Обґрунтування технічних та якісних характеристик предмета закупівлі, його очікуваної вартості та/або розміру бюджетного призначення

1. **Найменування:** Комунальне спеціалізоване монтажно-експлуатаційне підприємство
2. **Місцезнаходження:** 54028, Миколаївська обл., м. Миколаїв, вул. 11 Лінія, 80
3. **ЄДРПОУ:** 13845696
4. **Предмет закупівлі:** ДК 021:2015:48810000-9: Інформаційні системи - програмно-апаратний комплекс для створення системи оперативно-диспетчерського управління дорожнім рухом.
5. **Кількість в обсягах:** 1 одиниця
6. **Місце поставки товару:** вул. 11 Лінія, 80, Миколаївська 1обл. м. Миколаїв, 54028
7. **Очікувана вартість:** 4239720,00грн. з ПДВ.
8. **Строк поставки товару:** з моменту підписання договору і до 01.12.2023р.
9. **Кінцевий строк подання тендерних пропозицій:** 30.09.2023; 12:00.
10. **Умови оплати:** розрахунки проводяться шляхом: оплати Замовником після пред'явлення Постачальником рахунка на оплату товару (далі - рахунок), виставленого на підставі заявки, згідно акту прийому-передачі/ виставлених рахунків та видаткових накладних протягом 20 календарних днів.
11. **Гарантійний строк:** Гарантія на Товар – не менше 12 місяців з дати оформлення та підписання акту прийому-передачі.
12. **Мова, якою повинні готуватись тендерні пропозиції:** українська.
13. **Розмір, вид та умови надання забезпечення тендерних пропозицій:** розмір забезпечення тендерної пропозиції: 60 000,00 грн. (шістдесят тисяч гривень 00 коп.).
14. **Дата та час розкриття тендерних пропозицій:** визначаються електронною системою закупівель автоматично в день оприлюднення замовником оголошення про проведення відкритих торгів в електронній системі закупівель.
15. **Розмір мінімального кроку пониження ціни:** 1%.
16. **Забезпечення виконання договору про закупівлю:** розмір забезпечення виконання договору про закупівлю становить 5% від вартості договору.
17. **Підтвердження визначення очікуваної вартості:**

Здійснено розрахунок очікуваної вартості методом розрахунку очікуваної вартості товарів на підставі трьох отриманих цінових пропозицій . За найбільш економічно вигідними цінами розрахована вартість закупівлі.

ІНФОРМАЦІЯ ПРО НЕОБХІДНІ ТЕХНІЧНІ, ЯКІСНІ ТА КІЛЬКІСНІ ХАРАКТЕРИСТИКИ ДО ПРЕДМЕТА ЗАКУПІВЛІ

Предмет закупівлі: ДК 021:2015:48810000-9: Інформаційні системи - програмно-апаратний комплекс для створення системи оперативно-диспетчерського управління дорожнім рухом
Кількість товару: 1 одиниця

Специфікація закупівлі

№	Позиція	Од.виміру	Кількість
1	**Серверний комплект з програмним забезпеченням АСКДР**	комплект	1
2	**Обладнання візуалізації «Карта міста»**	комплект	1
3	**Робоча станція «Автоматизоване робоче місце диспетчера»**	комплект	1
4	**Стенд тестовий**	комплект	1
5	**Інженерний комплект**	комплект	1

*** У вартість обладнання включити вартість шефмонтажу та пусконалагоджувальних робіт.**

Основні позначення і скорочення

АСКДР - автоматизована система керування дорожнім рухом
ЦК АСКДР – центр керування АСКДР
АСКДІ – автоматизована система керування об'єктами дорожньої інфраструктури, яка є розвитком АСКДР
ЦК АСКДІ – центр керування АСКДІ
ВДМ – вулично-дорожня мережа
ДК – дорожній контролер
ДТ – детектор транспорту
ДТП – дорожньо-транспортна пригода
ЗІС – зовнішня інформаційна система
ТВП – табло виклику пішохідні
ЗВП – запасні вироби і пристрої
ОК – обчислювальний комплекс
ТЗ – транспортний засіб
Сисадмін – адміністратор інформаційної мережі
СО – світлофорний об'єкт

Загальні вимоги

1 <u>Вимоги до програмного забезпечення</u>

Програмне забезпечення АСКДР (далі - ПЗ) повинно базуватися на використанні відкритого протоколу обміну даних та використанням сучасних веб- та сервісно-орієнтованих технологій. Рішення в цілому повинно бути побудоване за клієнт-серверною архітектурою.

1.1. функціональна масштабованість (забезпечення нарощування кількісних та якісних показників функціонування АСКДР, можливість роботи із дорожніми контролерами типу РЕ та/або RTC);
1.2. територіальна масштабованість (можливість розширення територіального розташування об'єктів автоматизації);
1.3. корпоративність (забезпечення зручного, прозорого але з достатнім рівнем безпеки доступу користувачів до АСКДР згідно наданих їм прав доступу);
1.4. гнучкість (удосконалення/модернізація процесів управління не повинно призводити до зупинки АСКДР, при цьому АСКДР повинна мати можливість налагодження правил організації бізнес-процесів);
1.5. відкритість (наявність інтерфейсів прикладного програмування повинні дозволяти створювати нові програмні додатки та організувати обмін даними з іншими системами);
1.6. захищеність (АСКДР повинна здійснювати доступ користувача до даних, функцій, задач і настроювання управління бізнес-процесами виключно до рівня прав доступу, які призначені користувачу адміністратором АСКДР та/або через використання засобів персоніфікації /ідентифікації);
1.7. розподіленість АСКДР повинна підтримувати виконання розподілених транзакцій та забезпечити доступ для роботи згідно до певних бізнес-процесів для віддалених структурних підрозділів/співробітників через системи телекомунікацій, мереж у тому числі через інтернет

по кабельним лініям зв'язку та/або стільниковий зв'язок);

1.8. відмовостійкість (АСКДР повинна мати певні рівні надійності щодо Її працездатності, наприклад, резервні захищені копії бази даних, технологічна масштабованість захист від кібер атак тощо);

1.9. уніфікованість (опис робочих місць персоналу повинен бути уніфікованим та регламентованим, при цьому кожному співробітнику надається особистий акаунт в АСКДР відповідно до його посадових обов'язків);

2 Вимоги до структури АСКДР і призначення її елементів

2.1. Вимоги до складових частин АСКДР

2.1.1. Обладнання візуалізації «Карта міста»

Монітори відеостіни розміром 50” (4шт).

Монітори відостіни повинні мати такі характеристики або кращі:

- Роздільна здатність FulL HD чи Ultra HD 4K;
- Розмір кромки краю панелі 3,5 мм чи менше;
- Інтерфейси зв’язку: LAN (4G45), 2xHDMI, DP, OPS, DVI, USB, VGA;
- Пристосованість для роботи в режимі 24/7;
- Тип матриці: IPS/PLS;
- Інтерфейс кріплення VESA 400x400;
- Контрастність статична 1300:1 чи краще;
- Гарантія 36 місяців.

Кріплення відеостіни

Кріплення відеостіни повинні мати такі характеристики або кращі:

- Пристосованість для встановлення 4х відео панелей згідно вимог до моніторів відостіни;
- Пристосованість конструктиву кріплення кожної відео панелі для висунення, нахилу та повороту відео панелей;
- Максимальне навантаження 200 кг, чи більше;
- Максимальне навантаження одної секції встановлення відео панелей 40 кг чи більше;

- Передбачити мобільність конструктиву з встановленими відео панелями.

Комп'ютер відеостіни з операційною системою та Microsoft Office

Комп'ютер відеостіни повинен мати такі характеристики або кращі:

- Процесор Intel Core i5, 2,8-4 ГГц чи краще;

- ОЗУ - 8 ГБ чи краще;

- SSD - 240 ГБ чи більше;

- Відеокарта с 4 відеовиходами з роздільною здатністю Ultra HD 4K чи краще. Слоти підключення відео панелей (DVI, HDMI) відповідно до наявних слотів відео панелей;

- LAN 1 Гбіт/с (4G45) та інші;

- Дисплей 24” чи краще.

2.1.2 Серверний комплект

Серверний комплект ЦК АСКДР складається з:
Шафа напільна серверна повинна мати такі характеристики або кращі:

- Модель та розміри 42U 600x800;
- Патч - панель Hypernet 19” 24Xrj-45 UTP, cat. 5e (PP-KUTP24-NM / PP-KUTP24-LC) 2 шт.;
- Полка 19" 2U глуб. 450мм. Консольна 2 шт.;
- Кріплення 19" 2 шт. ;
- Силовий блок 19" 8 розеток.

Комп'ютер сервера АСКДР повинен мати такі характеристики або кращі (2 шт.):

- Процесор – s1200 Intel Core i9-10900K (3.7-5.3 ГГц) 10яд. 20пот. 20Mb DDR4 2933 95W;

- вбудована графічна карта -INTEL UHD 630 350-1200MHz BOX;

- ОЗУ – 16 Гб;

- SSD M.2 2280 NVMe 512ГБ;

-2xHHD 3.5”SATA III 2TB;

- Блок живлення ATX 700W;

- Кулер для процесора (або еквівалент).

Джерело безперебійного живлення повинно мати такі характеристики або кращі:

- Модель APC Smart-UPS SRT 2200VA (SRT2200XLI) 1980 Вт ;
- 2200 В*А (або еквівалент).

Мережеве устаткування повинно мати такі характеристики або кращі:

- комутатор LinkSys LGS124 24x1000 (або еквівалент);
- наявність аксесуарів та кабелів.

2.1.3 Робоча станція «Автоматизоване робоче місце диспетчера»

Автоматизоване робоче місце диспетчера АСКДР з операційною системою оснащується комп'ютером та монітором. Комп'ютер автоматизоване робочого місця диспетчера АСКДР повинен мати такі характеристики або кращі (2 шт.):

- Процесор - Intel Core i3-8100T (3.1 ГГц);

- вбудована графічна карта -INTEL UHD 630 ;

- ОЗУ - 4 ГБ;

- SSD для ОС- 128 ГБ;

- LAN 1 Гбіт/с;

- Клавіатура, миша.

2.1.4 Стенд тестовий

Стенд тестування дорожніх контролерів на 48 силових виходів та модулем I/0 на 8 входів та 8 виходів.

2.1.5 Інженерний комплект

Інженерний комплект складається з ноутбуку, кардрідера, монітору 7", кабелів та сумки.

Передбачити використання Firerwall (міжмережевого екрану) для захисту Системи від несанкціонованого доступу. Апаратний комплекс Системи повинен бути пристосований для віддаленого дистанційного контролю: стану живлення серверів, контролю трафіку тощо.

3 <u>Функціональні вимоги до АСКДР</u>

АСКДР повинна забезпечувати відповідність таким характеристикам:

- до експлуатації різними підприємствами з можливістю їх категоризації та сегментації, створенням розподілених користувацьких груп та ролей;
- на необмежену кількість ОДІ;
- для роботи з різними типами дорожніх контролерів;
- для підключення нових типів ОДІ та/або груп ОДІ;
- для підпорядкування в систему більш високого рівня інтеграції (муніципальні,загальнодержавні);
- можливість зберігання журналів операцій та протоколів роботи протягом усього часу використання модулів Системи (за наявності апаратних потужностей);
- здатність до горизонтального масштабування в режимі реального часу без зупинки сервісу;
- система повинна мати механізм синхронізації часу через використання «Протоколу мережевого часу» та забезпечувати синхронізацію часу по годинах еталонного часу у відповідності до поточного часового поясу в якому розташований Київ;

- можливість нарощування кількості користувачів та об'ємів баз даних без потреби будь-яких додаткових доробок;
- здатність адаптивного управління не тільки одного світлофорного об'єкту, а ВДМ в комплексі;
- на взаємодію (обміну даними) з іншими системами.

4 Вимоги до лінгвістичного забезпечення

Інтерфейс користувача АСКДР повинен бути виконаний українською мовою. Нормативно-довідкова інформація, класифікатори і довідники ведуться українською мовою, в деяких випадках
може бути присутня англійська мова.
Допускається використання англійської мови під час виконання регламентних процедур.

5 Вимоги до рольової моделі

Ліцензійне ПЗ повинно дозволяти робити розподіл ролей між фахівцями за їх функціональними обов'язками, з урахуванням керування певними визначеними для таких ролей
ОДІ.
В межах АСКДР передбачаються такі ролі:

- системний адміністратор - можливість доступу до інформації всіх сегментів АСКДР,управління конфігураціями, забезпечення функціонування, керування користувачами та групами,визначення прав доступу до інформації;

- адміністратор - можливість доступу до інформації конкретного сегменту АСКДР та керування правами користувачів та груп такого сегменту;

- технолог - право створювати та видаляти ОДІ й визначати їх режими роботи;

- диспетчер - право визначати режими роботи ОДІ;

- користувач - виключно перегляд інформації з певних сегментів АСКДР.

Має бути передбачена приблизна кількість автоматизованих робочих місць диспетчерського

та інженерно-технічного персоналу не менше 40 од.

Для визначення рольової моделі має бути передбачено відповідний інтерфейс.

Кожний обліковий запис користувача АСКДР повинен включати наступні параметри

конфігурації:

- Логін/ім'я (текстове поле);

- Організація/група (текстове поле);

- Пароль (текстове поле);

- Електронна пошта (текстове поле);

Система повинна підтримувати ієрархічну структуру користувачів і груп користувачів, і дозволяти наступне:

- Користувачі можуть бути призначені в групи користувачів.

- Групи користувачів можуть бути призначені на один або кілька ОДІ, груп, розділів.

- Кожній групі користувачів може бути призначено одне або декілька з наступних дозволів:

- Адміністратор;
- Підтвердження сигналів тривоги;
- Редагування бази даних;
- Конфігурація і управління ОДІ ;
- Плани контролю пристроїв;
- Час синхронізації;
- Тільки перегляд.

6 Вимоги до інтерфейсів та їх груп

Вимоги до картографічного інтерфейсу

Картографічний інтерфейс має бути основним інтерфейсом для таких користувацьких ролей: користувач, диспетчер, технолог.

Таблиця 1. Вимоги до картографічного компоненту

Масштабування	Картографічний компонент має дозволяти масштабувати електронні карти починаючи з рівня масштабування «квартал», на якому видимі будинки з їх номерами, до рівня масштабування «місто», на якому видиме все місто і його основні магістралі.
Карти	Інформація має надаватись на декількох типах карт (дві чи більше), що надаватиме додаткову стійкість (мапа Системи повинна підтримувати використання карт Google maps, Open Stree та ін.).
Підсистеми. Шари карт	Однотипні ОДІ мають бути об'єднані в компоненти або підсистеми. Однотипні ОДІ мають відображатись на карті у вигляді однакових іконок (піктограм). Кожна підсистема має відображатись в окремому шарі карти. Шари карт повинні бути налаштовані для

	відображення окремо чи сумісно з іншими шарами (підсистемами).
Вигляд піктограми	Вигляд піктограми визначає базові властивості стану об'єкту інфраструктури: тип об'єкту інфраструктури, наявність несправностей, стан зв'язку тощо.
Миттєва діагностика	При наведенні покажчика миші на піктограму ОДІ на екран має надаватись інформація миттєвої діагностики мінімального обсягу у складі: найменування ОДІ; поточний час останньої сесії зв'язку; стан ОДІ під час останньої сесії зв'язку; несправності в каналах керування (силових виходах дорожнього контролера).

Вимоги до інтерфейсу взаємодії з іконками для ОДІ

Функціональна наповненість відображення ОДІ має відповідати ролі користувача.

Інтерфейс з правами адміністратора має надавати можливості призначати права доступу до

інформації Системи іншим користувачам:

Інтерфейс з правами технолога має надавати можливості створення, редагування базових

властивостей ОДІ, видалення ОДІ з Системи та переміщення іконки ОДІ на карті.

Інтерфейс диспетчера має надавати можливості створювати/коригувати властивості ОДІ і

призначати їх режими роботи.

Під базовими властивостями ОДІ розуміється: ID № об'єкта (унікальний номер), його тип та

найменування, зображення, місцеположення ОДІ на перехресті тощо.

В межах Системи повинні існувати інтерфейси під ОДІ із певним набором сервісів (чи

еквівалент) та можливістю налаштування доступу до них згідно до ролевої моделі:

- Інтерфейс «Стрічка стану»;

- Інтерфейс «Оперативний стан»;

- Інтерфейс «Стан по ключам»;

- Інтерфейс «Режими»;

- Інтерфейс «Звіт»;

- Інтерфейс «Циклограма»;

- Інтерфейс «Диспетчер задач»;

- Інтерфейс «Параметри»;

- Інтерфейс «Модем»;

- Інтерфейс «Журнал режимів, відмов та несправностей».

Вимоги до інтерфейсу «Оперативний стан»

Інтерфейс повинен мати наступну інформацію:

- Дата/час зв'язку (дд:мм:рррр/гг:хх:сс)

- Режим роботи: № РП (Робоча програма), № Фази.

- Джерело управління (диспетчерське керування, паспортні дані, адаптивне керування тощо).

- Канал отримання команди управління (канал програмного доступу, диспетчер тощо).

- Час від початку такту, с.

- Час до кінця такту, с.

- Час несинхронізації з визначеним Денним планом.

- Друк оперативного стану ОДІ та технічного стану каналів (силових виходів).

- Апаратні та програмні індикатори:

№	Найменування індикатора	Варіанти індикації
1	Автоматичний роз'їзд	+/-
2	Проміжний такт	+/-
3	Тип дня:	робочий/вихідний
4	Стан входу дверей шафи дорожнього контролера	відкрито/закрито
5	Стан входів ТВП/ДТ (ТВП - Табло виклику пішохідне/ДТ-детектор транспорту)	+/-
6	Наявність КЗ (Коротке замкнення) в каналах керування дорожнього контролера:	+/-
7	Наявність на силових входах недозволених комбінації	+/-
8	Включений режим «Всім червоне» (Режим включення червоних сигналів світлофорів по всім напрямках руху)	+/-
9	Включений режим діагностики	+/-

10	Несправність з-за нестачі даних	+/
11	Недовантаження в каналах керування (на силових виходах)	+/
12	Є недоступні силові каналі (виходи)	+/

Вимоги до інтерфейсу «Режими»

Функціональна наповненість інтерфейсу має відповідати вимогам нижче.

Найменування опції	**Призначення**
ЖМ	Включити режим «Жовте миготіння» на необмежений проміжок часу (визначається оператором).
ВС	Включити режим «Відключення світлофорів» на необмежений проміжок часу (визначається оператором).
Відключити	Відключити обраний режим і повернутись до попереднього режиму роботи.
Встановити режим	Встановити визначений режим роботи з дата/час по дата/час.

Вимоги до інтерфейсу «Звіт»

Інтерфейс. «Звіт» має надавати можливість зберігання та друку інформації про стан ОДІ за вибраний дата/час.

Вимоги до інтерфейсу «Циклограма»

Інтерфейс «Циклограма» має надавати можливість on-line візуалізації роботи ОДІ типу «світлофор» у вигляді часової діаграми та роботи на схемі перехрестя.

Вимоги до інтерфейсу «Диспетчер задач»

Інтерфейс «Диспетчер задач» має бути призначений для періодичності виконання команд.

Найменування команди	**Діапазон**
Стан СО	Одноразова/ періодична/ статична
Інформація про силові виходи та напрямку руху	
Інформація про напругу	
Інформація про стан акумулятора резервного живлення	
Інформація про поточну температуру у шафі контролера	
Отримати РП (робоча програма)	

Отримати версію ПЗ контролера	
Встановити час	
Кількість сигналів, які підключені до одного каналу (силового виходу) контролера	
Кількість контрольованих сигналів в одному силовому каналі	
Значення одиниці навантаження	
Телефонний номер (при використанні мобільних каналів зв'язку)	
Стан рахунку	
Якість зв’язку	

Опція «Черга команд»

Найменування команди	Час створення команди	Час відправки на контролер	Статус виконання	Логін користувача	Видалення

Опція «Історія виконання команд»

Дата/час формування команди	Дата/час виконання команди	Найменування команди	Логін користувача

Вимоги до інтерфейсу налаштувань каналу зв'язку ОДІз АСКДР

Інтерфейс призначений для визначення параметрів зв'язку через канали GPRS/3G/4G.

Опції інтерфейсу:

- APN;
-IP;
- Номер порту;
- Стан рахунку за мобільний зв'язок (при його використанні);
- Модель модему;
- Номер телефону;

Вимоги до інтерфейсу «Журнал режимів, відмов та несправностей»

Інтерфейс призначений для ведення, зберігання і відображення режимів роботи, збоїв та несправностей. В журналі має визначатись таке: дата/час, режим/несправність.

Вимоги до групи інтерфейсів для управління з групами ОДІ

Система повинна мати зручний інтерфейс для об'єднання ОДІ в групи з метою подальшого групового управління (включення чи виключення).

Додаткові вимоги до інтерфейсу роботи з світлофорними об'єктами.

Вимоги до інтерфейсу режиму «Зелена Вулиця»

Для ОДІ типу «світлофор» має бути передбачений режим керування групою типу «Зелена вулиця», який має бути налаштований на включення конкретної фази регулювання на визначений час. Крім того має бути можливість відміни включеного режиму «Зелена вулиця».

Вимоги до інтерфейсу режиму «Координоване керування»

Режим «Координоване керування» це групова операція, яка призначена для збалансування початку роботу режимів ОДІ, наприклад, для «Зеленої Хвилі» ОДІ типу «світлофор».

Вимоги до інтерфейсу «Адаптивне керування»

Інтерфейс «Адаптивне керування» має застосовуватись для ОДІ типу «світлофор» для призначення і контролю параметрів адаптивного керування на світлофорному об'єкті. Інтерфейс повинен дозволяти зручне створення та редагування параметрів алгоритмів «Адаптивного керування».

Інтерфейс редагування властивостей ОДІ та редактора перехресть;

Інтерфейс має дозволяти:

- Визначати інтенсивність транспортного потоку та автоматично вибирати найбільш ефективний сценарій адаптивного управління;

- Форматувати флеш носій дорожнього контролера (ДК);

- Створювати/редагувати файли даних дорожніх контролерів;

- Визначати параметри роботи ДК;

- Визначати очікувані норми споживання силових виходів (каналів. керування) ДК;

- Визначати параметри настроювання каналу зв'язку з ДК;

- Створювати/редагувати файли ОДІ, які пов'язані з силовими виходами ДК та з логікою роботи ОДІ;

- Імпортувати графічні файли для створення макету ВДМ/перехрестя;

- Створювати/редагувати макети ділянки ВДМ / перехрестя із встановленими ОДІ. Для ОДІ типу «світлофор» додатково передбачаються створення напрямків руху, та іконок світлофорів;

- Визначати режими та добові плани роботи ОДІ;

- Визначати параметри роботи ОДІ;

- Проводити імітацію роботи ОДІ на попередньо створеному макеті ВДМ/перехресті;

- Зберігати параметри настроювання ДК та ОДІ в окремих файлах з подальшим імпорт в Систему;

- Друкувати/зберігати файли ДК та ОІ;

- Здійснювати запис файлів на флеш носій ДК.

Інтерфейс роботи з детекторами транспорту

Інтерфейс роботи з детекторами транспорту має надавати інформацію у графічному та табличному вигляді для кожної контрольованої зони кожного ОДІ про інтенсивність транспорту та затримки транспорту в контрольованій зоні. Інтерфейс (має бути пристосований для вибору періоду опитування детектора та друк вихідних результатів. Інтерфейс має дозволяти імпорт даних детекторів для дорожніх контролерів та експорт періодів опитування на дорожні контролери.

Вимоги до надійності програмного забезпечення АСКДР

ТІЗ має забезпечити можливість формування «холодних» резервних копій усіх компонентів та модулів із забезпеченням цілісності даних та можливості розгортання всіх компонентів Системи з «холодних» копій у цілісному та працездатному вигляді. Резервне копіювання даних повинно виконуватися не рідше одного разу на добу.

У разі необхідності програмне забезпечення АСКДР повинно створювати тимчасові файли, які використовуються для збереження технічної інформації, не пов'язаної з повідомленнями інтеграційних сервісів, які зберігаються в базі для тимчасових файлів.

Файли логів повинні бути доступні для читання тільки користувачам з ролями «Системний адміністратор».

Вимоги до збереження інформації в разі аварій та моніторингу системи

У разі виникнення аварійних подій або помилок у роботі АСКДР подія/помилка повинна реєструватися у відповідному електронному журналі, а адміністратор повинен отримати відповідне повідомлення із зазначенням типу події/ помилки.

До складу повідомлення щодо події аварійного типу повинні входити:

- час;
- текстова назва аварі
- код помилки та її опис.

Налаштування збереження інформації в разі аварій повинно забезпечувати такий режим роботи АСКДР:

- будь-яка операція, що виконана, повинна бути записана на основному та дублюючому сховищах даних;

- якщо будь-яка операція повністю не виконана, то інформація про таку послугу повинна доводити стан/крок виконання цієї операції.

Збереження інформації повинно бути забезпечене в разі виникнення таких подій (аварій, відмов тощо):

- відмови обладнання сервера/сховища даних;
- вимкнення живлення на робочому місці та/або на сервері баз даних;
- відмови обладнання робочої станції;
- відмови ліній зв'язку.

З метою забезпечення зберігання інформації повинні використовуватися:

- резервне копіювання;
- відновлення даних під час збоїв у роботі мережного, програмного й апаратного забезпечень.

ПЗ повинно надавати можливість онлайн-аналізу даних кожної підсистеми та кожного модуля Системи, а саме:

- лог-журнали:
- доступу;
- інтеграцій;
- помилок;
- метрики обладнання:
- завантаженість процесорів;
- стан бази даних;
- завантаженість оперативної пам'яті;
- завантаженість фізичних дисків;
- завантаженість мережних інтерфейсів;
- тощо.

АСКДР повинна надавати результати аналізу та моніторингу подій в режимі реального часу. Функції звітності повинні включати:

- загальні звіти з графіками;
- хронологія подій;
- моніторинг детекторів;
- завантаження бази даних, вивантаження і порівняльні звіти;
- інше.

Вимоги до інформаційної безпеки

Захист інформації від несанкціонованого доступу

АСКДР не повинна мати вбудовані та виконувані команди чи їх комбінації, застосування яких через помилкові дії чи зловживання можуть спричинити аварійні ситуації.

АСКДР повинна мати програмні інструменти рівня адміністратора для формування інформаційної політики, контролю інформаційного трафіку та встановлення режимів доступу до Системи для користувачів та груп користувачів, конкретних IP адрес, створення/редагування/видалення/деактивації користувачів, призначення прав.

В цілому за рівнем відповідності вимогам безпеки дані відносяться до категорії з обмеженим доступом (персональні, технологічні) - доступ до яких регулюється міжнародним та українським законодавством.

Повинні бути реалізовані такі заходи захисту початкового рівня:

- організаційно-адміністративні;

- апаратно-програмні;

- інженерно-технічні.

Під час виконання операцій з обробки інформації повинна бути забезпечена її цілісність, конфіденційність та доступність.

АСКДР повинна надавати рольовий доступ заявленим категоріям користувачів.

Для забезпечення захисту інформації від несанкціонованого доступу АСКДР повинна

забезпечити таке:

- функціональну можливість управління доступом, що забезпечує виконання таких

функцій захисту:

- створення ролей доступу з можливістю додавання персональних привілей доступу в разі необхідності до цієї ролі;
- блокування доступу у випадку виявлення порушень встановлених (правил розмежування доступу до системи;
- функціональної можливості, що передбачає обов'язкову реєстрацію:
- результатів ідентифікації користувачів та даних про точки, з яких здійснюється доступ користувача до системи (ip-адреси);
- спроб несанкціонованих дій з інформацією;
- фактів надання та позбавлення користувачів права доступу до інформації та її обробки (зміною повноважень користувачів).

Доступ користувача до веб інтерфейсу повинен мати обмеження терміну сесії авторизації.

До АСКДР висуваються вимоги із забезпечення безпеки інформації, які будуть враховані під час подальшої побудови комплексної системи захисту інформації, а саме:

- забезпечення цілісності інформації вимагає застосування технологій, що забезпечують

реалізацію контрольованого і санкціонованого доступу до інформації та заборону

неконтрольованої та несанкціонованої її модифікації, що повинно вирішуватися на рівні

операційної системи сервера, системи управління базами даних та програмного продукту;

- забезпечення здатності здійснення компонентами АСКДР первинної ідентифікації будь-яких користувачів (незареєстрованих та зареєстрованих) за IP-адресою;
- встановлення мінімальних привілеїв для користувачів під час доступу до файлів та папок (директорій) серверу застосувань, обмежених їх правом «тільки читання»;
- заборона можливості перегляду лістингу директорій та файлів серверу застосувань з Інтернету (наприклад, за допомогою конфігурування серверу застосувань);
- неприпустимість виникнення ситуації, під час якої існує можливість отримання доступу до компонента або функції АСКДР, минаючи авторизацію;

- збереження всіх файлів, що відносяться до АСКДР, в окремій структурі каталогів на рівні операційної системи і захист таких файлів;
- необхідність блокування несанкціонованих завантажень файлових об'єктів на сервер застосувань;

- можливість завантаження користувачами тільки таких документів/фалів, що необхідні для цільового використання;
- завантаження файлів до спеціально призначеної для цього директорії, запуск сценаріїв та скриптів з якої повинен бути заборонений;
- необхідність перевірки всіх даних та параметрів, що одержуються серверною частиною АСКДР через її веб інтерфейси, на відповідність типам, розмірам, допустимим діапазонам значень;
- необхідність контролю засобами АСКДР одержаної інформації на предмет відсутності шкідливого для неї програмного коду і керуючих послідовностей;
- запобігання можливості впровадження будь-якого шкідливого коду;
- механізм, що забезпечує недопущення шкідливих компонентів, повинен діяти не за принципом виключення даних, відповідних деяким зразкам або значенням, а за принципом виключення всіх даних, які не відповідають дозволеним значенням або зразкам. При цьому слід проводити перетворення службових символів у безпечний код, що забезпечує їх відображення на боці клієнта;

- визначення можливих типів помилок і механізмів обробки аварійних ситуацій;
- при виникненні помилок або аварійних ситуацій АСКДР повинна надавати

  користувачам повідомлення про це, не вказуючи при цьому жодних додаткових даних (наприклад,

  налагоджувальної інформації, дампів пам'яті тощо);

  - повідомлення про помилку не повинно містити інформацію про архітектуру і

  внутрішню структуру АСКДР;

- невідоме виключення повинно повертати загальний код помилки із мінімально

  достатнім коментуванням/описом;

- у АСКДР повинно бути забезпечено реєстрацію всіх подій, які мають безпосереднє

  відношення до безпеки, і зберігання їх у виділеній окремо від веб інтерфейсу базі даних;

- методика з тестування повинна передбачати перевірку вихідних кодів на предмет

  наявності вразливостей, що виникають при недостатній та/або некоректній фільтрації (обробці)

  вхідних даних (атаки типу JS, SQL-ін'єкцій, XSS та інші);

  - всі сценарії JavaScript, які виконуються на боці користувача, повинні знаходитись на

  сервері застосувань;

  - забороняється використовувати сценарії, які розміщені на сторонніх веб ресурсах;

  - повинен бути заблокований анонімний доступ до бази даних;

  - логічна структура бази даних повинна проектуватися з урахуванням реалізації функції

  СКБД з розмежуванням доступу до даних;

- всі паролі, що розміщуються у СКБД, повинні зберігатися у зашифрованому вигляді
- АСКДР повинна передбачати можливість резервного копіювання та відновлення системних та користувацьких даних.

Для забезпечення захисту інформації від несанкціонованого доступу в ПЗ АСКДР повинно також бути передбачено:

1. Механізми управління доступом, що забезпечують виконання таких функцій захисту:

- ідентифікація користувачів (закріплення за кожним об'єктом персонального ідентифікатора);

- автентифікація користувачів (визначення достовірності об'єкта або суб'єкта за поданим ним ідентифікатором);

- двох факторна автентифікація користувачів з адміністративними правами доступу та тих користувачів, які отримують доступ до інформації з обмеженим доступом, що застосовується під час входу в систему.

2. Механізми моніторингу, що передбачають обов'язкову реєстрацію:

- результатів ідентифікації та автентифікації користувачів;

- результатів виконання користувачем операцій з обробки інформації;

- даних про активність користувачів;

- спроб несанкціонованих дій з інформацією;

- даних щодо пристроїв користувачів та адміністраторів системи, з яких здійснюється доступ до компонентів (IP - адреса, територіальне розміщення згідно з даними IP - адреси, дані пристрою (операційна система, браузер, версії тощо);

-дій користувачів та результатів виконання користувачами операцій з обробки інформації;

- дій, пов'язаних із встановленням та зміною прав доступу;

- дій, пов'язаних із реєстрацією, видаленням та блокуванням облікових записів у Системі;

- спроб несанкціонованих дій з інформацією;

- результатів перевірки цілісності засобів захисту інформації (у випадку їх використання).

3. Механізми оповіщення, що передбачають повідомлення адміністратора системи про аномальну активність користувача в АСКДР.

4. Зберігання паролів у системі повинно забезпечуватися з використанням методів хешування з використанням модифікатора.

5. Повинен бути реалізований захист від SQL - ін'єкцій, XSS та інших атак.