

4.2.22.2 Порівняльна аналітика

Система онлайн-моніторингу повинна забезпечувати можливість порівняльного аналізу показників моніторингу між різними об'єктами спостереження, зокрема:

- між різними ЦНАП;
- між регіонами;
- між категоріями фронт-офісів;
- між різними періодами моніторингу.

Система онлайн-моніторингу повинна забезпечувати візуалізацію змін показників у часі (аналіз часових рядів), що дозволяє відстежувати динаміку показників за кварталами або роками.

4.2.22.3 Інтерактивні дашборди

Система онлайн-моніторингу повинна містити підсистему інтерактивних дашбордів, що забезпечують оперативний перегляд агрегованих показників моніторингу.

Дашборди повинні підтримувати:

- інтерактивні графіки та таблиці;
- фільтрування даних за періодом;
- фільтрування за регіоном;
- фільтрування за типом установи;
- фільтрування за групами показників;
- автоматичне оновлення візуалізацій при зміні параметрів фільтрації.

Дашборди повинні забезпечувати можливість відображення агрегованої інформації за повідомленнями про надмірні документарні вимоги, зокрема за регіонами, громадами, ЦНАП, адміністративними послугами, ЦОВВ/СНАП, категоріями повідомлень та статусами їх опрацювання.

4.2.22.4 Експорт аналітичних матеріалів

Система онлайн-моніторингу повинна забезпечувати можливість експорту згенерованих графіків, таблиць, дашбордів та супровідних текстових описів у презентаційні та документні формати.

Підтримувані формати експорту:

- pptx (Microsoft PowerPoint);
- pdf (Portable Document Format).

Для формату .pptx експорт повинен здійснюватися шляхом генерації нативних об'єктів формату Office Open XML.

Графіки, діаграми та таблиці повинні експортуватися як редаговані елементи PowerPoint (векторні об'єкти та таблиці з вбудованими даними), а не як растрові зображення, що забезпечує можливість подальшого редагування графіків, підписів та значень після експорту.

4.2.22.5 Формування презентацій за шаблонами

Система онлайн-моніторингу повинна забезпечувати можливість автоматичного формування презентаційних матеріалів на основі попередньо визначених шаблонів презентацій.

Шаблони презентацій повинні містити структуру слайдів, визначені місця для графіків, таблиць та текстових описів, які автоматично заповнюються агрегованими даними Системи.

4.2.22.6 API доступ до агрегованих даних моніторингу

Система онлайн-моніторингу повинна забезпечувати можливість програмного доступу до агрегованих даних моніторингу через прикладний програмний інтерфейс (API).

API повинен надавати доступ до узагальнених показників моніторингу з можливістю вибірки даних за визначеними параметрами, зокрема:

- за періодом моніторингу;
- за регіоном;
- за типом установи;
- за групами показників або окремими показниками.

API може використовуватися для інтеграції з зовнішніми аналітичними системами, інструментами візуалізації даних та системами підготовки звітності.

Доступ до API повинен здійснюватися з використанням механізмів автентифікації та авторизації відповідно до політики безпеки Системи онлайн-моніторингу.

4.2.22.7 Агрегування даних для аналітики

Для забезпечення високої продуктивності аналітичних запитів Система онлайн-моніторингу повинна використовувати механізми попереднього агрегування даних моніторингу.

Агреговані показники повинні формуватися на основі первинних даних моніторингу та зберігатися у спеціалізованих структурах даних (агреговані таблиці, матеріалізовані представлення або аналітичні набори даних).

Аналітичні модулі Системи онлайн-моніторингу (дашборди, графіки, звіти та API доступ) повинні використовувати агреговані дані, а не первинні транзакційні записи.

4.2.22.8 Версійність показників моніторингу

Система онлайн-моніторингу повинна забезпечувати підтримку версійності наборів показників моніторингу.

У разі зміни структури показників моніторингу (додавання нових показників, зміна критеріїв оцінювання або зміна формули розрахунку) повинна створюватися нова версія набору показників.

Дані моніторингу повинні зберігатися з прив'язкою до відповідної версії показників, що забезпечує коректний аналіз динаміки показників у часі.

4.3. Вимоги до персоналу, що забезпечує функціонування та експлуатацію засобу інформатизації.

Вимоги до чисельності та кваліфікації обслуговуючого персоналу КП Система онлайн моніторингу аналогічні вимогам до чисельності та кваліфікації обслуговуючого персоналу Єдиного державного вебпорталу електронних послуг. Додаткових вимог не висувається.

4.4. Вимоги до режимів функціонування засобу інформатизації.

Система онлайн-моніторингу після модернізації повинна забезпечувати безперервний режим функціонування у промисловому середовищі (24 години на добу, 7 днів на тиждень, 365 днів на рік), за винятком планових технологічних вікон.

Планові технологічні вікна для проведення оновлень або технічного обслуговування повинні бути попередньо погоджені із Замовником та/або технічним адміністратором та здійснюватися без втрати цілісності і збереження даних.

Для Системи онлайн-моніторингу розглядаються наступні режими функціонування:

- штатний режим (повна функціональність);
- режим регламентного обслуговування (з попередженням користувачів та/або обмеженням доступу);
- деградований режим: У разі недоступності зовнішніх інтеграцій Система онлайн-моніторингу повинна забезпечувати збереження часткової функціональності для користувачів.
- Аварійний режим (актуалізація процедур відновлення з резервних копій та плану реагування на інциденти — Disaster Recovery Plan)

Основним режимом функціонування Системи онлайн-моніторингу повинен бути штатний режим функціонування.

Режим регламентного обслуговування Системи онлайн-моніторингу призначений для виконання необхідних профілактичних регламентних заходів з обслуговування Системи онлайн-моніторингу (у складі Єдиного державного вебпорталу електронних послуг).

Під час регламентного обслуговування здійснюється створення резервних архівних копій баз даних і налаштувань Системи онлайн-моніторингу та оновлення версій програмного забезпечення.

Режим регламентного обслуговування Системи онлайн-моніторингу застосовується у період найменшого навантаження на Систему з боку користувачів і може передбачати виведення Системи із штатного режиму.

Аварійний режим функціонування Системи онлайн-моніторингу характеризується відмовою одного або декількох модулів Системи. У разі виявлення ознак, що свідчать про можливість переходу Системи онлайн-моніторингу в аварійний режим функціонування, обслуговуючий персонал повинен вжити необхідні заходи з метою:

- штатного завершення роботи програмних модулів Системи онлайн-моніторингу із збереженням даних;
- виконання резервного копіювання даних;
- за потреби - відключення доступу до Системи онлайн-моніторингу;
- усунення причин, що призвели до аварійного режиму Системи онлайн-моніторингу, та відновлення її працездатності.

Передача даних до зовнішніх систем повинна здійснюватися через механізм гарантованої доставки (guaranteed delivery) із використанням черги відкладеної обробки.

Усі помилки інтеграцій мають фіксуватися у журналі подій із можливістю автоматичної повторної відправки після відновлення доступності інтеграції.

При цьому зміст звіту не може бути змінений без створення нової версії відповідно до розділу 4.2.1.3 цього документа.

4.5. Вимоги до надійності роботи та збереження інформації.

Система онлайн-моніторингу повинна безвідмовно функціонувати, не зважаючи на наявність ймовірних помилок (дефектів), які можуть проявлятися під час експлуатації. Виправлення виявлених помилок (дефектів) повинно здійснюватися на етапах попередніх випробувань, дослідної експлуатації Системи онлайн-моніторингу та в ході постійної (промислової) експлуатації.

Система онлайн-моніторингу повинна взаємодіяти з іншими елементами Єдиного державного вебпорталу електронних послуг та не порушувати їх функціонування.

Відмова Системи онлайн-моніторингу не повинна викликати ушкодження даних або інших елементів Єдиного державного вебпорталу електронних послуг.

Збереженість інформації може забезпечуватись дотриманням вимог щодо:

- умов експлуатації Системи онлайн-моніторингу та його складових, визначених в експлуатаційній документації розробника Системи;
- порядку проведення резервного копіювання (ключових даних, еталонної копії та ін.) Системи онлайн-моніторингу та процедури відновлення з резервних копій.

Зокрема до процедур резервного копіювання висуваються наступні вимоги:

- існуючий регламент резервного копіювання бази даних (не рідше 1 разу на добу) має бути збережений із забезпеченням можливості позапланового резервування перед релізами;
- зберігання резервних копій – не менше 30 календарних днів (або інший строк відповідно до регламенту Замовника);
- цільовий показник RPO (Recovery Point Objective) для критичних даних – не більше 1 години. Для забезпечення зазначеного показника Виконавець зобов'язаний реалізувати механізм безперервного архівування журналів транзакцій (WAL) із підтримкою відновлення на довільний момент часу (Point-in-Time Recovery, PITR);
- технічна можливість відновлення на довільний момент часу в межах періоду зберігання резервних копій повинна бути забезпечена;
- перевірка відновлюваності резервних копій повинна проводитися шляхом тестового відновлення не рідше одного разу на квартал; результати перевірки документуються.

Оновлення Системи здійснюються у форматі релізів та поділяються на:

- **Major-релізи** — оновлення, що містять значні зміни функціоналу або архітектури;
- **Minor-релізи** — оновлення, що містять покращення функціоналу без зміни базової логіки;
- **Patch-релізи** — виправлення помилок та усунення вразливостей без зміни функціоналу.

Виконавець зобов'язаний забезпечити:

- зворотну сумісність API у межах однієї основної версії;
- відсутність втрати даних під час оновлення;
- можливість rollback до попередньої стабільної версії;
- проведення оновлень у погоджені технологічні вікна.

Зміни структури бази даних, що можуть вплинути на цілісність або сумісність, повинні супроводжуватися міграційними сценаріями та документацією.

4.5.1. Управління змінами (Change Request, CR)

Будь-які зміни до затверджених функціональних, архітектурних або інтеграційних вимог здійснюються виключно за процедурою управління змінами (Change Request, CR).

CR ініціюється Виконавцем або Замовником у письмовій формі та має містити:

- опис запропонованої зміни;
- обґрунтування необхідності;
- оцінку впливу на строки реалізації;
- оцінку впливу на бюджет (за наявності);
- оцінку впливу на архітектуру та безпеку.

Зміна набирає чинності лише після письмового погодження уповноваженими представниками сторін.

Внесення змін без погодженого CR не допускається.

4.5.2. Порядок міграції даних

У разі внесення змін до структури бази даних або моделей зберігання інформації Виконавець зобов'язаний забезпечити збереження цілісності та повноти наявних даних.

Міграція даних повинна:

- виконуватися із застосуванням контрольованих сценаріїв міграції (migration scripts);
- передбачати попереднє тестування у тестовому середовищі;
- супроводжуватися створенням резервної копії до початку виконання міграції;
- забезпечувати можливість rollback у разі помилки.

Міграційні сценарії та результати тестової міграції повинні бути задокументовані та погоджені із Замовником до виконання міграції у промисловому середовищі.

4.6. Вимоги до захисту інформації та кіберзахисту.

Управління інформаційною безпекою здійснюється відповідно до ризик-орієнтованого підходу (СУІБ) з урахуванням вимог законодавства України у сфері захисту інформації в інформаційно-комунікаційних системах. У випадках, прямо передбачених законодавством, вимоги щодо створення або модернізації авторизованої системи з безпеки інформації застосовуються відповідно до встановленого порядку.

Зокрема, висуваються наступні вимоги:

- передача даних – виключно з використанням захищених протоколів (TLS 1.2+);
- керування доступом – існуюча рольова модель (RBAC) має бути розширена за принципом найменших привілеїв, з можливістю розмежування доступу на рівні організації/регіону;
- захист коду – нові та доопрацьовані модулі мають бути захищені від типових вразливостей (OWASP Top 10) із застосуванням автоматизованих засобів DAST/SAST аналізу коду;
- управління секретами – має бути впроваджено зберігання секретів/ключів виключно через підсистеми Secrets Management, жорстке кодування (hardcoding) заборонено;
- проходження тестування на проникнення (pentest) – вимоги до проведення та критерії успішності визначаються у розділі 6 цього документа.
- існуючий механізм журналювання подій безпеки та ключових користувацьких дій має бути розширений для охоплення нових функцій (зміна ролей, конфігурація звітів, валідація, експорт);

- модернізація централізованого збору логів – логи повинні формуватися у форматі JSON із кореляційним ідентифікатором (request_id);
- маскуванню даних – має бути впроваджено механізм обов'язкового маскуванню персональних та чутливих даних перед їхньою відправкою до централізованого сховища (напр., ELK);
- має бути налаштований експорт метрик продуктивності (HTTP latency, error rate, queue depth) у форматі, сумісному з Prometheus (через /metrics endpoint);
- строк зберігання логів/аудиту — не менше 12 місяців (або інший строк за регламентом Замовника).

4.7. Вимоги до продуктивності.

Система онлайн-моніторингу повинна забезпечувати стабільну обробку не менше 5 000 одночасних активних користувацьких сесій (concurrent active sessions) у піковому режимі протягом не менше 60 хвилин під час навантажувального тестування.

Показник підтверджується навантажувальним тестуванням із використанням узгодженого із Замовником інструменту (k6, JMeter або еквівалентного) та погодженого сценарію тестування.

Архітектура рішення повинна забезпечувати можливість горизонтального масштабування до 10 000 одночасних користувацьких сесій без зміни програмного коду або бізнес-логіки застосунку шляхом масштабування інфраструктури Kubernetes.

4.8. Вимоги до інтерфейсу користувача та зручності використання.

Виконавець повинен забезпечити доступність інтерфейсів для осіб з інвалідністю, зокрема для осіб із порушеннями зору, слуху, опорно-рухового апарату, мовлення та інтелектуального розвитку, а також із різними комбінаціями порушень, відповідно до ДСТУ EN 301 549:2022 (EN 301 549 V3.2.1 (2021–03), IDT) «Інформаційні технології. Вимоги щодо доступності продуктів та послуг ІКТ» (далі – **Стандарт**), що, зокрема, включає відповідність всім критеріям успішності Настанов з доступності вебвмісту (WCAG) 2.1 (далі – **WCAG**), які мають рівні відповідності А і AA.

Нижче наведено уточнення:

Контрастність текстів. Вебсайт **повинен** бути забезпечений мінімальним коефіцієнтом контрастності між текстом і фоном, на якому він розташований, для забезпечення достатньої читабельності, навіть якщо людина не бачить повного діапазону кольорів. Коефіцієнт контрастності великого тексту повинен складати не менше **3:1**, а тексту, який не є великим, – не менше **4.5:1**. Винятки описані в пункті 1.4.3 WCAG.

Контрастність елементів інтерфейсу. Вебсайт **повинен** бути забезпечений мінімальним коефіцієнтом контрастності між інтерактивними елементами (посиланнями, кнопками, полями вводу, прапорцями, маркерами фокуса, тощо) та фоном, на якому вони розташовані, для забезпечення їх кращої видимості. Коефіцієнт контрастності таких елементів повинен складати не менше **3:1**. Винятки описані в пункті 1.4.11 WCAG.

Контрастність графічної інформації. Вебсайт **повинен** бути забезпечений мінімальним коефіцієнтом контрастності між елементами графічної інформації (секторами діаграм, елементами графіків, тощо) та фоном, на якому вони розташовані, для забезпечення їх кращої видимості. Коефіцієнт контрастності таких елементів повинен складати не менше **3:1**. Винятки описані в пункті 1.4.11 WCAG.

Колір **не повинен** використовуватися як єдиний візуальний засіб передачі інформації, вказівки на дію, спонукання до відповіді або розрізнення візуального елемента.

Фокус та підсвічування. Інтерактивні елементи, на яких можливо сфокусуватися (посилання, кнопки, поля вводу, прапорці, тощо) **повинні** отримувати явну візуальну індикацію при фокусуванні на них (маркер фокуса). Маркер фокуса може мати, наприклад,

вигляд рамки навколо елемента. Коефіцієнт контрастності маркера фокуса щодо фону повинен бути не менше **3:1**.

Підкреслення гіперпосилань. Всі гіперпосилання **повинні** бути підкреслені або мати інше явне стилістичне відображення, яке відрізняє їх від тексту. Для гіперпосилань, які розташовуються прямо посеред тексту, **рекомендується** застосовувати саме підкреслення як традиційний засіб оформлення гіперпосилань.

Сумісність з допоміжними технологіями. Вебсайт **повинен** бути сумісним з основними допоміжними технологіями, включаючи скринридери, збільшувачі екрану, голосові команди та інші спеціальні засоби доступу.

Навігація клавіатурою. Весь функціонал вебсайту **повинен** бути доступним з клавіатури, тобто не вимагати використання миші чи інших засобів позиціонування курсора. Це включає можливість як фокусуватися на всіх інтерактивних елементах, так і викликати події їх активації (натискання кнопок, перемикачів, прапорців, розгортання випадаючих списків, тощо), використовуючи лише клавіші клавіатури. Користувач при цьому не повинен потрапляти в ситуацію так званої "пастки фокуса".

Альтернативний текст для нетекстового змісту. Зображення **повинні** мати текстовий опис (альтернативний текст) для забезпечення доступності для користувачів зі скринридерами. Ця вимога не поширюється на графіку, яка виконує явно декоративні функції, тобто не передає значущу інформацію. Така графіка повинна бути прихована від скринридерів (мати атрибут `alt=""`).

Визначення основної мови сторінки. Правильно вказана мова сторінки забезпечує коректну роботу асистивних технологій. Якщо веб-сторінка використовує декілька мов, слід вказати мову, яка використовується найчастіше. Для української мови **повинно** бути так: `<html lang="uk">`.

Швидкий перехід до основного вмісту сторінки. У шапці вебсайту одним з перших елементів **повинно** бути розміщене посилання, при активації якого користувацький фокус ставиться на перший елемент основного вмісту сторінки. Текстову мітку такого посилання **рекомендується** робити "Перейти до основного вмісту". Це посилання може бути за замовчуванням невидимим, і ставати видимим лише в момент постановки фокусу клавіатури на нього.

Повинні мати програмні текстові мітки для скринридерів (`aria-label` чи ін.) наступні елементи:

- кнопки, якщо не мають видимого тексту (кнопки-іконки, тощо);
- посилання, якщо не мають видимого тексту (посилання-логотипи, посилання-зображення, тощо);
- поля форм.

Якщо використовуються не нативні HTML-елементи (`<button>`, `<select>`, тощо), то в коді елементів **повинні** бути присутні необхідні атрибути доступності для забезпечення коректної взаємодії скринридерів з такими елементами (`role="button"`, тощо).

Масштабування. **Повинна** бути забезпечена можливість масштабування (власними засобами, тобто використовуючи відповідний функціонал власних браузерів) тексту та іншого вмісту до 200% без втрати функціональності, контент при цьому **повинен** належним чином перекомпоновуватись без втрати функціональності, зникнення або взаємного перетинання елементів.

Щодо заголовків **повинні** виконуватися наступні твердження:

- Заголовок **повинен** бути програмно (семантично) визначений, а не просто бути жирним текстом збільшеного розміру (тобто слід застосовувати теги `<h1>` – `<h5>` АБО поєднання атрибутів `role="heading"` `aria-level="N"`, де N – потрібний рівень).
- Заголовки на сторінці **повинні** починатися з рівня 1 (`<h1>`).

- **Рекомендується**, щоб на сторінці був лише один заголовок рівня 1 (<h1>).
- **Не повинно** бути пропусків рівнів у заголовків на сторінці (тобто, наприклад, після <h3> не повинен йти <h5>).
- Заголовки **повинні** логічно відображати структуру вмісту сторінки, еквівалентні за змістом елементи повинні мати той самий рівень, а не різні.
- Заголовки **не повинні** застосовуватися до абзаців тексту чи інших елементів, які не виконують функцію заголовка.

Щодо списків **повинні** виконуватися наступні твердження:

- Списки **повинні** бути програмно (семантично) визначені за допомогою тегів , та .
- Безпосередніми нащадками елементів і **повинні** бути елементи .
- Списки **повинні** застосовуватися для досягнення відповідної мети.
- **Рекомендується** не застосовувати список, якщо в ньому лише 1 елемент.

Щодо таблиць **повинні** виконуватися наступні твердження:

- Таблиці **повинні** бути програмно (семантично) визначені за допомогою тегів <table>, <tr>, <td> та інших спеціально призначених для цього тегів.
- Комірки таблиць, які виконують роль заголовка для рядків чи стовпців, **повинні** бути визначені за допомогою тегу <th>.
- Таблиці **не повинні** застосовуватися для цілей побудови макета, верстки, тощо (тобто для суто візуальних цілей).

Рекомендується не об'єднувати комірки таблиць (скринридери не можуть коректно інтерпретувати їх).

5. ВИМОГИ ДО СУПРОВОДУ ТА ОБСЛУГОВУВАННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ

5.1. Вимоги до гарантійної підтримки.

Система онлайн-моніторингу та надана документація повинні забезпечуватися гарантійною підтримкою протягом не менше 12 календарних місяців з дати підписання Акта приймання-передачі комп'ютерної програми.

Зокрема гарантійна підтримка має включати:

- Реагування на інциденти, що спричинили неправильну роботу комп'ютерної програми;
- Конфігурація сервера, відновлення працездатності у випадку порушення функціонування;
- Перевірка логів та помилок на промисловому середовищі відповідно технічним вимогам;
- Виправлення виявлених помилок та недоліків в роботі та налаштуваннях;
- Перевірка логів та помилок на промисловому середовищі згідно з затвердженими регламентом та технічними вимогами;
- Аналіз та виправлення помилок бізнес-процесів за допомогою BPMN 2.0;
- Здійснення необхідних налаштувань для забезпечення ефективної роботи;
- Інформаційна підтримка.

Рреагування на інциденти, пов'язані з функціонуванням модернізованих компонентів Системи, здійснюється відповідно до погоджених рівнів сервісу (SLA), визначених договором та/або технічним завданням.

Інциденти повинні класифікуватися за рівнями критичності залежно від їх впливу на працездатність Системи, доступність функціоналу та цілісність даних.

Для кожного рівня критичності повинні бути визначені:

- максимальний час реагування;
- максимальний час відновлення працездатності;
- порядок ескалації;
- відповідальні сторони.

Конкретні значення показників SLA, зокрема час реагування та час відновлення, визначаються договором, технічним завданням або програмою гарантійної підтримки.

5.2. Вимоги до навчання користувачів (за потреби);

Виконавець **зобов'язаний забезпечити** проведення навчання користувачів та адміністраторів Системи за заздалегідь погодженою із Замовником програмою.

- Цільові аудиторії: Програма навчання повинна охоплювати всі ролі ієрархії RBAC: (1) Операторів (Адміністраторів) Мінцифри, (2) Операторів ОДА/ОВА та ЦОВВ, (3) відповідальних осіб ЦНАП (ТП/ВРМ) та СНАП, (4) технічних адміністраторів інфраструктури Замовника.
- Формат та матеріали: Навчання має проводитися у форматі онлайн-сесій (вебінарів) із демонстрацією реальної роботи в модернізованій Системі онлайн-моніторингу та сесіями запитань-відповідей.
- Артефакти навчання: Виконавець повинен передати Замовнику: записи проведених вебінарів, презентаційні матеріали, покрокові інструкції, чек-листи для типових сценаріїв роботи та короткі скринкасти (відеоінструкції) для найчастіших операцій (наприклад, конфігурація звітів, створення користувачів).

5.3. Вимоги до документації.

Виконавець **зобов'язаний розробити та надати** комплект актуальної проектної та експлуатаційної документації українською мовою у форматах .docx та у вигляді wiki-репозиторію (наприклад, Confluence/GitLab Wiki). Мінімальний склад документації **повинен включати**:

- Опис бізнес процесів.
- Технічне завдання.
- Опис КІ Система онлайн-моніторингу.
- Інструкція користувача.
- Інструкція адміністратора
- Керівництво з розгортання та експлуатації (DevOps Guide)
- План відновлення після збоїв (Disaster Recovery Plan)
- Документація з інформаційної безпеки.
- Програми та методики всіх видів випробувань (які проводить Виконавець).
- Протоколи випробувань (які проводить Виконавець).

Інструкція користувача повинна включати детальний опис основних бізнес-сценаріїв (подання/валідація звітності, функціональна робота Системи онлайн-моніторингу, завантаження матеріалів, формування та експорт звітів і дашбордів).

Інструкція адміністратора повинна включати інструкції з управління користувачами та ролевою моделлю, ведення довідників, регламенти створення нових шаблонів у «Конфігураторі звітів».

Керівництво з розгортання та експлуатації (DevOps Guide) повинно включати опис інфраструктури, процесу розгортання (CI/CD pipelines, Docker-контейнери), конфігурації

середовищ, міграції БД, процедур резервного копіювання (Backup) та моніторингу працездатності.

План відновлення після збоїв (Disaster Recovery Plan) повинен включати покрокову інструкцію з відновлення працездатності Системи у разі критичних аварій.

Документація з інформаційної безпеки повинна включати опис реалізованих механізмів захисту інформації у компонентах, що створюються або змінюються в межах модернізації, включаючи механізми автентифікації, авторизації та журналювання подій.

6. ВИМОГИ ДО ПРИЙМАННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ

6.1 Вимоги до проведення випробувань

Після завершення розробки Системи онлайн-моніторингу Виконавець проводить наступні види випробувань:

- Функціональне тестування;
- Навантажувальне тестування;
- Тестування на проникнення;
- Приймальне тестування.

6.1.1. Функціональне тестування

Функціональне тестування відбувається відповідно до документа «Програма та методика функціональних випробувань», що передбачає перевірку виконання оновлених функцій Системи онлайн-моніторингу. Результати тестування оформлюються протоколом функціональних випробувань.

6.1.2. Навантажувальне тестування

Після розгортання Системи онлайн-моніторингу у тестовому середовищі проводиться навантажувальне тестування з метою перевірки продуктивності, стабільності та відповідності встановленим показникам продуктивності, відповідно до програми та методики проведення навантажувального тестування.

Результати навантажувального тестування оформлюються окремим протоколом.

6.1.3. Тестування на проникнення (Pentest)

Перед введенням модернізованої Системи онлайн-моніторингу в промислову експлуатацію обов'язковим є проведення тестування на проникнення (pentest).

Критерієм приймання результатів pentest є відсутність не виправлених вразливостей рівня High та Critical відповідно до міжнародних стандартів оцінки вразливостей (CVSS або еквівалентних).

Pentest може проводитися як Виконавцем, так і незалежною стороною за погодженням із Замовником.

У межах гарантійної підтримки Виконавець зобов'язаний усувати виявлені вразливості рівня High та Critical у строки, визначені SLA (відповідно до рівня інциденту P1 або P2).

6.1.4. Приймальне тестування (UAT)

Перед введенням модернізованої Системи онлайн-моніторингу у промислову експлуатацію проводиться приймальне тестування (User Acceptance Testing, UAT) за участю Замовника.

UAT проводиться відповідно до розроблених програм та методик та включає:

- перевірку функціональних вимог;
- перевірку інтеграційних взаємодій;
- перевірку звітності та аналітичних показників;
- перевірку ролей і моделі доступу.

Результати UAT оформлюються протоколом проведення приймального тестування.

6.2. Вимоги до передачі результатів виконаних робіт та/або наданих послуг.

Перед початком проведення випробувань мають складатися наказ(и) щодо створення та складу приймальної комісії, акт завершення робіт, акт приймання в дослідну експлуатацію.

Програми та методики відповідного виду тестування готуються розробником Системи онлайн-моніторингу. Перелік та зміст перевірок, які підлягають включенню в програму та методику приймального тестування, зокрема повинні включати:

- Перевірку комплектності Системи онлайн-моніторингу;
- Перевірку комплектності і якості документації;
- Перевірку комплектності, достатності складу, якості програмних засобів і програмної документації;
- Перевірку ступеня виконання вимог функціонального призначення системи.

Перелік та зміст перевірок, які підлягають включенню в програму та методику приймального тестування, повинні також включати перевірки виконання всіх вимог Технічного завдання на створення Системи онлайн-моніторингу.

Протоколи всіх видів тестування мають містити:

- найменування об'єкту випробувань;
- перелік посадових осіб, які проводили випробування;
- мета випробувань;
- відомості про тривалості випробувань;
- Перелік тестів (або перелік пунктів технічного завдання), на відповідність яким проведені випробування;
- перелік пунктів «Програми випробувань», за якими проведені випробування;
- відомості про результати випробувань;
- відомості про відмови, збої і аварійні ситуації, що виникають при випробуваннях (за наявності);
- відомості про необхідні параметри коригування КП Системи онлайн-моніторингу і технічної документації (за необхідності);
- висновок щодо позитивних або негативних результатах випробувань.

6.3 Порядок приймання

Результати послуг з модернізації приймаються комісією за умови:

- успішного проходження функціонального тестування;
- підтвердження показників навантажувального тестування;

- відсутності не виправлених вразливостей рівня High та Critical;
- підписання протоколу UAT.

Впровадження Системи онлайн-моніторингу передбачає виконання наступних робіт:

- підготовка та передача КП Системи онлайн-моніторингу та документації на КП;
- передачу майнових прав на КП Система онлайн-моніторингу та ліцензій на використання елементів КП Система онлайн-моніторингу (в разі якщо при розробці КП використовувалось програмне забезпечення сторонніх компаній);
- оформлення та затвердження акту прийому-передачі програмного забезпечення та документації.

Перехід у промислове середовище допускається виключно після підписання Акта приймання-передачі КП «Система онлайн-моніторингу».

Передача результатів модернізації **повинна здійснюватися** у складі та форматі, що забезпечує повну незалежність, можливість повноцінної експлуатації та подальшого розвитку Системи онлайн-моніторингу власними силами або із залученням третіх осіб. Процес передачі **повинен включати:**

1. **Вихідний код:** Повний вихідний код із збереженою історією змін (commit history) передається у вигляді Git-репозиторію разом з інструкціями зі збирання (build) та локального запуску.
2. **Інфраструктура як код (IaC) та Конфігурації:** Комплект файлів конфігурації для розгортання у тестовому (Staging) та продуктивному (Production) середовищах. **Суворо забороняється** наявність у вихідному коді чи конфігураціях жорстко закодованих секретів (hardcoded passwords, API keys). Виконавець **повинен надати** опис механізму керування секретами.
3. **База даних:** Скрипти міграцій (наприклад, Liquibase/Flyway), повний опис моделі даних, скрипти для наповнення базовими довідниками (seeds).
4. **Звіти безпеки (SAST/DAST):** Результати автоматизованого сканування вихідного коду на наявність вразливостей (SAST) із підтвердженням відсутності критичних (Critical/High) загроз.
5. **Майнові права:** Передача Бенефіціару/Реципієнту всіх майнових прав інтелектуальної власності на всі створені програмні компоненти, модулі та документацію, розроблені в рамках даної модернізації.
6. **Звітні документи:** Акт приймання-передачі виконаних робіт (наданих послуг), що супроводжується детальним звітом із переліком реалізованих вимог (Traceability Matrix), Акт приймання-передачі комп'ютерної програми, що передається Замовнику за результатами модернізації; та посиланнями на відповідні релізи/коміти.

Передані матеріали повинні забезпечувати можливість повного розгортання, супроводу та розвитку Системи без обов'язкової участі Виконавця.

7. ВИМОГИ ДО ВИКОНАВЦЯ

Виконавець у складі тендерної пропозиції або на етапі розробки технічного завдання подає техніко-економічне обґрунтування (ТЕО), яке деталізує запропоновані технічні рішення в межах вимог цього документа.

ТЕО не може змінювати або нівелювати базові архітектурні вимоги до КП Система онлайн-моніторингу, без погодженого в установленому порядку Запиту на зміну (CR).

У складі пропозиції Виконавець також надає інформацію щодо команди розробників, залучених до реалізації проєкту, із зазначенням ролей та підтвердженого досвіду, а також резюме кожного ключового спеціаліста.

Наявність досвіду

Досвід успішного впровадження не менше 2 проєктів, аналогічного за предметом цих Технічних Вимог.

Досвід розробки, модернізації або супроводу інформаційних систем суміжних з предметом цих Технічних Вимог.

Наявність матеріально технічної бази

Виконавець повинен мати наявне обладнання, необхідне для проведення розробки програмного забезпечення, включаючи комп'ютери, робочі станції, сервери та інше необхідне обладнання.

У разі використання хмарних платформ для розробки, Виконавець повинен мати доступ до відповідних ресурсів, таких як віртуальні машини, контейнери, облачні сервіси тощо.

Виконавець повинен мати належні ліцензії на необхідне програмне забезпечення для розробки, таке як інтегровані середовища розробки (IDE), бази даних, сервери додатків тощо.

Виконавець повинен забезпечити безпеку своєї матеріально-технічної бази, включаючи захист від несанкціонованого доступу та збереження конфіденційності даних.

8. ОРІЄНТОВНИЙ КАЛЕНДАРНИЙ ПЛАН РОЗРОБКИ СИСТЕМИ ОНЛАЙН-МОНІТОРИНГУ

Загальний строк надання послуг зі створення комп'ютерної програми для модернізації Єдиного державного вебпорталу електронних послуг з метою розширення функціоналу Системи онлайн-моніторингу та оцінки якості послуг становить до 10 місяців з дати укладення договору.

Деталізований календарний план виконання робіт, у тому числі строки виконання окремих етапів, порядок взаємодії сторін, перелік проміжних результатів та строки їх погодження, визначається Виконавцем після укладення договору та погоджується із Замовником/Бенефіціаром.

Деталізований календарний план не може передбачати збільшення загального строку надання послуг, визначеного цими Технічними вимогами, крім випадків, прямо передбачених договором або погоджених сторонами у встановленому порядку.

Орієнтовні етапи виконання робіт:

Етапи виконання робіт	Орієнтовні строки виконання	Результат
1.1 Аналіз та документування БП	До 1 місяця	Документи з описами бізнес процесів
2.1 Розробка та погодження технічного завдання	До 2 місяців	Технічне завдання на створення Системи онлайн-моніторингу
3.1 Проєктування Системи онлайн-моніторингу	До 3 місяців	Документ «Опис Системи онлайн-моніторингу»
3.2 Розробка та налаштування функціоналу Системи онлайн-моніторингу	До 8 місяців	Дослідний зразок Системи онлайн-моніторингу
3.3. Розробка експлуатаційної документації Системи онлайн-моніторингу	До 9 місяців	Експлуатаційна документація на Систему онлайн-моніторингу
3.4 Тестування Системи онлайн-моніторингу, дослідна експлуатація та усунення виявлених недоліків	До 10 місяців	Протоколи тестування
3.5 Приймальне тестування та передача результатів робіт	До 10 місяців	Протокол приймального тестування