

**Методичні рекомендації
щодо розробки Технічного завдання
на створення (технічну модернізацію) територіальної
автоматизованої системи централізованого оповіщення населення**

ВСТУП

Методичні рекомендації щодо розробки Технічного завдання на створення (технічну модернізацію) територіальної автоматизованої системи централізованого оповіщення населення (далі — методичні рекомендації) розроблено ДСНС України за результатами створення та проведення тестової експлуатації Дослідного зразка територіальної автоматизованої системи централізованого оповіщення.

Методичні рекомендації розроблено з метою надання методичної допомоги обласним та Київський міський держадміністраціям при розробці технічного завдання на створення (технічну модернізацію) територіальної автоматизованої системи централізованого оповіщення населення в своєму регіоні.

ТЕРМІНИ, СКОРОЧЕННЯ ТА ВИЗНАЧЕННЯ ОСНОВНИХ ПОНЯТЬ

Скорочення та умовні позначення

Скорочення, умовні позначки	Визначення
АРМ	автоматизоване робоче місце
АС	автоматизована система
АСЦО	автоматизована система централізованого оповіщення
ДСНС	Державна служба України з надзвичайних ситуацій
ЗАСЦО	загальнодержавна автоматизована система централізованого оповіщення
КЗА	комплекс засобів автоматизації
МАСЦО	місцева автоматизована система централізованого оповіщення
НТМ	Національна телекомунікаційна мережа
ОДС	оперативно-диспетчерська служба
ОКЦ	оперативно-координаційні центри
ОС	операційна система
ПЗ	програмне забезпечення
ПТК	програмно-технічний комплекс
СКБД	система керування базами даних
ТАСЦО	територіальна автоматизована система централізованого оповіщення
Технічне завдання, ТЗ	Технічне завдання на створення територіальної автоматизованої системи централізованого оповіщення
API	Прикладний програмний інтерфейс (англ. Application Programming Interface)

Терміни та визначення

У даному Технічному завданні використані терміни та визначення, встановлені:

Законом України «Про електронні комунікації»,

Законом України «Про захист інформації в інформаційно-телекомунікаційних системах»

Законом України «Про основні засади забезпечення кібербезпеки України»;
ДСТУ ISO 1087-1:2007 Термінологічна робота. Словник термінів. Частина 1.
Теорія та використання;

ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення;

ДСТУ 2230-93 Системи оброблення інформації. Взаємозв'язок відкритих систем. Базова еталонна модель. Терміни та визначення;

ДСТУ ISO/IEC 2382:2017 Інформаційні технології. Словник термінів;

ДСТУ 2860-94 Надійність техніки. Терміни та визначення;

ДСТУ 2938-94 Системи оброблення інформації. Основні поняття. Терміни та визначення;

ДСТУ 2941-94 Системи оброблення інформації. Розроблення систем. Терміни та визначення;

ДСТУ 3891:2013 Безпека у надзвичайних ситуаціях. Терміни та визначення основних понять;

ДСТУ 5034:2008 Інформація і документація. Науково-інформаційна діяльність. Терміни та визначення понять;

ДСТУ ISO 9000:2015 (ISO 9000:2015,IDT) Системи управління якістю. Основні положення та словник термінів;

ДСТУ ISO/IEC TR 10032:2012 Інформаційні технології. Еталонна модель керування даними;

ДСТУ ISO/IEC 14764:2014 Інженерія програмного забезпечення. Процеси життєвого циклу програмного забезпечення. Технічне обслуговування;

ДСТУ ISO/IEC/IEEE 15288:2016 Розроблення систем і програмного забезпечення. Процеси життєвого циклу системи;

ДСТУ ISO/IEC 17000:2007 Оцінювання відповідності. Словник термінів і загальні принципи;

ДСТУ ISO/IEC 17788:2017 Інформаційні технології. Хмарні обчислення.
Огляд та основні терміни;

ДСТУ ISO 22320:2017 Соціальна безпека. Управління у надзвичайних
ситуаціях. Вимоги щодо реагування;

ДСТУ ISO 22322:2017 Соціальна безпека. Управління у надзвичайних
ситуаціях. Методичні рекомендації щодо оповіщення населення;

ДСТУ ISO/IEC 26514:2015 Інженерія систем і програмного забезпечення.
Вимоги до дизайнерів і розробників документації користувача;

ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту.
Настанови щодо кібербезпеки;

ДСТУ ISO/IEC 27034-1:2017 Інформаційні технології. Методи захисту.
Безпека прикладних програм. Частина 1. Огляд і загальні поняття;

ДСТУ ISO/IEC 38500:2016 Інформаційні технології. Управління ІТ в
організації;

ДСТУ ISO Guide 73:2013 Керування ризиком. Словник термінів.

Інші терміни і визначення, які використовуються у Технічному завданні,
зазначено у Таблиці 1.

Таблиця 1 - Терміни та визначення

Термін	Визначення
автоматизоване робоче місце адміністратора територіальної автоматизованої системи централізованого оповіщення, АРМ адміністратора	елемент (компонент) територіальної автоматизованої системи централізованого оповіщення, а саме спеціально визначене та обладнане автоматизоване робоче місце, призначене для координації (адміністрування) усіх робіт щодо функціонування програмно-технічного комплексу територіальної автоматизованої системи централізованого оповіщення
автоматизоване робоче місце оповіщення, АРМ оповіщення	елемент (компонент) територіальної автоматизованої системи централізованого оповіщення, а саме спеціально обладнане й оснащене необхідними технічними засобами автоматизоване робоче місце, призначене для виконання функціональних обов'язків черговим персоналом пункту управління системи оповіщення та відповідальними особами щодо оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій
загальнодержавна автоматизована система централізованого оповіщення	програмно-технічний комплекс, призначений для оповіщення чергових служб центральних і місцевих органів виконавчої влади, органів управління ДСНС
засоби інформатизації	електронні обчислювальні машини, програмне, математичне, лінгвістичне та інше забезпечення, інформаційні системи або їх окремі елементи, інформаційні мережі і мережі зв'язку, що використовуються для реалізації інформаційних технологій
інтерфейс користувача автоматизованої системи; інтерфейс користувача АС	Програмні та апаратні засоби взаємодії користувача з АС (ДСТУ 2226)

Термін	Визначення
інформаційний ресурс	сукупність документів в інформаційних системах
кваліфікований електронний підпис, КЕП	кваліфікований електронний підпис – удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа
комплекс засобів автоматизації територіальної автоматизованої системи централізованого оповіщення	сукупність програмних і технічних засобів програмно-технічного комплексу територіальної автоматизованої системи централізованого оповіщення за допомогою яких забезпечується управління територіальною автоматизованою системою централізованого оповіщення
настільний застосунок, десктопний застосунок (desk application)	прикладна програма, яку можна запустити безпосередньо з АРМ оповіщення користувача для отримання сервісів територіальної автоматизованої системи централізованого оповіщення
оповіщення	доведення сигналів і повідомлень органів управління цивільного захисту про загрозу та виникнення надзвичайних ситуацій, аварій, катастроф, епідемій, пожеж тощо до центральних і місцевих органів виконавчої влади, підприємств, установ, організацій та населення
прикладне програмне забезпечення; (application software) прикладна програма; застосунок; (application program)	програмне забезпечення чи програма, призначені для розв'язання прикладної проблеми
система оповіщення	комплекс організаційно-технічних заходів, апаратури і технічних засобів оповіщення, апаратури, засобів та каналів зв'язку, призначених для своєчасного

Термін	Визначення
	доведення сигналів та інформації про виникнення надзвичайних ситуацій до центральних і місцевих органів виконавчої влади, підприємств, установ, організацій та населення
територіальна автоматизована система централізованого оповіщення	програмно-технічний комплекс, призначений для оповіщення осіб керівного складу і чергових служб відповідних місцевих органів виконавчої влади, органів місцевого самоврядування, а також населення через місцеві автоматизовані системи централізованого оповіщення та інші системи оповіщення
технічні засоби телекомунікацій	обладнання, станційні та лінійні споруди, призначені для утворення телекомунікаційних мереж

1 ЗАГАЛЬНІ ВІДОМОСТІ

1.1. Повне найменування системи та її умовне позначення

Повне найменування: Територіальна автоматизована система централізованого оповіщення _____ області.

Скорочена назва: ТАСЦО.

Умовне позначення: Система.

1.2. Найменування підприємств замовника і розробника системи та їх реквізити

Замовник: _____

Виконавець: _____

1.3. Підстави для проведення робіт зі створення (технічної модернізації) ТАСЦО

Розробка даного технічного завдання виконана згідно:

Плану заходів щодо реалізації Концепції розвитку та технічної модернізації системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій, затвердженого розпорядженням Кабінету Міністрів України від 11 липня 2018 р. № 488-р;

Концепції розвитку та технічної модернізації системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій, схваленої розпорядженням Кабінету Міністрів України від 31 січня 2018 р. № 43-р (далі – Концепція);

Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту, затвердженого постановою Кабінету Міністрів України від 27 вересня 2017 р. № 733 (далі – Положення);

Інструкції щодо практик чи процедур проектування, дослідження, введення в експлуатацію, експлуатації та технічного обслуговування (супроводження) автоматизованих систем централізованого оповіщення затвердженою наказом Міністерства внутрішніх справ України від 08 лютого 2019 року №93, зареєстрованим в Міністерстві юстиції України 22 квітня 2019 року за № 418/33389 (далі – Інструкція).

Технічних вимог на створення (технічну модернізацію) територіальної автоматизованої системи централізованого оповіщення _____ області, затверджених _____ .

1.4. Планові терміни початку та закінчення надання Послуг

Початок робіт: «_____» _____ 20__ р.

Закінчення робіт: «_____» _____ 20__ р.

Терміни виконання етапів (процесів) реалізації проекту визначаються згідно плану заходів щодо реалізації Концепції розвитку та технічної модернізації системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій, затвердженого розпорядженням Кабінету Міністрів України від 11 липня 2018 року № 488-р.

1.5. Відомості про джерела і порядок фінансування послуг

Розробка Системи фінансується за рахунок коштів _____ та інших не заборонених законодавством джерел фінансування.

1.6. Порядок оформлення та пред'явлення Виконавцем Замовнику результатів робіт зі створення (технічної модернізації) ТАСЦО

Порядок виконання проєктних робіт зі створення (технічної модернізації) ТАСЦО здійснюється згідно чинного законодавства України, відповідно до вимог нормативно-правових та нормативно-технічних документів та зазначених у даному Технічному завданні національних стандартів.

Проєктні роботи виконуються поетапно відповідно до ДСТУ ISO/IEC/IEEE 15288:2016 (ISO/IEC/IEEE 15288:2015,IDT) та ДСТУ ISO/IEC TR 24748-2. Етапність та перелік робіт відповідних етапів визначаються календарним планом керування проєктом відповідно до ДСТУ ISO/IEC/IEEE 16326, ДСТУ ISO/IEC/IEEE 24748-4.

Календарний план керування проєктом та порядок пред'явлення Виконавцем до прийняття Замовником результатів виконання кожного етапу робіт (відповідні звітні документи) визначаються договором на виконання проєктних робіт.

2 ПРИЗНАЧЕННЯ ТА ЦІЛІ СТВОРЕННЯ ТАСЦО

2.1. Призначення ТАСЦО

Основним призначенням Системи є виконання наступних функцій:

1) прийому сигналів про загрозу виникнення або виникнення надзвичайних ситуацій державного рівня та інформації з питань цивільного захисту в загальнодержавній автоматизованій системі централізованого оповіщення (далі – ЗАСЦО);

2) оповіщення в автоматизованому режимі та забезпечення доведення сигналів про загрозу виникнення або виникнення надзвичайних ситуацій державного і регіонального рівнів та інформації з питань цивільного захисту відповідно до Положення про оповіщення та Положення про Систему:

членів регіональної комісії з питань техногенно-екологічної безпеки і надзвичайних ситуацій;

регіональну комісію з питань евакуації;

осіб керівного складу і чергових служб територіальних спеціалізованих служб цивільного захисту регіонального рівня;

рятувальну водолазну службу _____ області;

територіальні формування обласного підпорядкування;

районні державні адміністрації _____ області (далі – РДА);

міські, селищні, сільські ради територіальних громад _____ області (далі – ТГ);

населення області через місцеві автоматизовані системи централізованого оповіщення (далі – МАСЦО), системи зв'язку мобільних операторів та радіохвилі і ефірні телеканали, які охоплюють значну частину _____ області.

2.2. Мета проведення технічної модернізації ТАСЦО

Головною метою технічної модернізації Системи є реалізація автоматизації функцій оповіщення існуючої автоматизованої системи централізованого оповіщення «Сигнал-ВО» та її переоснащення сучасними програмно-технічними засобами з використанням новітніх інформаційних технологій та технологій електронних комунікацій.

Модернізація системи має забезпечити:

цифровізацію процесів оповіщення місцевих органів виконавчої влади, органів місцевого самоврядування, а також населення області;

доведення сигналів про загрозу виникнення або виникнення надзвичайних ситуацій територіального рівня та інформації з питань цивільного захисту відповідно до Положення про Систему;

оновлення морально застарілих технологій обробки і передачі інформації в Системі;

автоматичну або автоматизовану інформаційну взаємодію між елементами Системи із ЗАСЦО та автоматизованими системами централізованого оповіщення (далі – АСЦО) всіх рівнів, а також з автоматизованими системами раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення в разі їх виникнення, якими обладнуються об'єкти підвищеної небезпеки;

кібербезпеку, відсутність впливу та можливостей втручання у роботу Системи.

Модернізована Система має поступово замінити систему оповіщення, яка була створена за командно-сигнальним принципом в умовах глобального воєнного протистояння в 70 – 80-х роках минулого століття та орієнтована на доведення сигналів оповіщення лише в особливий період.

3 ХАРАКТЕРИСТИКИ ОБ'ЄКТІВ АВТОМАТИЗАЦІЇ ТАСЦО

3.1. Короткі відомості про об'єкти автоматизації або посилання на документи, що мають таку інформацію

Оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій організовується з урахуванням структури державного управління в Україні, максимально прогнозованого характеру і рівня надзвичайних ситуацій. Оповіщення може здійснюватися як централізовано, так і децентралізовано.

За рівнями системи оповіщення поділяються на загальнодержавну автоматизовану систему централізованого оповіщення, територіальні автоматизовані системи централізованого оповіщення, місцеві автоматизовані системи централізованого оповіщення, а також спеціальні, локальні та об'єктові системи оповіщення.

ТАСЦО функціонують в Автономній Республіці Крим, областях, мм. Києві та Севастополі для забезпечення прийому сигналів та інформації від ЗАСЦО, оповіщення осіб керівного складу місцевих органів виконавчої влади, а також органів місцевого самоврядування, підприємств, установ, організацій, органів

управління та сил цивільного захисту і населення через МАСЦО та інші системи оповіщення у разі загрози виникнення або виникнення надзвичайних ситуацій.

ТАСЦО передбачають взаємодію із ЗАСЦО, а також місцевими автоматизованими системами централізованого оповіщення, локальними, спеціальними і об'єктовими системами оповіщення та забезпечують централізоване (повне або вибіркоче) включення відповідних місцевих автоматизованих систем централізованого оповіщення.

З метою організації взаємодії систем оповіщення у ланці ЗАСЦО – ТАСЦО – МАСЦО для своєчасного доведення сигналів та інформації про загрозу виникнення або виникнення надзвичайних ситуацій до органів управління та сил цивільного захисту, підприємств, установ та організацій де функціонують спеціальні, локальні або об'єктові системи оповіщення у тому числі населення технологічно ТАСЦО може включати інструменти та інформаційні технології, що забезпечують централізоване або вибіркоче застосування/виконання функцій систем інших ланок.

Доведення сигналів, повідомлень про загрозу виникнення або виникнення надзвичайних ситуацій до населення, а також забезпечення інформування може здійснюватися:

через АТ «НСТУ», державні і публічні телерадіокомпанії, комунальні, громадські та інші телерадіоорганізації незалежно від форми власності з використанням їх телемереж та мереж ефірного радіомовлення (із супроводженням інформації жестовою мовою та/або субтитруванням, якщо вона є голосовою, і аудіокоментуванням, якщо вона є візуальною);

через операторів телекомунікацій (мобільного зв'язку), цифрового радіозв'язку із залученням телекомунікаційних мереж загального користування (телефонний зв'язок, текстові повідомлення (СBS, SMS, MMS, MBMS, E-mail МТ тощо);

через Інтернет-ресурси (сайти, соціальні мережі).

Для передачі сигналів та повідомлень оповіщення використовуються сигнально-гучномовні пристрої, у тому числі встановлені на транспортних засобах, що залучаються для оповіщення, електронні інформаційні табло, електросирени та інші технічні засоби.

Рішення про оповіщення у разі загрози виникнення або виникнення надзвичайної ситуації на обласному рівні приймає Голова _____ обласної держадміністрації.

На державному рівні оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій у _____ області здійснюється оперативно-черговою

службою на основному або запасному пунктах управління системою оповіщення (далі – ПУСО) Державної служби України з надзвичайних ситуацій (далі — ДСНС).

Відповідно до ДСТУ 2226-93 об'єкт автоматизації це сукупність функцій людини чи людино-машинного комплексу, що підлягають автоматизації.

Враховуючи завдання визначені пунктом 7 Положення про Систему до її об'єктів автоматизації відносяться:

основний та запасний пункти управління системою оповіщення (далі – ПУСО) ОДА;

оперативно-координаційний центр (далі – ОКЦ) головного управління Державної служби України з надзвичайних ситуацій в _____ області (далі – ГУ ДСНС);

оперативно-чергові (чергові, оперативно-диспетчерські, диспетчерські) служби територіальних підрозділів центральних органів виконавчої влади в _____ області та військових формувань сектору безпеки й оборони;

оперативно-чергові (чергові) служби РДА та міських, селищних, сільських рад ТГ;

МАСЦО районів та ТГ _____ області;

диспетчерські служби об'єктів підвищеної небезпеки _____ області (далі – ОПН), зона ураження від яких при виникненні аварії виходить за межі однієї ТГ, та їхні локальні системи оповіщення (далі – ЛСО);

телерадіостудії, мережі трансляція яких охоплюють територію _____ області.

3.2. Відомості про умови експлуатації об'єктів автоматизації та характеристики навколишнього середовища

Створення (модернізація) Системи має передбачати розгортання апаратних, програмних та апаратно-програмних засобів, які автоматизують процеси взаємодії Системи із ЗАСЦО, іншими АСЦО, кінцевими пристроями оповіщення про виникнення надзвичайних ситуацій, а також забезпечать кіберзахист всіх елементів Системи.

Для місцевих органів виконавчої влади та органів місцевого самоврядування _____ області Система має стати базисом при проектуванні та впровадженні ними власних МАСЦО.

Система для забезпечення взаємодії із ЗАСЦО, АСЦО нижчих рівнів, іншими системами оповіщення та інформаційно-телекомунікаційними системами (далі – ІТС) повинна мати уніфікований програмний прикладний інтерфейс (Application Programming Interface – API) з використанням відкритого формату обміну даними прикладного рівня, зокрема відповідно до ДСТУ ISO/TR 22351.

На об'єктах автоматизації Системи мають забезпечуватися наступні умови експлуатації:

установка та монтаж технічного обладнання Системи повинні виконуватись спеціально підготовленими спеціалістами відповідно до технічного проекту на розміщення обладнання;

комплекс засобів автоматизації (далі – КЗА) Системи на всіх стадіях розробки та впровадження має супроводжуватися зусиллями спеціалістів Замовника та Виконавця робіт із залученням у разі необхідності спеціальних підрядчиків;

умови розміщення технічних засобів Системи в робочих приміщеннях Замовника повинні бути визначені Замовником та узгоджені з Виконавцем;

розміщення технічних засобів Системи в робочих приміщеннях Замовника має здійснюватися у відповідності з паспортними вимогами до умов експлуатації цих технічних засобів;

має забезпечуватися дотримання вимог техніки безпеки при роботі із технічними засобами Системи;

має забезпечуватися дотримання вимог відповідних нормативно-методичних документів з охорони праці.

Експлуатація Системи має здійснюватися спеціалістами на основі автоматизованих робочих місць (далі – АРМ), створених на базі персональних електронно-обчислювальних машин (далі – ПЕОМ), і відповідати умовам експлуатації цих ПЕОМ. В штатному режимі Система забезпечує обробку даних згідно регламенту функціонування.

Експлуатація елементів Системи, які розташовані в опалювальних приміщеннях, має задовольняти наступним вимогам:

температура повітря: від +15°C до +40°C;

відносна вологість при 25°C: від 40% до 80%.

Додаткові вимоги до умов експлуатації визначаються залежно від місця розташування конкретного елемента Системи.

В режимі технічного обслуговування забезпечується технічне обслуговування та відновлення технічних засобів Системи (обробка даних не здійснюється).

Технічне обслуговування та ремонт технічних засобів Системи мають здійснюватися силами організацій, на які покладено технічний супровід апаратних засобів Замовника.

КЗА Системи повинен враховувати ті обчислювальні та комунікаційні засоби, що вже функціонують у складі систем Замовника.

Технічні засоби повинні складатися тільки з компонентів, що випускаються серійно і мають відповідні показники надійності, що наведені у технічних паспортах обладнання.

З метою своєчасного діагностування технічного стану Система повинна мати в своєму складі компоненти постійного моніторингу за станом Системи із обов'язковим веденням системного журналу, здійснювати постійне автоматичне відстеження стану підключень до Системи.

Система енергопостачання має забезпечувати надходження електроенергії, при якій гарантується працездатність Системи у всіх режимах роботи.

Електроенергією Системи має забезпечуватися від промислової мережі змінного струму напругою 220 В, частотою 50 Гц.

Технічні засоби Системи повинні функціонувати при змінах напруги 220 плюс 10 % мінус 15 % і частотою 50 Гц + 1%.

Якість, гарантованість та безперерійність енергопостачання забезпечується відповідними службами Замовника.

4 ВИМОГИ ДО ТАСЦО

4.1. Вимоги до Системи в цілому

Організаційно-технічні і технологічні основи Системи мають формуватися з врахуванням наступних загальних вимог:

забезпечення вертикальної інтеграції наявних та створюваних інформаційних ресурсів АСЦО;

дотримання єдності організаційних, технічних та технологічних принципів побудови АСЦО;

суворе дотримання міжнародних та національних стандартів в області цивільного захисту населення;

забезпечення інформаційної безпеки та захисту інформації від несанкціонованого доступу;

використання модульного принципу при проектуванні програмних комплексів обробки інформації і робочих місць користувачів Системи;

використання сертифікованих програмно-технічних рішень та уніфікованих компонентів функціонуючих АСЦО.

Система має забезпечити ефективне використання сучасних інформаційних технологій, сприяти підвищенню оперативності в опрацюванні інформації, поліпшення взаємодії між суб'єктами інформаційної діяльності.

Якісними показниками ефективності Системи мають бути:

поліпшення якості та прискорення виконання процесів обміну інформацією про сигнали оповіщення;

оптимізація потоків даних між АСЦО всіх рівнів;

підвищення рівня захищеності при роботі з інформацією.

Кожен користувач Системи повинен обмежуватися сферою його функціональної діяльності згідно з посадовими інструкціями. Дозвіл на роботу та повноваження користувачів мають визначатися згідно з правилами Системи.

Система не має бути прив'язана до конкретного комп'ютерного, периферійного, мережевого чи іншого обладнання, кількості робочих місць.

КЗА Системи повинен забезпечувати передачу інформації.

Система повинна будуватись таким чином, щоб допускати поетапне створення і впровадження в експлуатацію окремих складових частин, забезпечувати обмін даними з існуючими інформаційними системами.

Всі дії користувачів (включаючи адміністраторів) при роботі в Системі мають автоматично фіксуватися в спеціальних системних журналах, що захищені від модифікації. Передбачена можливість перегляду означених журналів в розрізі кожного користувача за будь-який період часу (оперативно, за певний календарний термін тощо).

Архітектура Системи будується на основі концепції "відкритих систем", і тому має бути відкритою для включення нових МАСЦО та АСЦО нижчого рівня.

В основу створення Системи має бути покладений увесь досвід інформаційної діяльності, накопичений на різних рівнях: державному, галузевому, а також новітні досягнення у сфері наукових розробок і технологій.

Обов'язковою умовою модернізації існуючої системи оповіщення є розробка бібліотек (програмних модулів) спеціалізованого програмного забезпечення для забезпечення інформаційної взаємодії з іншими АСЦО, а також інтеграції з існуючими системами оповіщення та інформування.

Система модернізується у рамках Концепції розвитку та технічної модернізації системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій, схваленої розпорядженням Кабінету Міністрів України від 31 січня 2018 року № 43-р та Технічних вимог до загальнодержавної автоматизованої системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій, затверджених наказом Міністерства внутрішніх справ від 05 листопада 2018 р. №884.

4.1.1. Вимоги до структури та функціонування автоматизованої системи

Архітектура Системи має організаційну та функціональну складові, що визначаються ознаками розподілу за призначенням об'єктів автоматизації та функціональних елементів Системи.

Організаційна складова Системи має об'єкти автоматизації, які визначені у пункті 3.1 цього Технічного завдання та зазначена на рисунку 4.1.

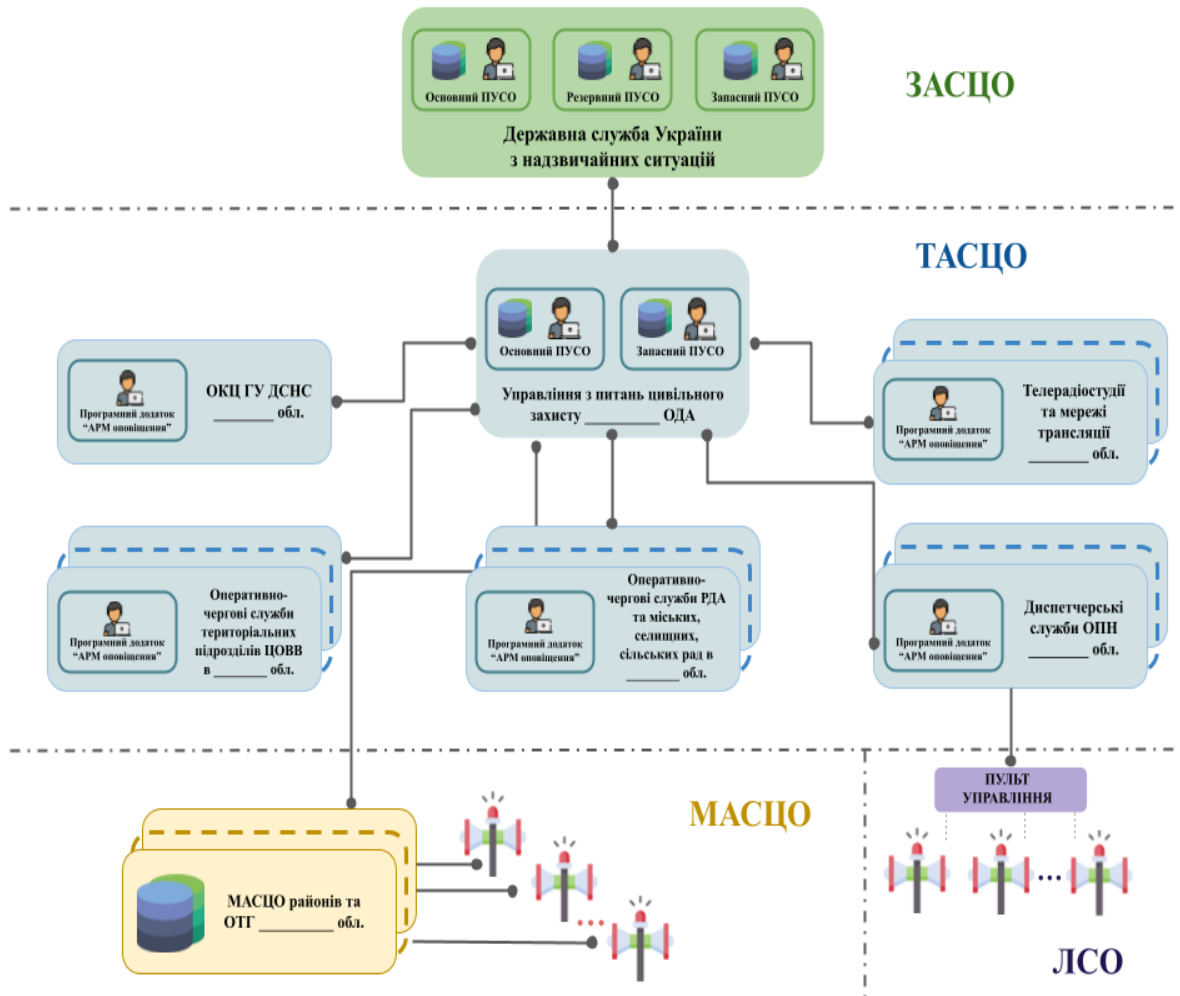


Рис. 4.1. Організаційна складова ТАСЦО

Елементами функціональної складової архітектури Системи, які забезпечують виконання нею основних функцій, є:

основний та запасний КЗА – сукупність програмних і технічних засобів ТАСЦО _____ області, за допомогою яких забезпечується управління нею;

АРМ адміністраторів – спеціально визначене та створене на базі персонально електронно-обчислювальної машини автоматизоване робоче місце, яке призначене для координації (адміністрування) усіх робіт щодо функціонування ТАСЦО _____ області, а також управління кібербезпекою та формування політик безпеки в ній;

АРМ оповіщення – спеціально визначене та створене на базі персонально електронно-обчислювальної машини автоматизоване робоче місце зі встановленим програмним додатком користувачького спеціалізованого програмного забезпечення оповіщення, яке призначене для виконання функціональних обов'язків черговим персоналом та відповідальними особами пунктів управління системою оповіщення _____ обласної державної адміністрації, оперативно-координаційного центру Головного управління Державної служби України з надзвичайних ситуацій в _____ області, оперативно-чергових (чергових, оперативно-диспетчерських, диспетчерських) служб територіальних підрозділів центральних органів виконавчої влади, оперативно-чергових (чергових) служб районних державних адміністрацій та територіальних громад, диспетчерських служб об'єктів підвищеної небезпеки та телерадіостудій _____ області щодо оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій;

користувачьке спеціалізоване програмне забезпечення оповіщення (далі - КСПЗ) – користувачьке програмне забезпечення, яке встановлюється на спеціально обладнані й оснащені необхідними технічними засобами АРМ оповіщення;

бібліотека спеціалізованого програмного забезпечення оповіщення (далі – СПЗ) – програмний модуль, який через уніфікований прикладний програмний інтерфейс забезпечує інформаційну взаємодію (інтеграцію) ТАСЦО _____ області із АСЦО інших рівнів, зовнішніми автоматизованими системами та кінцевими пристроями оповіщення;

апаратно-програмні засоби доступу до Системи (далі – АПЗД) – спеціалізовані технічні засоби, які забезпечують взаємодію ТАСЦО _____ області із її кінцевими пристроями оповіщення, а також пристрої переключення радіохвиль, телеканалів та існуючих гучномовних систем;

кінцеві пристрої оповіщення (далі – КПО) – технічні засоби, які через апаратно-програмні засоби доступу до ТАСЦО _____ області забезпечують доведення сигналів і повідомлень про загрозу або виникнення надзвичайних ситуацій, аварій, катастроф, епідемій, пожеж тощо до підприємств, установ, організацій та населення _____ області;

кінцеве обладнання взаємодії (далі – КОВ) – кінцеве обладнання системи міжвідомчого телефонного зв'язку (технічні засоби телефонного та відеозв'язку);

4.1.1.1. Вимоги до способів та засобів зв'язку для інформаційного обміну між компонентами автоматизованої системи

Електронна комунікаційна інфраструктура Системи в першу чергу має розгортатися на базі ресурсу територіально розподіленої транспортної платформи Національної телекомунікаційної мережі (далі – ТП НТМ). У разі відсутності ресурсів ТП НТМ задіюються ресурси електронних комунікаційних мереж загального користування або мережі Інтернет.

4.1.1.2. Вимоги до характеристик взаємозв'язків автоматизованої системи, що створюється, з суміжними автоматизованими системами, вимоги до її сумісності, у тому числі зазначення способу обміну інформацією (автоматично, пересилання документів, по телефону тощо)

Для організації взаємозв'язків Системи та ЗАСЦО необхідно використовувати бібліотеки спеціалізованого програмного забезпечення, що реалізують інформаційну взаємодію з дотриманням єдиного формату повідомлень, структура яких визначена ДСТУ ISO/TR 22351:2017 (ISO/TR 22351:2015, IDT) «Соціальна безпека. Управління у надзвичайних ситуаціях. Структура сповіщень для обміну інформацією».

Для організації автоматизованих взаємозв'язків Системи та інших АСЦО, автоматизованих систем раннього виявлення загрози виникнення надзвичайних ситуацій необхідно використовувати програмні або апаратно-програмні засоби доступу до ТАСЦО, які використовують бібліотеки спеціалізованого програмного забезпечення, що реалізують інформаційну взаємодію з дотриманням єдиного формату повідомлень, структура яких визначена ДСТУ ISO/TR 22351:2017 (ISO/TR 22351:2015, IDT) «Соціальна безпека. Управління у надзвичайних ситуаціях. Структура сповіщень для обміну інформацією».

4.1.1.3. Вимоги до режимів функціонування автоматизованої системи

Експлуатація Системи повинна передбачати режими роботи визначені пунктом 2 розділу III Інструкції щодо проектування АСЦО.

4.1.1.4. Вимоги по діагностуванню автоматизованої системи

Моніторинг та контроль стану елементів Системи повинен бути реалізований за наступними критеріями:

- повна готовність виконання покладених функцій;
- обмежена здатність виконання покладених функцій;
- збій або відмова.

Виконання цих критеріїв має забезпечуватися функціоналом СПЗ Системи, який надає користувачам інструменти моніторингу основних процесів виконання покладених на Систему функцій.

Компоненти інструментів моніторингу повинні мати зручний інтерфейс для можливості перегляду діагностичних подій, моніторингу процесу виконання оповіщення, передавання результатів діагностування і можливість виводу їх на друк.

При виникненні збоїв або помилок у Системі, інструменти моніторингу повинні мати можливість зберігати повний набір інформації, необхідної користувачеві і розробникові для ідентифікації проблеми (знімки екранів, коди помилок або збоїв, поточний стан пам'яті та файлової системи програмних засобів).

Компоненти інструментів моніторингу мають передбачати можливість виявлення непрацездатності власних технічних та програмних засобів, які входять до складу елементів (компонентів) Системи та засобів інформаційного обміну, сумісності і взаємодії.

4.1.1.5. Перспективи розвитку автоматизованої системи

СПЗ має реалізовувати можливість розвитку чи модернізації Системи без зміни програмних модулів (бібліотек) за рахунок незалежності відображення даних на концептуальному, програмному та фізичному рівнях.

4.1.2. Вимоги до чисельності та кваліфікації персоналу ТАСЦО та режиму його роботи

Кожна особа, яка входить до складу персоналу Системи, має застосовувати відповідні інформаційні моделі, працювати з технічними засобами Системи та документацією на неї.

4.1.2.1. Вимоги до чисельності персоналу (користувачів) автоматизованої системи

Модернізована Системи має зменшити кількість неавтоматизованих функцій оповіщення та створити передумови скорочення персоналу, який обслуговує системи оповіщення старого парку.

При цьому, в Системі необхідно передбачити категорії користувачів та їх профілі доступу, які визначені підпунктами 4) та 5) пункту 6 розділу II Інструкції щодо проектування АСЦО.

4.1.2.2. Вимоги до кваліфікації персоналу, порядку його підготовки та контролю знань та навичок

Кваліфікація персоналу Системи повинна забезпечувати її ефективне функціонування у всі заданих режимах. Для отримання необхідних навичок персонал Системи має бути підготовлений до виконання своїх обов'язків у відповідності до керівництва з експлуатації Системи.

Інструктажі (навчання) спеціалістів Замовника щодо навиків роботи із відповідними складовими частинами та СПЗ Системи здійснює Виконавець на стадії впровадження Системи в дослідну експлуатацію згідно із узгодженим обома сторонами Планом інструктажів (навчання).

4.1.2.3. Вимоги до режиму роботи персоналу

Режими роботи персоналу, який забезпечує функціонування Системи, мають бути визначені відповідними відомчими нормативно-правовими документами Замовника.

4.1.3. Показники призначення

Система має реалізовувати показники призначення виконання основних функцій щодо:

- автоматичного або автоматизованого приймання, передавання в реальному масштабі часу та реєстрації вхідної та вихідної інформації;

- автоматичного підтвердження прийому інформації (повідомлень, сигналів, команд, даних, документів) щодо оповіщення про загрозу або виникнення надзвичайних ситуацій від пунктів управління системами оповіщення у будь-якому напрямку оповіщення;

- документування (протоколювання) вхідної та вихідної інформації, подій усіх процесів оповіщення та дій користувачів Системи з можливістю формування друкованих звітів;

- впровадження єдиної інформаційної бази (бази даних) Системи для автоматизованого або автоматичного приймання (передавання) формалізованої інформації (даних, документів) щодо оповіщення та/або інформаційної взаємодії;

- циркулярного, циркулярного за задалегідь встановленими сценаріями, вибіркового або за пріоритетом передавання інформації за призначенням щодо оповіщення;

- інформаційної взаємодії між об'єктами автоматизації Системи;

- інформаційної взаємодії з АСЦО всіх рівнів;

- керування КПО через АПЗД;

- автоматичного моніторингу та контролю (діагностики) стану програмних та технічних засобів Системи;

впровадження багаторівневого доступу згідно встановлених пріоритетів і прав доступу в Системі;

впровадження технічних і програмних засобів із забезпеченням інформаційної безпеки інформаційних та мережевих ресурсів Системи.

4.1.4. Вимоги до надійності

Модернізація Системи повинна передбачати вимоги до стійкості її роботи, які визначені підпунктом 2) пункту 1 розділу II Інструкції щодо проектування АСЦО та є достатніми для досягнення встановлених цілей функціонування Системи, де забезпечені нормальні кліматичні умови:

температура повітря: від +15°C до +40°C;

відносна вологість при 25°C: від 40% до 80%.

атмосферний тиск від 84 до 107 кПа (від 630 до 800 мм рт. ст.).

4.1.5. Вимоги до безпеки

Вимоги до безпеки мають бути визначені в експлуатаційних документах та забезпечуватися при наладці, експлуатації і ремонті технічних засобів Системи.

З'єднувальні електричні кабелі на об'єктах автоматизації Системи мають бути змонтовані так, щоб уникнути можливості випадкового порушення електричних ланцюгів при експлуатації.

Технічні засоби Системи не повинні мати відкрито розміщених елементів, що знаходяться під напругою 5В і вище.

Приміщення, у яких розміщуються технічні засоби Системи, мають бути оснащені протипожежною сигналізацією типу, дозволеного до використання у міністерствах та відомствах.

Під час монтажу, наладки, експлуатації, обслуговування та ремонту технічних засобів Системи повинні виконуватись усі вимоги правил техніки безпеки та правил установки та експлуатації електрообладнання.

4.1.6. Вимоги до ергономіки та технічної естетики

Основна взаємодія персоналу, що обслуговує технічні засоби з програмним забезпеченням, які входять до складу Системи повинна здійснюється за допомогою інтерфейсу командного рядка (CLI) та вбудованих візуально-графічних WEB-інтерфейсів.

Система має забезпечувати коректну обробку аварійних ситуацій, викликаних неправильними діями персоналу, невірним форматом або недопустимими значеннями вхідних даних. У зазначених випадках Система видає користувачу відповідні повідомлення, після чого повертається у робочий стан, що

був до вводу невірної (неприпустимої) команди чи некоректного вводу даних, або взагалі не приймає до виконання невірні команди, що можуть призвести до непередбачуваного стану функціонування Системи.

Під час модернізації Системи мають бути враховані вимоги та рекомендації до ергономіки та технічної естетики КСПЗ наступних національних стандартів:

ДСТУ 7245 (вимоги до кодування зорової інформації);

ДСТУ 7299 (вимоги до розміщення засобів відображення інформації);

ДСТУ 8604 (вимоги до робочих місць для виконання робіт у положенні сидячи);

ДСТУ ISO 9241-8 (вимоги до кольорів тексту та графічних зображень на екрані дисплея);

ДСТУ ISO 9241-13 (вимоги до керівництва користувача в меню інтерфейсу користувача прикладних програм);

ДСТУ ІЕС 60073 (вимоги до певних візуальних, звукових і тактильних сигналів).

4.1.7. Вимоги до експлуатації, технічного обслуговування, ремонту та зберігання

Склад Системи має бути достатнім для виконання всіх автоматизованих функцій в ній.

Всі технічні засоби Системи мають бути засобами серійного виробництва. Технічні засоби, які будуть використовуватися для модернізації Системи, повинні відповідати вимогам державних технічних регламентів:

Технічного регламенту низьковольтного електричного обладнання, затвердженого постановою Кабінету Міністрів України від 16 грудня 2015 р. № 1067;

Технічного регламенту з електромагнітної сумісності обладнання, затвердженого постановою Кабінету Міністрів України від 16 грудня 2015 р. № 1077.

Технічні засоби Системи мають встановлюватися з дотриманням вимог, що містяться в технічній, у тому числі експлуатаційній документації на них, і так, щоб було зручно використовувати їх при функціонуванні Системи та виконувати технічне обслуговування.

Розміщення технічних засобів Системи, що використовуються персоналом при виконанні автоматизованих функцій, має відповідати вимогам ергономіки:

ДСТУ 7299 (вимоги до розміщення засобів відображення інформації);

ДСТУ 8604 (вимоги до робочих місць для виконання робіт у положенні сидячи);.

Технічні засоби Системи, що будуть використовуватися при взаємодії з іншими АСЦО, мають бути сумісні за інтерфейсами з відповідними технічними засобами цих систем та систем зв'язку.

В модернізованій Системі технічні засоби повинні мати термін служби, який визначений підпунктом 3) пункту 1 розділу II Інструкції щодо проектування АСЦО та становити не менше ніж десять років.

Будь-який із технічних засобів Системи має передбачати можливість заміни його засобом аналогічного функціонального призначення без будь-яких конструктивних змін або регулювання в інших технічних засобах Системи.

Технічні засоби Системи можуть використовуватися лише за умов, визначених в експлуатаційній документації на них.

4.1.8. Вимоги до захисту інформації від несанкціонованого доступу

Захист інформаційних ресурсів та функцій Системи має передбачати:

- запобігання несанкціонованого використання інформації баз даних;
- запобігання несанкціонованого внесення змін або знищення баз даних;
- розмежування доступу користувачів до інформації, яка вимагає захисту від несанкціонованого внесення змін або знищення баз даних;
- забезпечення контролю за діями користувачів та реєстрації подій, які мають відношення до безпеки інформації;
- документування спроб несанкціонованого доступу оперативного з видачою попереджувального повідомлення — «Спроба несанкціонованого доступу»;
- надійне забезпечення цілісності інформації, що обробляється в Системі;
- віддалене керування технічними засобами Системи із захищеною передачею (криптографічний захист) керуючих посилки (SSH, SNMP, HTTPS).

Доступ до функцій прикладних програм та інформації у Системі повинен надаватися лише авторизованим користувачам з урахуванням їх службових повноважень, а також, з урахуванням категорії інформації, яка запитується. Спроби модифікації чи знищення інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора, повинні блокуватися.

Модернізація Системи має передбачати створення рівнів доступу користувачів, які визначений підпунктом 4) пункту 6 розділу II Інструкції щодо проектування АСЦО.

4.1.9. Вимоги до збереження інформації при аваріях

Модернізація Системи має передбачати:

захист від хибних дій користувача – помилки у діях персоналу не призводять до відмов (збоїв) у роботі;

контроль за вхідною та вихідною інформацією;

регламентований час відновлення після відмови (збою).

Збереження інформації має проводитися при настанні наступних подій:

збій або відмова технічних засобів (зокрема процесорів, накопичувачів на жорстких дисках);

збій або відключення електроживлення;

відмова каналів обміну даними;

збій або відмова операційної системи;

збій або відмова прикладних програм.

СПЗ Системи має автоматично дублювати та резервувати дані, а також відновлювати своє функціонування при коректному перезапуску технічних засобів із збереженням всіх даних.

При попаданні або відключенні електроживлення технічних засобів Системи, які призводять до перезавантаження операційної системи та СПЗ Системи, має відбуватися відновлення даних конфігурацій СПЗ Системи без їх втрати.

Для відновлення даних і СПЗ Системи з резервних копій повинні використовуватися засоби автоматичного та/або ручного резервного копіювання й архівації.

Для скорочення об'єму копійованих даних має бути передбачено копіювання лише змін, які виникли, починаючи з моменту попереднього копіювання.

Періодичність копіювання даних повинно складати не менше ніж один раз на добу.

Також має бути передбачена можливість відновлення даних за допомогою їх повторного введення або імпорту (для даних із зовнішніх систем, що отримуються автоматично).

4.1.10. Вимоги до захисту від зовнішніх впливів

Проектні рішення розташування та захисту технічних (ПЕОМ, лінії живлення, канали зв'язку між ПЕОМ) та програмних засобів мають враховувати відсутність впливу наявних у зоні експлуатації електричних та магнітних полів, можливі перешкоди у колах електроживлення і звичайні природні атмосферні явища.

4.1.11. Вимоги до патентної чистоти

Технічні та програмні засоби Системи повинні мати законне походження, а їх використання не повинно спричинити порушення будь-яких авторських та/або патентних прав.

4.1.12. Вимоги до стандартизації та уніфікації

Технічні рішення щодо модернізації Системи повинні базуватися на логічній моделі комунікаційного середовища ISO 7498.

Для проведення модернізації Системи у проектних рішеннях при виборі варіантів реалізації перевага надається стандартизованим рішенням (тобто тим, які пройшли процедуру стандартизації і затверджені або рекомендовані державними або відомчими нормативними документами).

Програмні та технічні засоби Системи мають бути сумісні програмно, та мати загальний API для вводу-виводу даних, забезпечувати єдину структуру даних, базуватися на єдиних схемних, конструктивних та програмно-технічних рішеннях з максимальним використанням уніфікованих елементів.

У Системі має бути забезпечена взаємозамінюваність за призначенням уніфікованих програмних засобів та змінних одностипних виробів, компонентів, модулів.

4.1.13. Додаткові вимоги

Додаткові вимоги до Системи не висуваються.

4.2. Вимоги до функцій (задач), що виконуються автоматизованою системою

В Системі мають бути реалізовані такі функції:

1) автоматизоване гарантоване оповіщення осіб керівного складу місцевих органів виконавчої влади, органів місцевого самоврядування та населення, а також підприємств, установ і організацій незалежно від форми власності на території _____ області, доведення до громадян сигналів цивільного захисту;

2) автоматизоване доведення до населення _____ області у визначеному районі оповіщення попереджувальних сигналів небезпеки «УВАГА ВСІМ!»;

3) автоматизоване приймання, передавання в реальному масштабі часу та реєстрація вхідної і вихідної інформації;

4) автоматизоване підтвердження прийому інформації (повідомлень, сигналів, команд, даних, документів) щодо оповіщення та інформування населення _____ області про загрозу виникнення або виникнення надзвичайних ситуацій від пунктів управління в будь-якому напрямку оповіщення;

5) документування (протоколювання) вхідної та вихідної інформації, подій, усіх процесів оповіщення та інформування населення _____ області та дій користувачів Системи з можливістю формування друкованих звітів;

6) автоматизована обробка, приймання (передавання) формалізованої інформації (даних, документів) єдиної інформаційної бази даних Системи щодо оповіщення та інформування населення _____ області;

7) інформаційна взаємодія між об'єктами автоматизації Системи, взаємодія через уніфікований API Системи з АСЦО всіх рівнів та з іншими автоматизованими системами, що відносяться до територіальної підсистеми єдиної державної системи цивільного захисту;

8) циркулярне, циркулярне за завчасно визначеними сценаріями, вибіркоче або за пріоритетом передавання інформації щодо оповіщення та інформування населення _____ області;

9) оперативне інформування населення _____ області через мережі операторів мобільного зв'язку України, у тому числі:

автоматизоване створення повідомлення інформування населення _____ області на базі параметрів (даних) сформованих в картці надзвичайної ситуації;

формування повідомлення у форматі, з яким працює уніфікований API;

редагування тексту повідомлення інформування населення _____ області з урахуванням обмежень по його довжині, як на кирилиці так і латиниці;

вибір терміновості повідомлення інформування населення _____ області;

контроль за результатами оперативного інформування населення _____ області через мережі операторів мобільного зв'язку України;

10) керування КПО через АПЗД;

11) автоматичний моніторинг та контроль (діагностика) стану КПО та контроль доступності АПЗД;

12) автоматизоване створення та передавання в реальному масштабі часу сигналів та/або файлів формалізованих звукових повідомлень на КПО;

13) графічне відображення на мапі зони дії оголошених в Системі надзвичайних ситуацій у тому числі у адміністративно — територіальних регіонах інших АСЦО;

14) багаторівневий доступ користувачам Системи згідно встановлених пріоритетів і прав доступу до її інформаційних ресурсів.

4.3. Вимоги до видів забезпечення

4.3.1. Вимоги до математичного забезпечення

Математичне забезпечення СПЗ Системи має бути реалізовано з урахуванням таких критеріїв як універсальність, алгоритмічна надійність, точність та економічність.

Математичне забезпечення СПЗ Системи має включати такі основні алгоритми:

приймання та обробку достовірної інформації (зокрема сигналів, команд, розпоряджень, повідомлень, документів) про загрозу виникнення або виникнення надзвичайних ситуацій від будь-яких джерел інформації;

формування, маршрутизацію та відображення інформації на відповідних АРМ Системи для приймання (підготовки) рішень щодо оповіщення населення про загрозу виникнення або виникнення надзвичайних ситуацій та контролю за результативністю їх виконання;

інформаційної взаємодії між складовими частинами Системи та іншими АСЦО.

Всі алгоритми мають бути працездатними за будь-яких допустимих значень вхідної інформації та інформації, що обробляється.

4.3.2. Вимоги до інформаційного забезпечення

Інформаційне забезпечення Системи має бути достатнім для виконання всіх її автоматизованих функцій. Під інформаційним забезпеченням слід формі достовірної інформації (у вигляді послідовності символів, букв, цифр, розуміти сукупність відображеної у формалізованому вигляді або у заданій передавання цієї інформації з метою аналізу одержаних результатів, графіків, таблиць, документів, повідомлень, довільних текстів, картографічних зображень тощо) для збору, зберігання, опрацювання і підготовки, обґрунтування і прийняття управлінських рішень органами управління цивільного захисту _____ області щодо оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та контролю за результативністю їх виконання.

Інформаційне забезпечення має передбачати:

спадкоємність щодо використання накопиченої інформації у Системі;

мінімізацію вірогідності дублювання по введенню (прийому) і накопиченню даних в інформаційній базі даних;

високу ефективність алгоритмів, методів і засобів збору, обробки, зберігання, накопичення, оновлення, пошуку і надання інформації;

простоту та зручність доступу до інформації;

перетворення вхідної інформації у цифрову форму, якомога ближче до місця її здобуття;

перетворення вихідної інформації з цифрової форми у фізичну форму, якомога ближче до місця її використання;

захист від недостовірної і несанкціонованої інформації, а також захист визначених користувачів від зайвої непотрібної інформації;

завадостійке кодування та захист інформації від руйнування й несанкціонованого доступу;

регламентацію доступу до інформаційних даних з різним рівнем доступу, а також часу зберігання задокументованої інформації.

4.3.2.1. Вимоги до складу, структури та способу обробки даних у автоматизованій системі

В Системі має оброблятися інформація про надзвичайні ситуації, яка описує: режим, в якому здійснюється оповіщення про загрозу виникнення або виникнення надзвичайної ситуації;

терміновість повідомлення про загрозу виникнення або виникнення надзвичайної ситуації;

місце виникнення (зона дії) надзвичайної ситуації;

класифікацію надзвичайної ситуації згідно з ДК 019:2010;

класифікаційний рівень надзвичайної ситуації;

прогноз розвитку надзвичайної ситуації;

об'єкти, які створюють загрозу;

назву організації, яка є автором повідомлення про загрозу виникнення або виникнення надзвичайної ситуації;

дату та час виникнення (загрози виникнення) надзвичайної ситуації;

дату та час евакуації (можливої евакуації);

додатковий опис місцевості (об'єктів);

команди, сигнали або інструкції щодо дії внаслідок виникнення (загрози виникнення) надзвичайної ситуації;

алгоритм дій ОЧС/ОДС, які оповіщаються, про загрозу виникнення або виникнення надзвичайної ситуації;

додаткова інформація про загрозу виникнення або виникнення надзвичайної ситуації, яка може передаватися Системою у вигляді файлів;

облікові та технічні данні підключених КСПЗ (АРМ оповіщення), АСЦО та АПЗД (КПО);

облікові дані користувачів Системи;

заздалегідь підготовлені списки оповіщення;

текст повідомлення для оповіщення через систему оперативного інформування населення через мережі операторів мобільного зв'язку України (далі - COI);

пріоритет текстового повідомлення для оповіщення через COI.

Також, в Системі обробляється інформація щодо звукових файлів, які відтворюються на КПО для оповіщення населення _____ області.

Окремий вид інформації, що обробляється в Системі, це технологічна інформація про всі події в Системі та дії її користувачів. Технологічна інформація формується Системою автоматично та зберігається у журналі реєстрації подій.

4.3.2.2. Вимоги до інформаційного обміну між компонентами автоматизованої системи

Інформаційний обмін між компонентами Системи повинен здійснюватися через єдину транспортну інфраструктуру із забезпеченням резервування створених каналів передавання даних.

4.3.2.3. Вимоги до інформаційної сумісності зі суміжними автоматизованими системами

Інформаційна сумісність Системи зі суміжними автоматизованими системами має бути реалізована через уніфіковані API СПЗ.

Для взаємодії із АСЦО всіх рівнів в уніфікованому API СПЗ Системи необхідно впровадити єдиний формат повідомлень, структура яких визначена ДСТУ ISO/TR 22351:2017 (ISO/TR 22351:2015, IDT) «Соціальна безпека. Управління у надзвичайних ситуаціях. Структура сповіщень для обміну інформацією».

В Системі також має бути впроваджений уніфікований API СПЗ для взаємодії з COI.

4.3.2.4. Вимоги до загальнодержавних, галузевих класифікаторів, уніфікованих документів та класифікаторів

Для кодування інформації, яка використовується лише в даній Системі, повинні застосовуватися класифікатори, прийняті у Замовника.

Для кодування в Системі вихідної інформації, яка використовується на вищому рівні, мають бути застосовані класифікатори ЗАСЦО.

4.3.2.5. Вимоги до застосування автоматизованої системи управління базами даних

В Системі має бути впроваджена відкрита об'єктно-реляційна система керування базами даних (далі - СКБД), яка дозволяє використовувати та змінювати її для реалізації задач Системи.

4.3.2.6. Вимоги до захисту даних від руйнації при аваріях та збоях в електроживленні автоматизованої системи

Для захисту даних в Системі має бути реалізований процес реплікації даних на двох серверах основного (запасного) КЗА Системи.

4.3.2.7. Вимоги до контролю, збереження, поновлення та відновлення даних

Контроль, збереження, поновлення та відновлення даних в Системі щодо облікових даних користувачів, технічних параметрів елементів Системи, шаблонів оповіщення тощо мають здійснювати її адміністратори.

4.3.2.8. Вимоги до процедури надання юридичної сили документам, технічним засобам, які продукуються автоматизованою системою

В Системі має бути передбачена можливість формування виписки про дії її користувачів, які потім можуть бути використані у якості доказових матеріалів у службових розслідуваннях щодо порушення порядку та вимог оповіщення про загрозу виникнення або виникнення надзвичайної ситуації.

4.3.3. Вимоги до лінгвістичного забезпечення

Під лінгвістичним забезпеченням слід розуміти порядок вживання мов програмування та інформаційних мов (визначення даних, маніпулювання даними, запитів, взаємодії користувачів і прикладних програм).

Для розробки прикладних програм пріоритет має надаватися мовам програмування (програмного коду) високого рівня (зокрема, C#, Java, JavaScript).

Налаштування прикладних програм при доопрацюванні, зміни переліку та структури вхідної й вихідної інформації не має викликати необхідності зміни програмного коду.

Інформаційні мови повинні включати:

мову взаємодії користувачів Системи і КСПЗ;

мову визначення даних – формальна мова, що використовується для визначення структури баз даних та є засобом формального опису концептуальних і логічних структур баз даних;

мову управління даними – сукупність засобів мови для організації доступу до даних у моделі даних, що використовується, а також у відповідних їй СКБД;

мову запитів – сукупність засобів мови користувачів КСПЗ, які дозволяють задовольнити інформаційні потреби без додаткового програмування.

Мовою взаємодії користувачів Системи та КСПЗ є державна українська мова (виняток можуть становити лише системні повідомлення загального СПЗ (ОС, СКБД, програм-утиліт).

4.3.4. Вимоги до програмного забезпечення

Програмне забезпечення Системи має базуватися на сервіс-орієнтованій архітектурі та об'єктно-реляційній моделі СКБД, яка заснована на підході до проектування систем і розробки програмного забезпечення з точки зору сервісних послуг (ДСТУ ISO/IEC 18384-1, ДСТУ ISO/IEC 18384-2).

4.3.4.1. Перелік програмних засобів, що закупляються

До переліку програмних засобів Системи, що закупляються можуть входити операційні системи, програмне забезпечення віртуалізації та управління серверами, програмне забезпечення реалізації відеостіни, а також СПЗ, яке реалізовує автоматизацію визначених цим Технічним завданням функцій Системи.

4.3.4.2. Вимоги до незалежності програмних засобів від операційних систем, що використовуються

Програмні модулі (бібліотеки) СПЗ Системи, які входять до її складу не повинні:

- мати ділянок коду, що викликають появу рекурентних циклів або статичних витоків пам'яті;

- викликати системних помилок, що призводять до часткового або повного виходу з ладу прикладних програм або технічних засобів.

Елементи програмного коду, що здійснюють обробку даних за стандартними алгоритмами, мають бути скомпоновані у вигляді окремих бібліотек, окрім критичних до швидкості виконання ділянок коду.

СПЗ повинно дозволяти реалізовувати можливість розвитку чи модернізації Системи без зміни програмних модулів (бібліотек) за рахунок незалежності відображення даних на концептуальному, програмному та фізичному рівнях.

4.3.4.3. Вимоги до якості програмних засобів, а також до способів його забезпечення та контролю

Якість СПЗ Системи має забезпечувати надійність обчислювального процесу з можливістю автоматичного діагностування збоїв, переривання різних видів тощо.

Якість функціональної та експлуатаційної надійності СПЗ забезпечуватися належними інформаційним, математичним має та лінгвістичним забезпеченнями.

4.3.5. Вимоги до технічного забезпечення

В Системі має бути забезпечено надійне функціонування всіх технічних засобів та унеможливлення несанкціонованого доступу до них.

Для Системи технічні засоби повинні постачатися у варіанті для монтажу у стійках (Rack Mount) для монтажу або серверних шафах також типу Rack Mount.

Для технічних засобів, які не призначені для монтажу в серверних шафах, мають бути передбачені полиці, які дозволяють їх монтаж у серверних шафах типу Rack Mount.

Технічні засоби, які застосовуються у Системі, мають враховувати не тільки нормальні умови експлуатації, а й імовірні порушення цих умов, можливі несправності, неправильне використання та зовнішні чинники, що впливають на експлуатацію, такі як температура, висота, забруднення, вологість, перенапруги в мережі живлення та перенапруги в мережах електронних комунікацій або в системі кабельного розподілу.

Розміри ізоляційних відстаней повинні враховувати можливі зменшення допусків під час виготовлення або там, де можливі деформації, що можуть виникнути в разі оброблення, ударів і вібрацій, імовірних зіткнень у процесі виробництва, транспортування або нормальної експлуатації.

Система має забезпечувати високу ступінь готовності з відсутністю єдиних точок відмови для критичних, з точки зору функціонування Системи, елементів.

В Системі має бути реалізована відмовостійкість за рахунок дублювання і резервування каналів (ліній) зв'язку, критичних для роботи Системи в цілому програмних, програмно-апаратних та апаратних засобів.

Технічні засоби Системи повинні мати можливість швидкого відновлення працездатності шляхом заміни елементів, що вийшли з ладу.

Технічні засоби Системи повинні мати необхідну кількість інтерфейсів для підключення резервних каналів (ліній) зв'язку.

Технічні засоби Системи повинні мати можливість збереження конфігураційних файлів, протоколювання внесених змін в конфігураційні файли, можливість швидкого повернення до попередньої версії конфігураційних файлів.

У разі виходу з ладу основного КЗА перемикавання на запасний КЗА і зворотне перемикавання після відновлення повинне здійснюватися в автоматичному режимі.

Для розгортання КЗА Системи Замовник надає інженерну інфраструктуру об'єктів з системою гарантованого електроживлення, яка забезпечує надійний захист від непередбачуваних збоїв з урахуванням індивідуальних особливостей об'єктів. Час автономної роботи Системи повинен бути не менше ніж 0,5 години.

Система повинна мати можливість подальшого розширення як кількісного (робочі місця, структурні підрозділи), так і якісного (кількість АСЦО та КПО, що підключаються). Розширення Системи не має призводити до суттєвих змін у раніше встановлених налаштуваннях обладнання.

З'єднання АРМ адміністраторів та користувачів ОЧС ПУСО ОДА Системи з КЗА будуть організовані засобами автоматизованих локальних обчислювальних мереж, які розгорнуті на об'єктах ПУСО.

4.3.6. Вимоги до метрологічного забезпечення

В Системі мають бути впроваджені функції моніторингу (контролю за станом) її технічних засобів та алгоритмічних процесів, які будуть забезпечувати визначення з потрібною точністю характеристик технічних засобів та параметрів алгоритмічних процесів.

Метрологічне забезпечення в Системі має охоплювати всі стадії життєвого циклу, починаючи з етапу введення даних в Систему:

- аналіз коректності введених даних;

- встановлення раціональної номенклатури вимірювальних величин та використання засобів вимірювання належної точності;

- здійснення періодичних перевірок працездатності технічних засобів та алгоритмічних процесів Системи щодо сигналів оповіщення (тестові сигнали оповіщення);

- постійний контроль черговими службами за станом технічних засобів та алгоритмічних процесів Системи.

4.3.7. Вимоги до організаційного забезпечення

Організаційне забезпечення в Системі визначається як сукупність методів та засобів, які регламентують взаємодію фахівців Замовника з її технічними засобами та СПЗ.

На етапі постачання та впровадження разом з технічними засобами та СПЗ Системи постачальник надає експлуатаційну документацію на кожен окремий виріб КЗА, а також інструкції користувачів СПЗ Системи за кожним профілем, інструкції по інсталяції програмних засобів.

Для підготовки фахівців Замовника постачальник або інтегратор проводять первинні інструктажі (навчання) з питань технічної експлуатації технічних засобів та СПЗ Системи.

4.3.8. Вимоги до методичного забезпечення

На етапі введення в експлуатацію та промислової експлуатації Системи Замовник організовує методичне забезпечення навчання та перевірку кваліфікації персоналу.

Для цього Замовник затверджує Типове положення з урахуванням специфіки сфери цивільного захисту та вимог нормативно-правових актів, розробляє і затверджує відповідні функціональні обов'язки працівників Замовника з питань забезпечення функціонування Системи, а також формує плани-графіки проведення інструктажів (навчання) та перевірки знань з питань забезпечення функціонування Системи, з якими мають бути ознайомлені працівники.

Первинні інструктажі (навчання) працівників УЦЗ ОДА здійснює за рахунок Замовника організація, яка займається постачанням технічних засобів та СПЗ Системи.

5. СКЛАД ТА ЗМІСТ РОБІТ З ТЕХНІЧНОЇ МОДЕРНІЗАЦІЇ ТАСЦО

Виконавець має передбачити участь у робочій групі всіх необхідних для роботи над створенням та впровадженням Системи фахівців з боку Виконавця та Замовника і подати їх перелік. Розподіл відповідальності, опис рівнів ескалації проблем та інші елементи організації робіт мають бути включені до договору на модернізацію Системи.

Роботи з технічної модернізації Системи мають розділятися на чотири етапи:
проектні роботи;
впровадження проекту;
впровадження комплексної системи захисту інформації (далі — КСЗІ) на Систему;
проведення дослідної експлуатації Системи.

Мета першого етапу – провести аналіз існуючих технічних рішень щодо автоматизації процесів оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та визначити економічно обґрунтований варіант реалізації технічної модернізації Системи.

При проектуванні технічної модернізації Системи слід враховувати, що процеси, її функції і завдання мають бути пов'язані між собою та визначені їх

взаємозв'язки із процесами, функціями та завданнями існуючої загальнодержавної автоматизованої системи централізованого оповіщення.

Програмно-технічні (зокрема, алгоритми, структури і формати даних тощо) та організаційні (регламенти, вимоги, інструкції, обмеження тощо) проєктні рішення, що реалізуються під час експлуатації і супроводу Системи (визначені у проєктній та експлуатаційній документації згідно цього Технічного завдання) мають бути передані Замовнику Розробником (Постачальником) у вигляді, достатньому для їхнього незалежного використання (без звернення до Розробника та/або Постачальника).

Реалізація програмно-технічних проєктних рішень без визначеної вище технічної документації не допускається.

Проєктні рішення з технічної модернізації Системи повинні задовольняти вимогам щодо реалізації та дотриманням таких основних принципів і критеріїв, а саме:

задоволеності Замовника – сприйняття Замовником ступеня виконання його вимог та очікувань відповідно до ДСТУ ISO 10001;

гарантування якості проєктних рішень – наявність підтверджувальної документації від Розробника (Постачальника) для доведення відповідності проєктних рішень встановленим вимогам цього Технічного завдання відповідно до ДСТУ ISO/IEC 17050-1, ДСТУ ISO/IEC 17050-2;

відповідальності – документованого призначення відповідальних осіб зацікавлених сторін щодо реалізації таких процесів:

підготовки цього Технічного завдання,

проєктування (планування і керування проєктом, підготовки проєктних рішень і проєктної документації),

контролю за виконанням проєкту (плану керування проєктом), підготовкою проєктної документації і процесом верифікації;

стандартизації – заходи з планування, керування і контролю процесу проєктування з технічної модернізації Системи повинні відповідати нормативно-правовим актам, вимогам і рекомендаціям національних стандартів: ДСТУ ISO/IEC/IEEE 15288 та ДСТУ ISO/IEC/IEEE 16326;

безперервності і спадкоємності (технологічність, модульність і масштабованість програмних і технічних засобів), а саме:

розроблення і вдосконалення функцій має забезпечувати можливість подальшого розвитку системи з використанням сучасних вискоелективних інформаційних технологій і програмно-технічних засобів разом із забезпеченням захисту початкових вкладень фінансових, матеріально-технічних та трудових ресурсів,

застосування єдиної для всієї системи технології створення, поновлення, збереження і використання інформаційних ресурсів, у тому числі одноразове введення і оброблення даних при забезпеченні їх багаторазового використання,

проєктування функцій системи з позиції системного аналізу, об'єктно-орієнтованого підходу та концепції створення єдиної інформаційної бази даних;

відкритості та інформаційної сумісності (інтеграції з іншими інформаційними системами):

відкритість має забезпечуватися можливістю нарощування технічних засобів системи, поновлення й розширення її функцій відповідно до її розвитку без порушення функціонування та кардинальної зміни її структури і складу,

інформаційна сумісність має бути організована на основі стандартів взаємозв'язку відкритих систем відповідно до встановлених протоколів обміну даними, правил і регламентів для забезпечення інформаційної взаємодії;

інформаційної безпеки – забезпечення необхідного рівня конфіденційності, кіберзахисту, цілісності, доступності, автентичності та достовірності інформації і ефективності технічного захисту інформаційного ресурсу системи від втрат, спотворення, руйнування та несанкціонованого використання;

мобільності (здатності до адаптації, простотавзаємозамінність) – забезпечення результативності та встановлення, ефективності перенесення системи, програмного продукту або компонента з однієї апаратної, програмної чи іншої експлуатаційної платформи (використовуваного середовища) на іншу (інше);

ефективності – вибір проєктних (програмних, технічних) рішень з технічної модернізації Системи повинен забезпечувати мінімізацію нових вкладень фінансових, матеріально-технічних та трудових ресурсів.

Мета другого етапу – впровадити визначений проєктом варіант реалізації технічної модернізації Системи.

Другий етап завершується попередніми випробуваннями Системи, мета та заходи яких полягають у забезпеченні об'єктивних доказів того, що обласна ТАСЦО дійсно виконує задані вимоги і функції за призначенням, а також гарантуванні того, що система побудована відповідно до ДСТУ ISO/IEC/IEEE 15288:2016 та вирішені всі питання щодо можливості приймання Замовником обласної ТАСЦО в дослідну експлуатацію.

Мета третього етапу – визначити вимоги до функціонального профілю захищеності Системи, а також порядку їх впровадження та створення КСЗІ на Систему.

Мета четвертого етапу – проведення дослідної експлуатації Системи, під час якої відпрацьовуються всі можливі сценарії функціонування Системи в різних

режимах, а також здійснюється перевірка захищеності Системи до зовнішніх та внутрішніх впливів.

Термін реалізації першого етапу – не більше ніж п'ять місяці з моменту підписання договору на розробку проєкту з технічної модернізації Системи.

Термін реалізації другого етапу – не більше ніж шість місяців з моменту завершення першого етапу.

Термін реалізації третього етапу – не більше ніж п'ять місяців з моменту завершення першого етапу.

Термін реалізації четвертого етапу – не більше ніж три місяці з моменту завершення другого етапу.

Примітка: Терміни та склад кожного етапу є орієнтовними і можуть бути уточнені до підписання договору.

Визначені цим Технічним завданням вимоги є обов'язковими. У процесі технічного проєктування до даного Технічного завдання можуть бути внесені зміни, уточнення та доповнення, які обґрунтовуються та оформлюються окремим документом та затверджуються таким же чином, як дане технічне завдання.

6. ПОРЯДОК КОНТРОЛЮ ТА ПРИЙМАННЯ ТАСЦО

Заходи щодо планування, оцінки та контролю виконання робіт з технічної модернізації Системи повинні виконуватися відповідно до ДСТУ ISO/IEC/IEEE 16326 та ДСТУ ISO/IEC/IEEE 24748-4.

6.1. Планування технічної модернізації Системи

Мета процесу планування технічної модернізації Системи – підготовка ефективного досяжного для реалізації Плану виконання робіт з технічної модернізації Системи. Даний процес визначає сферу управління технічною модернізацією Системи та технічну діяльність, визначає результати процесу, завдання технічної модернізації Системи та кінцеві результати, встановлює графіки виконання завдань технічної модернізації Системи, включаючи критерії досягнення мети і необхідні ресурси для виконання завдань технічної модернізації Системи.

План виконання робіт з технічної модернізації Системи готується Розробником проєкту та погоджується із Замовником. План виконання робіт з технічної модернізації Системи має містити таку інформацію:

- номери та найменування етапів робіт з технічної модернізації Системи;
- перелік робіт, які будуть виконуватися для проведення технічної модернізації Системи та строки їх виконання;
- кінцевий результат за кожним видом робіт з технічної модернізації Системи.

6.2. Оцінка та контроль виконаних робіт технічної модернізації Системи

Основною метою оцінки та контролю виконаних робіт з технічної модернізації Системи є визначення статусу виконання технічної модернізації Системи та забезпечення його виконання відповідно до планів та графіків в рамках прогнозованих бюджетів для задоволення завдань з технічної модернізації Системи.

Даний процес також визначає заходи та дії щодо виправлення відхилень від Плану виконання робіт з технічної модернізації Системи та запобігання повторенню проблем, виявлених під час виконання Проєкту.

В рамках впровадження Системи має бути передбачено проведення випробувань та дослідної експлуатації.

Контроль за виконанням робіт здійснюється Замовником.

Приймання Системи здійснюється комісією Замовника, до якої можуть бути залучені представники організацій, які проводили поставку, монтаж та налагодження як окремих елементів Системи так і Системи в цілому.

Виконані етапи роботи з технічної модернізації Системи приймаються Замовником, який призначає комісію своїм наказом.

Підсумковим документом роботи комісії є Акт приймання етапу виконаної роботи, що затверджується Замовником.

Попередні випробування та дослідна експлуатація здійснюються на об'єктах автоматизації, що визначені Замовником. Порядок організації проведення випробувань та дослідної експлуатації визначається окремо.

За результатами приймання етапів роботи, у разі необхідності, Виконавець складає План-графік заходів по усуненню недоліків та рекомендації, які затверджуються Замовником.

7. ВИМОГИ ДО ЗМІСТУ РОБІТ З ПІДГОТОВКИ ОБ'ЄКТІВ АВТОМАТИЗАЦІЇ СИСТЕМИ ДО ВВЕДЕННЯ В ЕКСПЛУАТАЦІЮ

7.1. Перелік технічних й організаційних заходів

Для створення умов функціонування об'єкта автоматизації, за яких гарантується відповідність Системи вимогам, що містяться в цьому Технічному завданні, і можливості ефективного використання Системи, в організації Замовника

на стадії робіт «Підготовка об'єкта автоматизації до введення Системи в дію» має бути проведений комплекс технічних і організаційних заходів, а саме:

- підготовка приміщень для розміщення Системи;
- заходи щодо організаційного забезпечення роботи Системи;
- первинне налаштування Системи;
- первинне наповнення Системи інформацією;
- контроль і випробування Системи;
- передача Виконавцем Замовнику всіх системних логінів і паролів;
- заходи щодо інструктажу персоналу.

7.2. Підготовка приміщень для розміщення Системи

В термін до початку проведення пусконаладжувальних робіт Замовник здійснює підготовку відповідних приміщень для розміщення Системи відповідно до вимог Виконавця.

7.3. Організаційне забезпечення роботи Системи

Організаційне забезпечення Системи має бути достатнім для ефективного виконання користувачами обов'язків при здійсненні автоматизованих та пов'язаних з ними неавтоматизованих функцій керування процесом оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій.

Замовником мають бути визначені посадові особи, відповідальні за наступні функції:

- обробку інформації в Системі;
- адміністрування Системи;
- забезпечення безпеки інформації Системи;
- управління роботою персоналу з обслуговування Системи.

Замовником має бути проведений комплекс організаційних заходів щодо забезпечення роботи Системи.

Для підтримки функціонування Системи в цілому рекомендується створення необхідних структурних підрозділів відповідно до вимог, викладених у проєктній документації.

Виконавець повинен надати Замовнику Програму інструктажу персоналу і План дослідної експлуатації Системи.

Зміни в організаційній структурі підрозділів, складі робочих місць та посадових інструкціях персоналу, який бере участь у дослідній експлуатації Системи, мають бути розроблені Замовником відповідно до робочої документації на Систему та затвердженої Програми дослідної експлуатації в термін до початку дослідної експлуатації.

Силами Замовника в термін до початку проведення пусконаладжувальних робіт мають бути вирішені організаційні питання забезпечення доступності інформаційних джерел зовнішніх організацій, перелік яких визначається в процесі технічного проектування Системи.

Силами Замовника в термін до початку дослідної експлуатації мають бути видані і затверджені регламентні, директивні та розпорядчі документи, що встановлюють порядок взаємодії підрозділів Замовника при роботі Системи.

7.4. Первинне налаштування Системи

Замовник надає Виконавцю сервери та технічні засоби Системи для встановлення і налаштування операційних систем, СКБД та СПЗ згідно з вимогами Техноробочого проекту.

Виконавець здійснює встановлення базового програмного забезпечення (операційних систем, СКБД тощо) та СПЗ.

7.5. Первинне наповнення Системи інформацією

На основі наданих Замовником інформаційних матеріалів Виконавець готує інформаційне наповнення Системи в обсязі, достатньому для того, щоб Замовник міг самостійно продовжити наповнення Системи.

Подальше наповнення Системи інформацією здійснюється силами Замовника.

7.6. Передача Системи в експлуатацію

В рамках передачі Системи в промислову експлуатацію організація, яка здійснює постачання технічних засобів та СПЗ Системи, повинна надати комплект експлуатаційної документації, що включає в себе:

настанову з процедури початкового налаштування Системи (первинна процедура налаштування системи здійснюється силами Виконавця і повинна повністю відповідати настанові, тобто бути відтворюваною по крокам, які прописані в настанові);

настанову з початкового наповнення Системи інформацією (первинна процедура наповнення Системи інформацією виконується силами Виконавця і повинна повністю відповідати настанові, тобто бути відтворюваною по крокам, які прописані в настанові; даний посібник може бути об'єднано з попереднім в один документ);

настанову адміністратора безпеки (в цьому посібнику мають бути описані всі основні процедури адміністрування параметрів кібербезпеки Системи та реєстрації користувачів, АСЦО та КПО, а також параметрів підключення до СОІ);

настанову системного адміністратора (в цьому посібнику мають бути описані всі основні процедури адміністрування Системи з посиланнями на оригінальні системні настанови, що поставляються компанією- розробником СПЗ);

настанову користувача (в цьому посібнику мають бути описані всі основні процедури роботи в Системі);

опис складу, призначення і паролів всіх системних логінів, зареєстрованих в Системі до моменту передачі її Замовнику. Після приймання та перевірки працездатності всіх системних логінів, відповідальні співробітники Замовника повинні змінити паролі всіх логінів.

Інші документи, що надаються Замовнику при передачі Системи, наведені в розділі 8 цього Технічного завдання.

Приймання Системи в дослідну експлуатацію здійснюється на підставі демонстрації заявлених функцій Системи за узгодженою програмою і методикою випробувань.

Приймання Системи в дослідну експлуатацію супроводжується підписанням Протоколу приймання і оформленням Акта введення Системи в дослідну експлуатацію.

Замовник повинен забезпечити проведення дослідної експлуатації Системи на реальному обсязі даних.

В процесі дослідної експлуатації Замовник повинен дотримуватися умов проведення дослідної експлуатації, зазначених в Акті введення Системи в дослідну експлуатацію, вести журнал зауважень та пропозицій (форма і регламент роботи розробляється Замовником). Виконавцем мають бути розділені зауваження до заявлених функцій Системи від інших зауважень і пропозицій.

Зауваження до заявлених функцій Системи, виявлені на етапі дослідної експлуатації, мають бути усунені Виконавцем в узгоджені із Замовником терміни.

Після усунення Виконавцем зауважень до заявлених функцій Системи має бути підготовлений Акт про завершення дослідної експлуатації.

7.7. Вимоги до інструктажу персоналу

7.7.1. Процес інструктажу користувачів

Рішення про проведення інструктажу та вибір типу інструктажу (інструктаж всіх користувачів в повному обсязі, інструктаж частини користувачів в дистанційному режимі, інструктаж в режимі консультацій, тощо) має бути прийняте до початку процесу тестування Системи. У ці ж терміни має бути прийняте рішення про процес інструктажу адміністраторів Системи.

Відповідальними за ухвалення даного рішення є керівники проекту від

організації, яка здійснює постачання технічних засобів і СПЗ Системи, та Замовника.

Інструктаж користувачів та адміністраторів проводиться організацією, яка здійснює постачання технічних засобів і СПЗ Системи.

Передбачається наступна організація процесу інструктажу:

у ході технічної модернізації Системи створюється документація користувача та адміністратора Системи. Крім того, створюється комплект матеріалів для проведення інструктажу (презентації);

одночасно з технічною модернізацією Системи відокремлюється група користувачів, що формується з підрозділу, в якому відбувається впровадження Системи, виділяється як мінімум один ключовий користувач;

у разі розподіленого розміщення підрозділів ключові користувачі повинні обиратися із врахуванням можливості надання ними консультації користувачам з урахуванням географічної віддаленості;

ключові користувачі повинні володіти необхідними навичками для швидкого засвоєння принципів роботи з Системою і надання необхідної підтримки іншим користувачам Системи;

на період дослідної та на початку постійної експлуатації ключові користувачі повинні мати можливість витратити близько 30% робочого часу для надання консультацій.

Після формування групи ключових користувачів проводиться їх інструктаж протягом 2-3 днів (у зв'язку з можливим завантаженням ключових користувачів передбачається проведення інструктажу без відриву їх від виробництва). За результатами інструктажу ключових користувачів проводиться корекція документації та навчальних матеріалів.

Інструктаж проводиться для всіх потенційних користувачів Системи.

Час навчання користувачів – близько 0,5 дня. З метою оптимізації витрат робочого часу інструктаж проводиться по групах.

7.7.2. Процес інструктажу адміністраторів

Процес інструктажу адміністраторів Системи проводиться окремо від процесу інструктажу користувачів в навчальному центрі Замовника.

Терміни інструктажу, а також кількість учнів і програми їх інструктажу узгоджуються Замовником та Виконавцем.

8. ВИМОГИ ДО ДОКУМЕНТАЦІЇ

8.1. Загальні положення

Зміни до затвердженого Технічного завдання та іншої документації Системи, необхідність внесення яких виявлено в процесі виконання робіт, оформлюються окремим доповненням до них, яке погоджується у порядку погодження Технічного завдання та іншої документації Системи.

Доповнення до даного Технічного завдання та іншої документації Системи, складається з вступної частини та розділів (підрозділів), до яких вносяться зміни. У вступній частині зазначається причина випуску доповнення. У розділах (підрозділах), до яких вносяться зміни, наводяться їх номери та зміст змін, а також номери та зміст нових пунктів та/ч и таких, що скасовуються.

8.2. Перелік документів

Вся документація, що розробляється в рамках технічної модернізації Системи, оформлюється українською мовою та затверджується в друкованому вигляді із наданням копій в електронному вигляді.

Перелік документів, що має бути розроблений в процесі впровадження Системи:

- 1) Техноробочий проект на технічну модернізацію Системи, у складі:
 - загальносистемні рішення;
 - рішення з технічного забезпечення;
 - рішення з інформаційного забезпечення;
 - рішення з програмного забезпечення
 - вихідні дані на постачання основних технічних засобів та СПЗ;
 - кошторисна документація
 - робоча документація;
- 2) експлуатаційна документація, у складі:
 - настанова з інсталяції програмного забезпечення;
 - настанова з адміністрування параметрів безпеки Системи;
 - настанова з адміністрування параметрів функціонування Системи;
 - настанова користувачів відповідно до визначених профілів (ролей).
- 3) програма-методики приймальних випробувань.

Наведений перелік та зміст не є вичерпним, на етапі технічного проектування Виконавець має скласти уточнений Перелік проектної документації.

За своїм складом та змістом розроблена документація повинна відповідати вимогам законодавства України, національним стандартам, відповідним нормативним документам Замовника.

Вся документація відносно проектних рішень, що надається Розробником Замовнику під час проектування є предметом процесу узгодження. Замовник надає

свої вимоги, рекомендації та пропозиції на вміст, точність та форму кожного документу, що є пріоритетом.

Звітна документація повинна передаватися Замовнику в паперовому та електронному вигляді (на жорстких дисках) українською мовою. Допоміжна документація (що не вказана як безпосередній результат проєктних робіт) надається тільки в електронному вигляді.

8.3. Вимоги до стандартів

Проектна, програмна та експлуатаційна документація повинна розроблятися відповідно до вимог державних стандартів