Додаток
до листа ДСНС
від 08.07.2019 р.
№ 16-9577/163

РЕКОМЕНДАЦІЇ
щодо проектування, введення в експлуатацію, експлуатації та технічного обслуговування (супроводження) територіальних (місцевих) автоматизованих систем централізованого оповіщення

I. Сфера застосування і призначення

Рекомендації щодо проектування, введення в експлуатацію, експлуатації та технічного обслуговування (супроводження) територіальних (місцевих) автоматизованих систем централізованого оповіщення (далі — Рекомендації) розроблені з метою роз'яснення вимог наказу МВС України від 08.02.2019 № 93 "Про затвердження Інструкції щодо практик чи процедур проектування, дослідження, введення в експлуатацію, експлуатації та технічного обслуговування (супроводження) автоматизованих систем централізованого оповіщення", зареєстрованого у Міністерстві юстиції України 22 квітня 2019 р. за № 418/33389, для використання відповідальними особами і профільними фахівцями територіальних органів ДСНС України, які мають потребу у вичерпному їх розумінні, з'ясуванні та аналізі процесів реалізації проектів (проектних рішень) щодо створення та/або технічної реконструкції (модернізації) автоматизованих систем централізованого оповіщення (далі — АСЦО).

Рекомендації розроблені відповідно до:

Кодексу цивільного захисту України (далі — Кодекс);

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

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);

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;

Технічних вимог до загальнодержавної автоматизованої системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій, затверджених наказом МВС від 05 листопада 2018 року № 884;

вимог, правил і рекомендацій національних, міжнародних та європейських стандартів.

Під час розроблення Рекомендацій також було враховано досвід створення, проектування та експлуатації існуючих автоматизованих систем централізованого оповіщення та проаналізовано різні сучасні підходи, технологічні та технічні рішення щодо забезпечення необхідної їх функціональності, технічного обслуговування і супроводження.

За структурою і технічним змістом цей документ виконано відповідно до рекомендацій таких національних стандартів: ДСТУ ISO/IEC/IEEE 29148, ДСТУ ISO/IEC TR 24766, ДСТУ-Н ISO/IEC Guide 15 та ДСТУ 1.5.

Основні положення, наведені у Рекомендаціях, ґрунтуються на поєднанні положень національних та міжнародних стандартів щодо:

застосування, створення, проектування АСЦО та їх складових за функціональним призначенням;

технічного, програмного і інформаційного забезпечення експлуатації систем централізованого оповіщення, їх технічного обслуговування та супроводження;

використання різних інформаційних технологій для оповіщення та інформування населення про загрозу виникнення або виникнення надзвичайних ситуацій.

Положення Рекомендацій безпосередньо не впливають на організацію діяльності оперативно-чергових (чергових) служб пунктів управління цивільного захисту, а визначають лише організаційно-технічні питання щодо впровадження та функціонування АСЦО.

ІІ. Нормативні посилання

Нижченаведені документи (технічні регламенти, національні і міжнародні стандарти), на які є посилання в тексті, необхідні для застосування Рекомендацій. Для датованих посилань застосовують лише зазначене видання. Для недатованих посилань є дійсним останнє видання зазначеного документа (включаючи будь-які зміни).

У Рекомендаціях є посилання на такі національні стандарти:

ДСТУ 1.5:2015 Національна стандартизація. Правила розроблення, викладання та оформлення національних нормативних документів;

ДСТУ-Н ISO/IEC Guide 15:2008 Зведені правила ISO/IEC щодо «посилання на стандарти»;

ДСТУ 2861-94 Надійність техніки. Аналіз надійності. Основні положення;

ДСТУ 2862-94 Надійність техніки. Методи розрахунку показників надійності. Загальні вимоги;

ДСТУ 3486-96 Засоби обчислювальної техніки. Системи мікропроцесорні таймерні. Загальні технічні вимоги;

ДСТУ 3524-97 Надійність техніки. Проектна оцінка надійності складних систем з урахуванням технічного і програмного забезпечення та оперативного персоналу. Основні положення;

ДСТУ 7245:2011 Дизайн і ергономіка. Кодування зорової інформації. Загальні вимоги ергономіки;

ДСТУ 7299:2013 Дизайн і ергономіка. Робоче місце оператора. Взаємне розташування елементів робочого місця. Загальні вимоги ергономіки;

ДСТУ EN ISO 7731:2016 Ергономіка. Сигнали небезпеки для місць громадського призначення і робочого простору. Звукові сигнали небезпеки;

ДСТУ 8604:2015 Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги;

ДСТУ ISO 9241-8:2006 Ергономічні вимоги до роботи з відеотерміналами в офісі. Частина 8. Вимоги до відображуваних кольорів;

ДСТУ EN ISO 9241-13:2017 Ергономічні вимоги до роботи з відеотерміналами в офісі. Частина 13. Настанова щодо використання;

ДСТУ EN ISO 9241-14:2017 Ергономічні вимоги до роботи з відеотерміналами в офісі. Частина 14. Діалогове меню;

ДСТУ ISO 10001:2013 Управління якістю. Задоволеність замовників. Настанови щодо кодексів поведінки для організацій;

ДСТУ ISO 11428:2008 Ергономіка. Сигнали небезпеки візуальні. Загальні вимоги, проектування та випробування;

ДСТУ ISO/IEC 12207:2016 Інженерія систем і програмного забезпечення. Процеси життєвого циклу програмного забезпечення;

ДСТУ ENV 13269:2005 Технічне обслуговування. Настанови щодо складання договорів.

ДСТУ EN 13460:2005 Обслуговування технічне. Документи на технічне обслуговування;

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

ДСТУ ISO/IEC TR 15271:2010 Інформаційні технології. Настанови щодо застосування ISO/IEC 12207 (Процеси життєвого циклу програмного забезпечення);

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

ДСТУ ISO/IEC 15289:2014 Інженерія систем і програмного забезпечення. Контент життєвого циклу інформаційної продукції (документації);

ДСТУ ISO/IEC/IEEE 16326:2015 Розроблення систем та програмного забезпечення. Процеси життєвого циклу. Керування проектами;

ДСТУ ISO/IEC 17050-1:2006 Оцінювання відповідності. Декларація постачальника про відповідність. Частина 1. Загальні вимоги;

ДСТУ ISO/IEC 17050-2:2006 Оцінювання відповідності. Декларація постачальника про відповідність. Частина 2. Підтверджувальна документація;

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

ДСТУ ISO/TR 22351:2017 Соціальна безпека. Управління у надзвичайних ситуаціях. Структура сповіщень для обміну інформацією;

ДСТУ ISO/IEC TR 24748-1:2015 Розроблення систем і програмного забезпечення. Управління життєвим циклом. Частина 1. Настанова з управління життєвим циклом;

ДСТУ ISO/IEC/IEEE 24748-4:2018 Інженерія систем і програмних засобів. Керування життєвим циклом. Частина 4. Інженерне проектування систем;

ДСТУ ISO/IEC TR 24766:2016 Інформаційні технології. Інженерія систем і програмних засобів. Настанови щодо розроблення технічних вимог до програмних засобів;

ДСТУ ISO/IEC/IEEE 29148:2015 Розроблення систем і програмного забезпечення. Процеси життєвого циклу. Розроблення вимог;

ДСТУ IEC 60073:2005 Основні принципи та правила з безпеки щодо інтерфейсу «людина-машина». Принципи кодування індикаторів та органів керування;

ДСТУ EN 60950-1:2015 Обладнання інформаційних технологій. Безпека. Частина 1. Загальні вимоги;

ДСТУ EN 60950-22:2017 Обладнання інформаційних технологій. Безпека. Частина 22. Обладнання, встановлюване на відкритому повітрі;

ISO 8201:2017 Alarm systems — Audible emergency evacuation signal — Requirements (Системи тривожної сигналізації — Звукові сигнали евакуації при надзвичайних ситуаціях);

ISO 9921:2003 Ergonomics — Assessment of speech communication (Ергономіка — Оцінювання мовної комунікації)

ISO 11429:1996 Ergonomics — System of auditory and visual danger and information signals (Ергономіка — Система звукових, візуальних та інформаційних сигналів небезпеки);

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

IEC 60849:1998 Sound systems for emergency purposes (Звукові системи для використання при надзвичайних ситуаціях);

EN 50849:2017 Sound systems for emergency purposes (Звукові системи для використання при надзвичайних ситуаціях);

ETSI TS 102 182 V1.4.1 (2010-07) Emergency Communications. Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies (Інформаційна взаємодія при надзвичайних ситуаціях. Вимоги з інформаційної взаємодії державних органів/організацій з окремими особами, групами і широкою громадськістю в умовах надзвичайних ситуацій).

III. Терміни та визначення понять

У Рекомендаціях ужито:

терміни та визначення, які наведено в законах України «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах» та «Про основні засади забезпечення кібербезпеки України»;

застандартизовані терміни та визначення, які наведено у:

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 5127:2007 Інформація і документація. Словник термінів;

ДСТУ ISO 9000:2015 Системи управління якістю. Основні положення та словник термінів;

ДСТУ EN 13306:2006 Технічне обслуговування. Терміни та визначення понять;

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

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

ДСТУ ISO/IEC/IEEE 24765:2015 Розроблення систем і програмного забезпечення. Словник;

ДСТУ ISO/IEC 27000:2017 Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів;

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

IV. Скорочення та абревіатура

1. Скорочення

У Рекомендаціях вжито такі позначки та скорочення:

АРМ — автоматизоване робоче місце;

АС — автоматизована система;

АСЦО — автоматизована система централізованого оповіщення;

КЗА — комплекс засобів автоматизації;

КСЗІ — комплексна система захисту інформації;

НТМ — Національна телекомунікаційна мережа;

ОС — операційна система;

ПЗ — програмне забезпечення;

ПТК — програмно-технічний комплекс;

ПУСО — пункт управління системи оповіщення;

СКБД — система керування базами даних;

УКХ — діапазон ультракоротких хвиль, який використовується для радіомовлення;

ЧМ — частотна модуляція

2. Абревіатура

У рекомендаціях вжито таку абревіатуру:

CBS (Cell Broadcast Service) — послуга широкомовної трансляції коротких повідомлень по мережі стільникового зв’язку;

DigTV (Digital television) — цифрове телебачення;

E-mail MT — електронна пошта з використанням мобільного термінала стандарту GSM;

E-mail PC — електронна пошта з використанням персональних комп’ютерів у мережах Інтернет;

GSM (Global System for Mobile telecommunications) — глобальна система мобільного зв’язку;

MBMS (Multimedia Broadcast/Multicast Service) — послуга мультимедійного багатоадресного мовлення;

MMS (Multimedia Messaging Service) — послуга передавання мультимедійних повідомлень;

MT (Mobile Terminal) — мобільний термінал мережі стільникового зв’язку;

PC (Personal Computer) — персональний комп’ютер;

RDS (Radio Data System for VHF/FM broadcasting) — система широкомовного передавання даних по каналах УКХ/ЧМ-радіомовлення;

SMS (Short Message Service) — послуга передавання коротких повідомлень;

Web (англ.:web — павутина) — інтернет-простір.

V. Загальні положення

1. Концептуальні аспекти системи оповіщення населення

Органи управління цивільного захисту всіх рівнів повинні постійно оцінювати потенційно можливі небезпечні ситуації, які можуть виникнути у певній сфері, та рівень кожного потенційного ризику їх виникнення. Результати цієї оцінки повинні визначати організаційні та технічні складові системи оповіщення населення. Концептуальна організаційна структура системи оповіщення населення наведена на рисунку 1.

Рисунок 1. Концептуальна організаційна структура системи оповіщення населення

Система оповіщення населення, яка створена, впроваджена, реконструюється (модернізується), вдосконалюється органом управління цивільного захисту кожного відповідного рівня єдиної державної системи цивільного захисту повинна:

дотримуватися виконання вимог чинного законодавства (державної політики у сфері цивільного захисту) та інших загальнообов’язкових вимог національних нормативних документів;

структурно передбачати постановку та аналіз завдань оповіщення населення;

бути спроектованою на перспективу;

бути задокументованою, впровадженою і мати відповідне технічне обслуговування та супроводження технічних і програмних засобів;

мати людські, технічні та фінансові ресурси для реалізації, впровадження, підтримання та вдосконалення системи оповіщення населення;

бути інформаційно доступною для всіх осіб у рамках їх компетенції, які працюють у структурах органів управління цивільного захисту, та інших суб’єктів забезпечення цивільного захисту;

забезпечувати відповідну підготовку відповідальних фахівців органів управління цивільного захисту;

бути доступною і комунікабельною для населення в цілому та особливо для людей, які можуть піддаватися впливу надзвичайної ситуації;

передбачати відповідну інформаційну взаємодію з іншими системами оповіщення у рамках державної системи оповіщення населення згідно з Концепцією;

включати рішення щодо постійного її вдосконалення.

Системи оповіщення населення повинні забезпечувати процес доведення сигналів оповіщення до населення про небезпеку та відповідати таким основним вимогам:

постійна готовність до застосування у цілодобовому режимі функціонування (24/7);

оперативність задіяння мереж оповіщення та інформування;

використання сучасних засобів оповіщення, мереж телекомунікацій і телерадіомовлення, які забезпечують оповіщення та інформування в мінімальні терміни максимальної кількості населення, незалежно від часу доби, місць його перебування і проживання.

2. Інформаційні складові процесу оповіщення населення

Інформаційними складовими процесу оповіщення населення про загрозу виникнення або виникнення надзвичайної ситуації є доведення сигналів небезпеки та інформаційних повідомлень.

Мета доведення до населення сигналу небезпеки полягає в приверненні уваги людей при загрозі виникнення або виникненні надзвичайної ситуації шляхом стимуляції слухових, візуальних, тактильних почуттів для прийняття відповідних заходів (дій) щодо забезпечення безпеки та отримання допоміжної інформації. Процес доведення сигналів небезпеки повинен гарантувати, що цей сигнал привернув максимальну увагу населення з урахуванням особливостей і стану людей, які можуть знаходиться або знаходяться в зоні (районі, регіоні) ризику (небезпеки), включаючи соціально незахищені групи населення.

Системи оповіщення повинні бути здатні реалізовувати оповіщення в короткий передбачуваний період часу цільової аудиторії досяжних громадян за технологією, доступною для них у цей час.

Відповідно до вимог європейського нормативного документа ETSI TS 102 182, на який надається посилання у Концепції, системи оповіщення населення повинні бути здатні реалізовувати оповіщення:

до 50 % населення у відповідній зоні (відповідному районі, регіоні) надзвичайної ситуації протягом 3 хвилин,

до 97 % населення в цій зоні (відповідному районі, регіоні) протягом 5 хвилин.

Період часу три (п’ять) хвилини — це час між моментом, коли повідомлення відправляється для обробки в систему оповіщення, і моментом, коли повідомлення доведено до населення. Ці часові параметри не можуть застосовуватися, наприклад, при таких надзвичайних ситуаціях як землетруси та цунамі. Такі випадки потребують реалізовувати оповіщення якомога більшої кількості громадян у певному постраждалому районі на рівні секунд (наприклад, 10 секунд для землетрусу).

Система повинна мати можливість трансляції черговою службою в автоматизованому режимі першого попереджувального сигналу небезпеки «УВАГА ВСІМ!» протягом 3 секунд з моменту надходження відповідної команди або автоматично у разі надходження відповідного сигналу від автоматизованої системи раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення населення у разі їх виникнення.

В останньому випадку (для спеціальних, локальних та об’єктових систем оповіщення) часовий період 3 секунди не включає часу реакції автоматизованої

системи раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення населення у разі їх виникнення від моменту виявлення першої ознаки аварійної ситуації до моменту управління трансляцією попереджувального сигналу небезпеки системою оповіщення. Цей часовий параметр (3 секунди) визначено міжнародним стандартом IEC 60849 (його аналогом є європейський стандарт EN 50849), посилання на який надається в ДСТУ EN ISO 7731.

Основною вимогою для попереджувального сигналу небезпеки «УВАГА ВСІМ!» є наявність деяких характерних типових ознак, які забезпечують розрізнюваність цього сигналу і його розпізнавання в різних найскладніших умовах оточуючої обстановки. Необхідні варіації подання сигналу можуть бути отримані декількома способами його подання, наприклад у вигляді:

уривчастого періодичного однотонального звукового сигналу;

уривчастого періодичного однотонального звукового сигналу та візуального червоного миготливого світлового сигналу;

уривчастого періодичного однотонального звукового сигналу та інформаційного повідомлення про небезпеку;

уривчастого періодичного однотонального звукового сигналу, візуального червоного миготливого світлового сигналу та короткого інформаційного повідомлення про небезпеку.

Синхронність подання звукових і світлових сигналів не є обов’язковою вимогою, але може поліпшити їх сприйняття населенням. Вибір конкретного виду попереджувального сигналу небезпеки «УВАГА ВСІМ!» визначається залежно від рівня та характеру походження надзвичайної ситуації. Вимоги до структури цього сигналу регламентовані міжнародним стандартом ISO 11429, посилання на який надається у ДСТУ ISO 11428 та ДСТУ EN ISO 7731.

Будь-який обраний попереджувальний сигнал небезпеки «УВАГА ВСІМ!» повинен мати часовий цикл (циклограму), чітко відмінний від сигналу евакуації при надзвичайних ситуаціях. Вимоги до сигналів евакуації регламентовані міжнародним стандартом ISO 8201, посилання на який надається у ДСТУ ISO 114288 та ДСТУ EN ISO 7731. Загальна тривалість звучання попереджувального сигналу небезпеки «УВАГА ВСІМ!» повинна становити три-п’ять хвилин. Рівень звукового сигналу небезпеки повинен відповідати вимогам ДСТУ EN ISO 7731.

Звуковий сигнал небезпеки «УВАГА ВСІМ!» може доповнюватися інформаційним повідомленням, яке повинно бути коротким, повністю завершеним і мати точно виражене значення. Тривалість інформаційного повідомлення має визначається обраним варіантом звукового сигналу небезпеки і видом небезпеки.

Звуковий сигнал може супроводжуватися синхронним візуальним червоним миготливим світловим сигналом. Синхронність подання звукових і світлових сигналів не є обов’язковою вимогою, але може поліпшити їх сприйняття. Рекомендована частота миготіння світлового сигналу в межах кожного сегмента повинна складати від 2 до 3 Гц з приблизно рівними інтервалами включення/виключення.

Переважно використовувати більше одного джерела світлового сигналу у сигнальному пристрої, щоб забезпечити можливість створення ефекту просторової та часової зміни сигналу (ефект миготіння).

Під час розвитку надзвичайної ситуації може виникнути необхідність доведення до населення оновленої інформації, яка може мати вирішальне значення для порятунку життів людей і зниження втрат. Від того, як регулярно буде здійснюватися інформаційний вплив на людей у сфері безпеки життєдіяльності, з якою оперативністю буде доведено сигнал оповіщення до органів управління цивільного захисту, наскільки своєчасно буде оповіщено та проінформовано населення, залежить у кінцевому підсумку результативність заходів щодо зниження людських втрат та матеріальних збитків у надзвичайних ситуаціях.

3. Аспекти інформування населення

Основна проблема інформування населення полягає у тому, що населення потенційно може бути не готове до небезпечних подій і явищ, що відбуваються в звичайний мирний час. Яскравими прикладами є надзвичайні ситуації будь-якого рівня, коли більшість людей не розуміють, а частіше не знають як діяти в тій чи іншій ситуації.

Заходи процесу інформування населення (рисунок 2) в основному поділяються на завчасні (перед впливом надзвичайної ситуації) та при виникненні надзвичайних ситуацій (після впливу надзвичайної ситуації).

Заходи при виникненні надзвичайних ситуацій (після впливу надзвичайної ситуації) виконуються органами управління цивільного захисту кожного відповідного рівня єдиної державної системи цивільного захисту автоматизованим способом з використанням технічних засобів АСЦО шляхом трансляції попереджувального сигналу небезпеки «УВАГА ВСІМ!», складовими частинами якого мають бути звуковий та візуальний сигнали, а також короткі інформаційні мовні повідомлення з відповідними інструкціями для здійснення заходів (дій) щодо реагування на надзвичайну ситуацію.

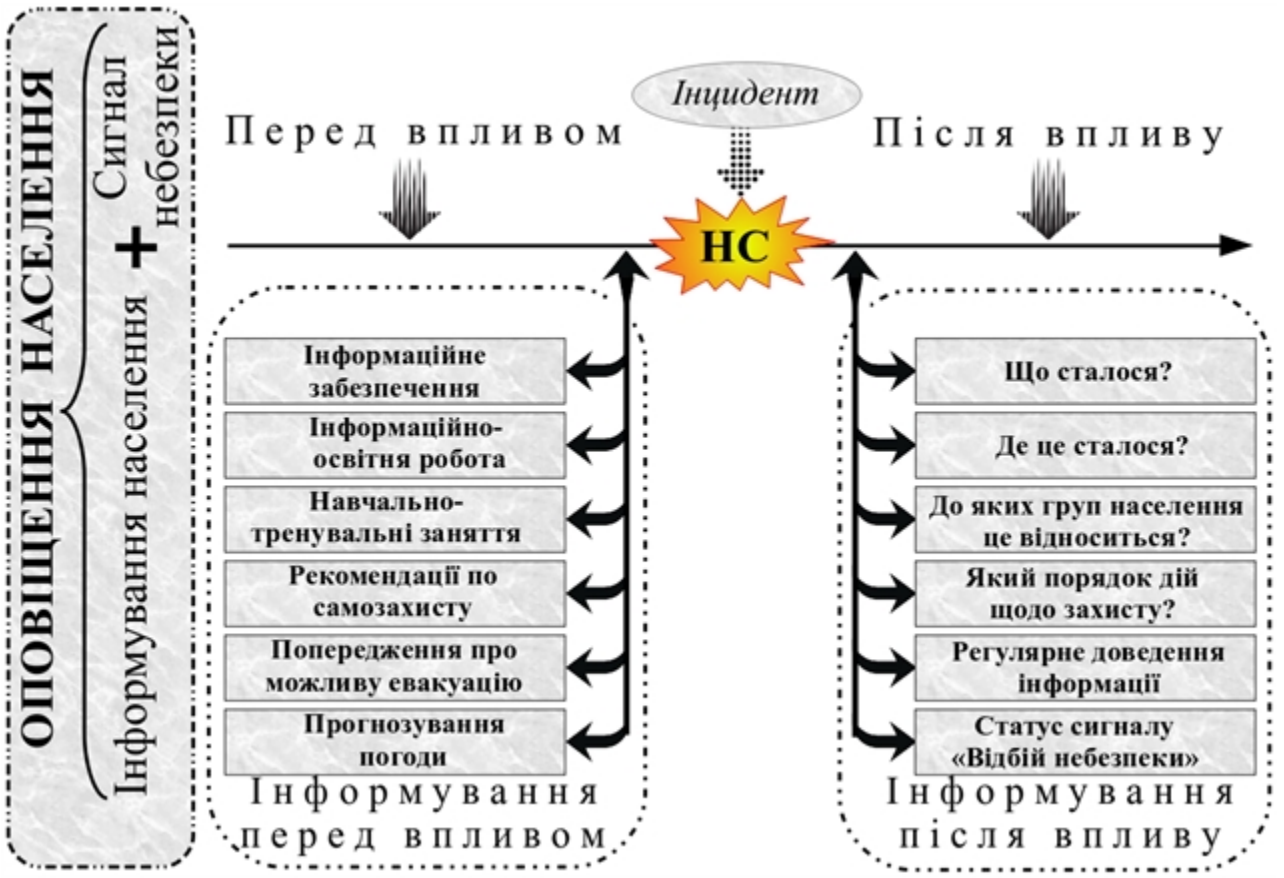

Рисунок 2. Основні особливості заходів щодо інформування населення (адаптовано з ДСТУ ISO 22322)

Завчасні заходи (перед впливом надзвичайної ситуації) щодо інформування населення виконуються в основному шляхом організації:

навчально-виховного процесу з питань безпеки життєдіяльності та цивільного захисту Міністерством освіти і науки України та місцевими органами управління освіти у навчальних закладах;

навчання працюючого населення безпосередньо на підприємствах, в установах та організаціях згідно з програмами підготовки працівників до дій у надзвичайних ситуаціях, а також під час проведення спеціальних об’єктових навчань і тренувань з питань цивільного захисту;

інформаційно-просвітницької роботи за місцем проживання непрацюючого населення щодо навчання діям у надзвичайних ситуаціях місцевими органами виконавчої влади та органами місцевого самоврядування;

самостійного вивченням населенням загальної програми навчання діям у надзвичайних ситуаціях та інших інформаційно-довідкових матеріалів з питань цивільного захисту.

Загальні вимоги до завчасних заходів щодо інформування населення надаються у таких нормативних документах:

постанові Кабінету Міністрів України від 26 червня 2013 р. № 444 «Про затвердження Порядку здійснення навчання населення діям у надзвичайних ситуаціях»;

наказі ДСНС від 19.02.2016 № 83 «Про затвердження Організаційно-методичних вказівок з підготовки населення до дій у надзвичайних ситуаціях»;

ДСТУ 5058 Безпека у надзвичайних ситуаціях. Навчання населення діям у надзвичайних ситуаціях. Основні положення.

Інформування населення при виникненні надзвичайних ситуацій і при завчасних заходах, як пасивні способи цивільного захисту населення, мають певну схожість, однак між ними існують і значні відмінності:

за часовими періодами реалізації;

за частотою доведення інформації;

за обсягом та контекстом інформації, яка надається населенню;

за номенклатурою технічних засобів і технологій доведення інформації.

Крім цього, відповідно до сигналів небезпеки і коротких інформаційних повідомлень у процесі оповіщення населення виконуються нескладні, заздалегідь відпрацьовані дії. Це передбачає наявність системи навчання таким діям при отриманні сигналів оповіщення, відпрацювання умінь і навичок безпечної поведінки. У той же час інформування населення після впливу надзвичайної ситуації, разом із традиційними методами навчання, є складовою частиною системи підготовки населення у сфері цивільного захисту.

У процесі оповіщення повинні бути визначені адекватні способи і технології доведення сигналів оповіщення. При цьому повинні бути враховані такі фактори:

своєчасність — можливість отримати попередження та відповідні інструкції, дотримуючись яких здійснювати заходи (дії) щодо реагування на надзвичайну ситуацію;

доступність — наскільки легко люди, у тому числі соціально незахищені групи населення, можуть отримати доступ до цих сигналів оповіщення;

ефективність і технічна надійність доведення сигналів оповіщення.

При виборі технологій і способів доведення сигналів оповіщення необхідно враховувати:

необхідність забезпечення використання декількох каналів передавання даних (інформації) одночасно і переважно на безкоштовній основі;

можливість використання всіх доступних сучасних і перспективних каналів передавання даних (інформації) для забезпечення максимального покриття зони (району, регіону) оповіщення та для своєчасного доведення сигналів оповіщення;

можливість забезпечення контролю стану каналів передавання даних (інформації) для підтримки якості доведення сигналів оповіщення і проведення періодичної перевірки їх якості, ефективності та цілісності.

Безпосередньо процес доведення сигналів небезпеки та інформаційних повідомлень при загрозі виникнення або виникненні надзвичайної ситуації повинен передбачати:

систематичне доведення інформаційних повідомлень з використанням різних каналів передавання даних (інформації) визначеною мовою (мовами);

визначення дат і часу доведення повторюваних або періодичних інформаційних повідомлень для населення про загрозу виникнення надзвичайної ситуації;

врахування потреб населення, яке тимчасово перебуває в зоні (районі, регіоні) впливу надзвичайної ситуації і не знайоме з місцевим навколишнім середовищем;

підтвердження, що зміст сигналів небезпеки, інформаційних повідомлень та іншої відповідної інформації задовольняє потреби соціально незахищених груп населення;

запитування та отримання коментарів від заінтересованих сторін щодо вдосконалення доведення сигналів оповіщення.

4. Аспекти впливу людського фактора

Під людськими факторами необхідно розуміти здатність людей, які потенційно можуть знаходиться або знаходяться в зоні (районі, регіоні) ризику (небезпеки), особливо осіб з інвалідністю, сприймати і розуміти сигнали небезпеки і інформаційні повідомлення у процесі оповіщення.

Під час оповіщення населення необхідно враховувати аспекти людських факторів, що впливають на ефективність заходів безпеки, які повинні бути виконані людьми, що потенційно можуть знаходиться або знаходяться в зоні (районі, регіоні) ризику (небезпеки). Необхідно забезпечити їм рівноцінний доступ до інформації щодо оповіщення і сигналів небезпеки. Лише у цьому разі доведена інформація буде зрозумілою настільки, що люди в небезпечній ситуації, у тому числі з різними соціальними та культурними потребами, можуть відреагувати, як передбачалося, і виконати відповідні заходи.

5. Проблемні технологічні аспекти оповіщення населення

Системи оповіщення населення повинні забезпечувати доведення сигналів небезпеки та інформаційних повідомлень при різних сценаріях розвитку надзвичайних ситуацій.

1) Доведення сигналів небезпеки та інформаційних повідомлень до громадян повинно бути можливим при їх перебуванні:

у житлових приміщеннях;

у приміщеннях або на територіях за місцем роботи;

у місцях із масовим перебуванням людей;

на вулиці, при подорожах пішки або в транспортному засобі.

2) Системи оповіщення населення у надзвичайних ситуаціях повинні передбачати можливість:

надання достатніх інструкцій щодо дій, які необхідно здійснити для реагування на надзвичайну ситуацію;

ідентифікації відправника сигналу небезпеки та/або інформаційного повідомлення;

доведення інформаційних повідомлень у запланований час;

одночасного доведення інформаційних повідомлень в окремі географічні регіони, цільовим або численним групам населення;

доведення досить детальної інформації про надзвичайну ситуацію;

повтору інформаційних повідомлень;

підтримки доведення інформаційних повідомлень людям з особливими потребами (наприклад, підтримка терміналів для осіб з вадами слуху та мовлення);

доведення інформаційних повідомлень на декількох мовах;

управління перевантаженнями в різних мережах передавання даних.

3) При проектуванні зони покриття необхідно враховувати технологічні можливості технічних засобів телекомунікацій, телекомунікаційних мереж та їх ресурсів, каналів електрозв'язку, які мають використовуватися для керування кінцевими технічними пристроями оповіщення населення.

При визначенні цих елементів АСЦО переважними критеріями є:

максимальне покриття зони (району, регіону) оповіщення;

своєчасність доведення сигналів оповіщення;

якість, ефективність та надійність каналів електрозв'язку.

4) Необхідно враховувати узагальнені практичні результати міжнародного досвіду, визначені у європейському нормативному документі ETSI TS 102 182, на який надається посилання у Концепції.

У цей час, як основні канали керування кінцевими технічними пристроями оповіщення населення, найчастіше використовуються канали мереж загального користування, такі як ефірне радіо та Інтернет. Однак ці канали зв'язку не можуть повністю відповідати вимогам щодо впровадження систем оповіщення, оскільки вони не є гарантованими і не можуть використовуватися самостійно для оповіщення населення. Крім цього, вони енергозалежні, мають відносно невисоку завадостійкість і залежні від рішень провайдерів і операторів зв'язку.

Своєчасність, гарантованість і адресність доведення попереджувального сигналу «УВАГА ВСІМ!» можуть забезпечити тільки спеціальні канали зв'язку, які є енергонезалежними, захищеними від несанкціонованого доступу та централізовано керованими уповноваженими органами управління цивільного захисту.

6. Особливості використання інформаційних технологій для інформування населення

1) У Рекомендаціях термін «інформаційні технології» визначає ресурси, що використовуються для отримання, обробки, зберігання і розповсюдження інформації (ДСТУ ISO/IEC 38500, ДСТУ ISO/IEC/IEEE 24765) в АСЦО.

Інформаційні технології, які можуть використовуватися в АСЦО для інформування населення, можливо поділити на:

технології радіомовлення (RDS) та цифрового телебачення (DigTV);

технології надання послуг широкомовної трансляції коротких повідомлень по мережі стільникового зв'язку (CBS, SMS, MMS, MBMS, E-mail);

інтернет-технології (Web, E-mail).

Також необхідно враховувати, що найчастіше стадія негайного оповіщення населення про загрозу виникнення або виникнення надзвичайної ситуації за допомогою попереджувального сигналу «УВАГА ВСІМ!» минає до того, як виникає можливість транслювати попереджувальну інформацію про небезпеку, використовуючи зазначені інформаційні технології.

2) Технології радіомовлення (RDS) та телебачення (DigTV)

RDS

RDS-системи в основному використовуються для підправки повідомлень та іншої інформації на автомобільні радіоприймачі від певної мовної радіостанції і можуть розглядатися як потенційний спосіб передачі інформації про загрозу виникнення або виникнення надзвичайної ситуації. Разом з цим, необхідно, щоб радіоприймач був налаштований на відповідну радіочастоту та був включеним.

DigTV

Перехід в Україні з аналогового на цифрове телебачення (DigTV) свідчить про можливість доповнення і підвищення ефективності систем інформування населення про загрозу виникнення або виникнення надзвичайної ситуації. Доступ до повідомлень з використанням цієї технології здійснюється, наприклад, за допомогою смарт-карт, які встановлюються в телевізійних абонентських пристроях. У цьому разі попереджувальні повідомлення можуть бути адресними. Області відображення повідомлень на екранах телевізорів також можуть бути спроектовані на замовлення і повідомлення можуть бути доступні на всіх каналах, які є вільними для доступу.

3) Технології надання послуг широкомовної трансляції коротких повідомлень по мережі стільникового зв'язку (CBS, SMS, MMS, MBMS, E-mail MT)

CBS

Послуга широкомовної трансляції (CBS) у мережах стільникового зв’язку передбачає розсилку (доставку) коротких повідомлень на всі мобільні телефони на певній території.

Територія охоплення може бути, як в межах зони покриття однієї соти (мережі стільникового зв’язку), так і у масштабах всієї України. Ця технологія не дозволяє контролювати успішну доставку повідомлень, однак повідомлення циклічно повторюються для приймання тими, хто пізніше потрапляє в зону дії надзвичайної ситуації або пропустив попередні повідомлення.

Для отримання повідомлення на мобільному телефоні абонента повинна бути включена функція широкомовної трансляції мережі стільникового зв’язку (CBS) та активовані певні канали щодо ідентифікації повідомлення.

Враховуючи, що мобільні телефони мають режим вібрації, люди з порушенням слуху можуть бути попереджені про небезпеку. Додатки типу «текст-мова» (перетворення текстової інформації в мовну) для мобільних телефонів також можуть забезпечити доступність інформування людей з порушеннями зору.

Послуга CBS передбачає трансляцію повідомлень на різних мовах.

При широкомовної трансляції повідомлень використовується виділений (службовий) канал, тому функціональність, як правило, буде доступна навіть при перевантаженні голосового трафіка і трафіка передачі даних.

SMS, MMS

Послуга коротких повідомлень (SMS) і послуга мультимедійних повідомлень (MMS) достатньо добре відомі і прийняті для використання.

SMS-повідомлення можуть бути відправлені на мобільний термінал без встановлення на ньому будь-яких спеціальних параметрів. Повідомлення можуть містити досить детальні інструкції для населення про виконання необхідних дій.

MMS-повідомлення можуть бути відправлені на мобільний термінал як без встановлення на ньому будь-яких спеціальних параметрів, так і (в окремих випадках) з попереднім встановленням певних функцій мобільного телефону. Повідомлення може включати зображення, голос і текстове повідомлення та містити детальні інструкції для населення про виконання необхідних дій.

У нормальних умовах доставка SMS- і MMS-повідомлень може бути практично миттєвою, але велика кількість повідомлень вимагає значного часу. Сильне перевантаження мережі може призвести до затримки доставки повідомлень.

MBMS

Послуга мультимедійного багатоадресного мовлення (MBMS) має два режими використання.

Режим широкомовної трансляції (broadcast) — односпрямоване «точка-багатоточка» передавання мультимедійної інформації (текст, аудіо, зображення, відео) всім користувачам у зоні обслуговування широкомовної трансляції.

Режим багатоадресного передавання (multicast) дозволяє односпрямовану передачу «точка-багатоточка» мультимедійної інформації групі користувачів у зоні обслуговування багатоадресної трансляції. У цьому режимі є мережева можливість вибіркового передавання інформації до соти зони обслуговування, в межах якої знаходяться абоненти багатоадресної групи.

E-mail MT

Інформування за допомогою електронної пошти на абонентські термінали (E-mail MT) у мережах стільникового зв'язку є можливим лише для користувачів мобільних терміналів, що мають функцію електронної пошти.

4) Інтернет технології (Web, E-mail PC)

Web

Для інформування за допомогою Web-технологій можуть використовуватися сервісні послуги Інтернет, які підтримують обмін повідомленнями в реальному масштабі часу, наприклад, Facebook Messenger, MSN Messenger, Windows Live Messenger тощо. За допомогою них можна інформувати осіб, які активували ці послуги на персональному комп'ютері або мобільному терміналі. Певним недоліком цієї технології є те, що без активації послуги абонентом доведення повідомлень є неможливим і повідомлення можуть бути втрачені.

E-mail PC

Інформування за допомогою електронної пошти на персональні комп'ютери (E-mail PC) користувачів не є гарантованою послугою доставки повідомлень. Однак при персоналізації і регулярному використанні є висока ймовірність того, що ця послуга буде мати високу ступінь корисності. Відразу, як тільки користувач зареєстрував свою адресу електронної пошти у службі з інформування про надзвичайну ситуацію, він може розраховувати на отримання електронних листів, що повідомляють його про надзвичайні ситуації та містять рекомендації про належні дії в певний час. Варіантом цього можуть бути призначені для користувачів реєстри попереджувальних повідомлень для розсилки інформаційних повідомлень про небезпеку.

VI. Вимоги до процесу проектування та введення в експлуатацію АСЦО

1. Загальні вимоги до процесу проектування системи

1) Проектування системи — це дії, що виконуються з моменту визначення вимог до системи до моменту створення системи, яка задовольняє ці вимоги (ДСТУ 2941).

Під час проектування АСЦО необхідно, щоб процеси, її функції і завдання були пов’язані між собою і визначені їхні взаємозв’язки з попередніми процесами, функціями і завданнями існуючих систем оповіщення населення.

Практичний досвід реалізації проектних рішень останніх років щодо впровадження АСЦО різних рівнів свідчить про недостатню якість процесів керування проектами та контролю за виконанням проектів, підготовки документації на системи.

2) Документація на систему — це сукупність документів, які описують вимоги, можливості, обмеження, проектування, експлуатацію і обслуговування системи обробки інформації (ДСТУ ISO/IEC 2382).

Проектна документація відповідно до ДСТУ ISO/IEC/IEEE 24765 — це документ, який описує проект системи або компонент системи (синоніми: проектний документ, специфікація проекту).

3) Проектне рішення — це рішення будь-якої задачі, пов’язаної з проектуванням, подане у формалізованому вигляді (ДСТУ 2941).

Програмно-технічні (зокрема, вихідний код програмних модулів і команди компілятора, алгоритми, структури і формати даних тощо) та організаційні (регламенти, вимоги, інструкції, обмеження тощо) проектні рішення, що можуть застосовуватися під час експлуатації і супроводу системи, а також технічна документація до них повинні передаватися Замовнику Розробником (Постачальником) у вигляді, достатньому для їхнього незалежного використання (без звернення до Розробника та/або Постачальника).

Реалізація проектних рішень без проектної документації не допускається.

Проектні рішення зі створення, технічної реконструкції, розвитку автоматизованих систем централізованого оповіщення повинні задовольняти вимоги щодо реалізації та дотримання основних принципів і критеріїв, а саме: задоволеності Замовника, гарантування якості проектних рішень, відповідальності, стандартизації, безперервності і спадкоємності, відкритості, інформаційної сумісності, інформаційної безпеки, мобільності, ефективності.

Задоволеність Замовника проектними рішеннями — сприйняття Замовником ступеня виконання його вимог та очікувань Розробника (Постачальника) відповідно до ДСТУ ISO 10001.

Гарантування якості проектних рішень — наявність підтверджувальної документації від Розробника (Постачальника) для доведення відповідності проектних рішень установленим вимогам до АСЦО відповідно до ДСТУ ISO/IEC 17050-1, ДСТУ ISO/IEC 17050-2.

Відповідальність — призначення відповідальних осіб заінтересованих сторін щодо реалізації процесів проектування.

Стандартизація — заходи з планування, керування і контролю процесу проектування щодо створення, технічної реконструкції системи оповіщення повинні відповідати нормативно-правовим актам і національним стандартам: ДСТУ ISO/IEC/IEEE 29148, ДСТУ ISO/IEC 12207, ДСТУ ISO/IEC/IEEE 15288,

ДСТУ ISO/IEC 15289, ДСТУ ISO/IEC/IEEE 16326, ДСТУ ISO/IEC TR 24748-1, ДСТУ ISO/IEC/IEEE 24748-4, ДСТУ ISO/IEC TR 24766.

Безперервність, спадкоємність, технологічність, модульність і масштабованість програмних і технічних засобів, а саме:

розроблення і вдосконалення функцій повинно забезпечувати можливість подальшого розвитку системи з використанням сучасних високоефективних інформаційних технологій і програмно-технічних засобів, а також повинен бути забезпечений захист початкових вкладень фінансових, матеріально-технічних і 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 багаторазового їх використання;

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

Відкритість системи повинна забезпечуватися шляхом нарощування технічних засобів системи, поновлення й розширення функцій відповідно до її розвитку без порушення функціонування та кардинальної зміни її структури і складу.

Інформаційна сумісність системи (інтеграція з іншими інформаційними системами) повинна бути організована на основі стандартів взаємозв'язку відкритих систем відповідно до встановлених протоколів обміну даними, правил і регламентів для забезпечення інформаційної взаємодії.

Інформаційна безпека системи — забезпечення необхідного рівня конфіденційності, кіберзахисту, цілісності, доступності, автентичності і достовірності інформації та ефективності технічного захисту інформаційного ресурсу системи від втрат, спотворення, руйнування і несанкціонованого використання.

Мобільність — здатність до адаптації, простота установки, взаємозамінність, забезпечення результативності та ефективності переносу системи, програмного продукту або компонента з однієї апаратної, програмної чи іншої експлуатаційної платформи (використовуваного середовища) в іншу (інше).

Ефективність — вибір проектних (програмних, технічних) рішень щодо реконструкції існуючих систем оповіщення повинен забезпечувати мінімізацію вкладень фінансових, матеріально-технічних та трудових ресурсів.

2. Визначення моделі життєвого циклу АСЦО

Типова модель життєвого циклу будь-якої інформаційної системи охоплює життя системи від установлення вимог і до припинення її використання та складається із сукупності процесів (робіт) і завдань, основними з яких є визначення вимог, розроблення (проектування), експлуатація, технічне обслуговування та супровід як системи в цілому, так і її складових компонентів, зокрема, програмних засобів.

Аналіз об’єктивних умов (порядок і обсяги фінансування, динамічний і безперервний розвиток інформаційних технологій, зміна масштабів цілей і завдань щодо оповіщення населення про загрозу виникнення або виникнення надзвичайних ситуацій), організаційних та технічних складових процесу реалізації заходів щодо створення, реконструкції (модернізації) та вдосконалення існуючих АСЦО свідчить, що оптимальним є вибір комбінованої (змішаної) моделі життєвого циклу АСЦО всіх рівнів.

Обрана модель життєвого циклу АСЦО за структурою є інкрементною (рисунок 3), а з точки зору розвитку і вдосконалення — еволюційною (рисунок 4) відповідно до ДСТУ ISO/IEC TR 15271.

Рисунок 3. Обрана модель життєвого циклу АСЦО (у цілому)

Під час вибору моделі життєвого циклу також ураховано рекомендації ДСТУ ISO/IEC 12207, ДСТУ ISO/IEC/IEEE 15288, ДСТУ ISO/IEC 15289, ДСТУ ISO/IEC TR 24748-1, ДСТУ ISO/IEC/IEEE 24748-4.

Інкрементна модель (модель нарощування функцій, метод «крок за кроком») передбачає реалізацію самих основних базових функцій (мінімальна функціональність), які потім нарощуються новими. Перевага підходу — в будь-який момент часу є працююча система.

Рисунок 4. Обрана еволюційна складова моделі життєвого циклу АСЦО

Основними перевагами обраного варіанта моделі життєвого циклу АСЦО всіх рівнів є:

початкове визначення тільки основних можливостей системи, що запобігає формуванню громіздкого переліку вимог;

можливість оцінки найбільш важливих функціональних особливостей системи на більш ранніх етапах розроблення, що дозволяє знизити ризик невдачі, здійснити перегляд і зміни вимог;

розподіл системи на нарощувані компоненти (інкременти) дозволяє об’єднати отриманий досвід у вигляді вдосконаленого компонента і використовувати при цьому набагато менше ресурсів і часу на розроблення;

можливість керованого розподілу ресурсів з урахуванням важливості реалізованих в інкременті функцій, тобто залучення фінансових, матеріально-технічних і трудових ресурсів у міру необхідності;

реалізація процесів експлуатації та супроводу паралельно з процесом розроблення.

3. Технічні складові процесів проектування

До технічних складових процесу проектування необхідно відносити такі основні технічні процеси (ДСТУ 2941, ДСТУ ISO/IEC/IEEE 29148, ДСТУ ISO/IEC 12207, ДСТУ ISO/IEC/IEEE 15288):

визначення основних системних вимог до АСЦО;

аналіз і узгодження вимог та підготовка технічного завдання на проектування;

визначення архітектури (організаційної структури) АСЦО;

реалізація проекту;

верифікація проектних рішень (попередні випробування);

валідація проектних рішень (приймальні випробування).

1) Визначення основних вимог

Вимоги до АСЦО визначаються відповідним органом управління цивільного захисту, до компетенції якого належить забезпечення її створення та застосування за призначенням щодо оповіщення та інформування населення про загрозу виникнення або виникнення надзвичайних ситуацій.

За різними критеріями національних стандартів (ДСТУ ISO/IEC/IEEE 29148, ДСТУ ISO/IEC 12207, ДСТУ ISO/IEC/IEEE 15288) технічні вимоги до інформаційної системи поділяються на функціональні вимоги (специфікація основних функцій) і нефункціональні вимоги (додаткові вимоги і обмеження).

2) Аналіз і узгодження вимог та підготовка технічного завдання на проектування

Аналіз вимог — це систематизоване дослідження вимог замовника до системи для реалізації їх у проектних рішеннях (ДСТУ ISO/IEC 2382).

Вимоги до АСЦО повинні бути однозначні і добре досліджені, оскільки неоднозначне розуміння сукупності вимог може призвести до збільшення вартості, порушення графіка створення та зниження якості системи.

Мета процесу аналізу і узгодження вимог полягає в тому, щоб у процесі проектування перетворити їх в завершене якісне системне технічне рішення щодо створення (модернізації, вдосконаленню) АСЦО. Цей процес створює уявлення про майбутню систему (компоненти системи), яка буде відповідати вимогам Замовника.

Узгодження вимог — це процес або нарада, під час яких вимоги до системи, елемента системи, технічного засобу або програмного забезпечення надаються заінтересованим сторонам для коментарів або узгодження (ДСТУ ISO/IEC/IEEE 24765).

Помилковою необхідно вважати думку, що узгодження вимог є їх перевіркою. Вимоги повинні вказувати «що», а не «як» (ДСТУ ISO/IEC/IEEE 29148).

Технічне завдання на автоматизовану систему — це оформлений та затверджений належним чином документ, що визначає обґрунтування доцільності й мету створення АС, вимоги до неї, а також основні засадничі дані та план-графік створення АС (ДСТУ 2226).

Відповідно до встановленої практики і рекомендацій національних стандартів (ДСТУ ISO/IEC 12207, ДСТУ ISO/IEC/IEEE 15288, ДСТУ ISO/IEC/IEEE 29148) технічне завдання, як правило, складається з розділів і підрозділів (додаток 1 до Рекомендацій).

3) Визначення архітектури (організаційної структури) АСЦО

Архітектура (організаційна структура) АСЦО всіх рівнів має складові, що визначаються ознаками розподілу за призначенням об’єктів автоматизації та функціональних елементів (компонентів) АСЦО. У зв’язку з цим архітектура АСЦО має дві складові — організаційну та функціональну.

Організаційна складова архітектури (організаційної структури) АСЦО всіх рівнів визначена пунктом 3 Положення.

Функціональна складова архітектури (організаційної структури) АСЦО визначає функціональні елементи (компоненти) об’єктів автоматизації у складі АСЦО за їх призначенням. У зв’язку з тим, що вони мають жорстку прив’язку до організаційної складової архітектури (організаційної структури) АСЦО, її функціональна складова повинна мати таку ж саму прив’язку.

Елементами (компонентами) функціональної складової архітектури (організаційної структури) АСЦО є складові, які забезпечують виконання системою основних функцій, а саме: комплекси засобів автоматизації пунктів управління, програмно-технічні комплекси, АРМ оперативно-чергових (чергових) служб, технічні засоби телекомунікацій, кінцеві пристрої оповіщення, технічні засоби електроживлення тощо.

4) Реалізація проекту

Етап реалізації проекту починається з досить детального технічного уточнення системних вимог та проектних рішень до АСЦО, перетворення їх в єдине комплексне рішення щодо створення (модернізації, вдосконалення) АСЦО, яке забезпечить її подальше технічне обслуговування і супровід на етапі використання за призначенням.

Цей етап також повинен передбачати гарантії Виконавця відповідно до ДСТУ ISO/IEC 15026-4, що проектні рішення забезпечують задоволеність Замовника на всіх інших наступних етапах життєвого циклу АСЦО.

5) Верифікація проектних рішень (попередні випробування)

Метою процесу верифікації є надання об’єктивних доказів того, що система або елемент системи виконує свої функції відповідно до визначених вимог (ДСТУ ISO 9000, ДСТУ ISO/IEC 12207, ДСТУ ISO/IEC/IEEE 15288). Перевірка системи здійснюється за допомогою формальних засобів для визначення її відповідності встановленим вимогам (ДСТУ 2941).

Попередні випробування здійснюються Виконавцем проекту з використанням відповідних методів, методик, стандартів або правил. Відповідно до встановленої практики заходи цього процесу проводяться Виконавцем проекту під час попередніх випробувань перед передачею результатів проектування замовнику.

Для забезпечення гарантій якості проектних рішень Виконавцем проекту розробляється програма і методика випробувань, які узгоджуються з Замовником. Результати випробувань надаються замовнику при передачі проекту.

6) Валідація проектних рішень (приймальні випробування)

Валідація (затвердження) — це підтвердження наданням об’єктивного доказу, що вимоги щодо конкретного передбаченого використання або застосування виконано. Слово «затверджено» використовують для позначення відповідного статусу (ДСТУ ISO 9000, ДСТУ ISO/IEC 12207, ДСТУ ISO/IEC/IEEE 15288).

Метою процесу валідації є надання об’єктивних доказів, що система або елемент системи виконує свої функції відповідно до визначених вимог. Цей процес надає необхідну інформацію замовнику проекту для визначення відповідності проектних рішень, що реалізовані виконавцем відповідно до визначених вимог.

Відповідно до встановленої практики заходи цього технічного процесу проводяться Замовником під час приймальних випробувань АСЦО, які рекомендовано проводити методом дослідної експлуатації.

Приймальні випробування АСЦО проводяться комісією. Статус приймальної комісії та її склад визначається Замовником проекту.

Під час приймальних випробувань АСЦО виконують:

випробування на відповідність технічному завданню згідно з програмою та методикою приймальних випробувань;

оцінку відповідності проектних рішень технічним вимогам, визначеним технічним завданням;

аналіз результатів випробувань АСЦО та усунення недоліків, що виявлені під час випробувань;

оформлення акта про приймання АСЦО в постійну експлуатацію.

Програма та методика приймальних випробувань АСЦО (елемента системи) призначені для встановлення об’єктивних доказів, які забезпечують отримання певних результатів та перевірку проектних рішень, виявлення причин збоїв, визначення якості проектних робіт, показників якості функціонування системи (елементу системи), а також визначається тривалість і режим випробувань.

Програма випробувань повинна містити переліки конкретних перевірок, які необхідно здійснювати під час випробувань для підтвердження виконання вимог технічного завдання, з посиланнями на відповідні розділи методики випробувань.

Опис методів випробувань АСЦО за окремими показниками рекомендується розташовувати в тій же послідовності, в якій ці показники розташовані в технічних вимогах.

Результати приймальних випробувань АСЦО (елемента системи) фіксуються в протоколі випробувань.

4. Уведення в експлуатацію АСЦО

Відповідно до встановленої практики термін «уведення в експлуатацію» будь-якої автоматизованої інформаційної системи, а саме АСЦО, визначає подію (дію), яка документально оформлена відповідним розпорядчим документом в установленому порядку, щодо використання цієї системи за призначенням при позитивних результатах приймальних випробувань.

Уведення в експлуатацію передбачає виконання таких попередніх основних заходів та/або робіт:

навчання персоналу і перевірку його здатності забезпечити функціонування АСЦО;

комплектацію АСЦО відповідно до проектної документації;

монтаж технічних засобів і засобів телекомунікацій відповідно до встановлених норм, стандартів і правил;

автономне пусконалагодження технічних та програмних засобів і комплексну перевірку функціонування АСЦО у цілому для проведення приймальних випробувань.

VII. Вимоги до АСЦО

1. Функціональні вимоги:

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 відповідної адміністративно-територіальної одиниці (району, міста, об'єднаної територіальної громади), доведення до громадян сигналів цивільного захисту;

автоматизоване доведення до населення створеної у визначеному районі зони оповіщення попереджувальних сигналів небезпеки «УВАГА ВСІМ!»;

автоматичне або автоматизоване приймання, передавання в реальному масштабі часу та реєстрація вхідної і вихідної інформації;

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

документування (протоколювання) вхідної та вихідної інформації, подій, усіх процесів оповіщення та інформування населення і дій користувачів автоматизованої системи централізованого оповіщення з можливістю формування друкованих звітів;

упровадження єдиної інформаційної бази (бази даних) автоматизованої системи централізованого оповіщення для автоматизованого або автоматичного приймання (передавання) формалізованої інформації (даних, документів) щодо оповіщення та інформування населення та/або інформаційної взаємодії;

інформаційна взаємодія між елементами автоматизованої системи централізованого оповіщення, з автоматизованими системами централізованого

оповіщення інших рівнів, іншими автоматизованими системами, що належать до єдиної державної системи цивільного захисту;

циркулярне, циркулярне за завчасно визначеними сценаріями, вибіркове або за пріоритетом передавання інформації щодо оповіщення та інформування населення;

доведення сигналів і повідомлень до осіб з фізичними, психічними, інтелектуальними та сенсорними порушеннями, керівників підприємств, установ і організацій УТОСу та УТОГу, інших підприємств, установ і організацій, що надають послуги особам з інвалідністю та маломобільним групам населення, визначених місцевими органами виконавчої влади та органами місцевого самоврядування, або за місцем роботи зазначених осіб (у доступній для них формі), керівників інтернатних закладів, закладів охорони здоров'я, які мають ліжковий фонд, установ виконання покарань, слідчих ізоляторів;

2. Вимоги до стійкості роботи системи:

автоматичне збереження інформації у разі відмови та збоїв;

автоматичний контроль та діагностика стану програмних, технічних та комунікаційних засобів;

упровадження багаторівневого доступу згідно зі встановленими пріоритетами і правами доступу до мережевих та інформаційних ресурсів автоматизованої системи централізованого оповіщення;

упровадження технічних і програмних засобів із функціями забезпечення інформаційної безпеки інформаційних та мережевих ресурсів автоматизованої системи централізованого оповіщення;

автоматичне за встановленими сценаріями (алгоритмами) змішане резервування елементів (технічних засобів) автоматизованої системи централізованого оповіщення;

3. Вимоги до надійності роботи системи:

коефіцієнт технічного використання — не менш як 0,95;

коефіцієнт готовності — не менш як 0,98;

середній строк служби — не менш як 10 років;

середній наробіток до відмови — не менш як 15000 год;

середня тривалість відновлення — не більше ніж 0,5 год.

Ці показники аналізуються, уточнюються, узгоджуються та регламентуються в проектній документації Розробником та Замовником на етапі проектування відповідно до ДСТУ 2861, ДСТУ 2862, ДСТУ 3524.

4. Вимоги до сумісності:

програмно-технічна сумісність складових частин програмно-технічного комплексу із загальним інтерфейсом, що забезпечує введення-виведення даних, єдину структуру даних та базується на єдиних схемних, конструктивних та

інших програмно-технічних рішеннях з максимальним використанням уніфікованих елементів програмно-технічного комплексу автоматизованої системи централізованого оповіщення;

взаємозамінюваність у програмно-технічному комплексі автоматизованої системи централізованого оповіщення уніфікованих програмних засобів та змінних однотипних виробів, компонентів, модулів.

5. Вимоги до конструкції:

використання серверних технічних засобів та технічних засобів телекомунікацій у варіанті для монтажу в стійках або серверних шафах типу Rack Mount;

використання технічних засобів, не призначених для монтажу в серверних шафах, у комплекті з полицями для їх монтажу з наступним поміщенням у серверні шафи типу Rack Mount;

відповідність технічних засобів, які можуть застосовуватися в програмно-технічному комплексі автоматизованої системи централізованого оповіщення, вимогам нормативних документів з питань безпечної експлуатації обладнання, інформаційних технологій та безпеки;

використання технічних засобів телекомунікацій, включених до Переліку технічних засобів, які можуть застосовуватися в телекомунікаційних мережах загального користування України, відповідно до Положення про порядок визначення переліку технічних засобів, які можуть застосовуватися в телекомунікаційних мережах загального користування України, та погодження застосування засобів телекомунікацій, не внесених до цього переліку, затвердженого наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 17 березня 2014 року № 115, зареєстрованого у Міністерстві юстиції України 10 квітня 2014 року за № 405/25182.

6. Вимоги до програмного забезпечення:

використання операційних систем та систем керування базами даних із відкритими програмними кодами;

наявність прикладних програм функціонального призначення програмно-технічного комплексу системи, що забезпечують:

підтримку дій відповідальних осіб, які приймають (готують) рішення щодо оповіщення населення про загрозу виникнення або виникнення надзвичайних ситуацій та контролюють результативність їх виконання;

виконання заданих алгоритмів обробки, маршрутизації, відображення і зберігання інформації та управління інформаційними базами даних з можливістю зміни їх конфігурації та реалізації через стандартні бібліотечні блокові структури;

автоматичний контроль, діагностика та перевірка працездатності;

захист інформації від несанкціонованого доступу і неправильних дій користувачів;

мультисервісний обмін даними між елементами (компонентами) системи;

обмін даними з автоматизованими системами централізованого оповіщення інших рівнів та складовими єдиної державної системи цивільного захисту;

відповідність програмних модулів, які входять до складу прикладної програми, таким умовам:

відсутність ділянок коду, що викликають появу рекурентних циклів або статичних витоків пам’яті;

відсутність системних помилок, що призводять до часткового або повного виходу з ладу прикладної програми або технічних засобів;

компонування елементів програмного коду, що здійснюють обробку даних за стандартними алгоритмами, у вигляді окремих бібліотек, крім критичних до швидкості виконання ділянок коду;

реалізація можливості реструктуризації програмно-технічного комплексу системи без зміни прикладних програм за рахунок незалежності подання даних на концептуальному, програмному і фізичному рівнях;

налаштування прикладної програми під час доопрацювання, зміни переліку і структури вхідної та вихідної інформації без необхідності зміни програмного коду.

7. Інформаційне забезпечення та інформаційна взаємодія

1) Процес управління оповіщенням та інформуванням населення при загрозі виникнення або виникненні надзвичайної ситуації в основному має полі-ієрархічну структуру (рисунок 5).

Від ефективності інформаційної взаємодії між усіма АСЦО, які задіяні у процесі оповіщення в зоні впливу надзвичайної ситуації, може залежати у кінцевому підсумку результативність заходів щодо зниження людських втрат та матеріальних збитків у надзвичайних ситуаціях.

Протокол інформаційної взаємодії між АСЦО всіх рівнів повинен відповідати вимогам та рекомендаціям національного стандарту — ДСТУ ISO/TR 22351.

Щодо інформаційної взаємодії АСЦО із іншими суміжними інформаційними системами єдиної державної системи цивільного захисту (за необхідністю) в проектній документації повинно бути визначено:

необхідні відомості щодо протоколу обміну даними низького рівня;

необхідні відомості щодо протоколу обміну даними прикладного рівня;

алгоритм взаємодії між системами;

визначення об’єму та змісту вхідної та вихідної інформації для конкретної АСЦО і суміжної АС;

перелік параметрів, що визначають цілісність інформації.

Рисунок 5. Циклограма процесу управління оповіщенням населення

Вимоги до протоколів інформаційної взаємодії АСЦО із суміжними інформаційними системами єдиної державної системи цивільного захисту обґрунтовуються Розробником і узгоджуються із Замовником на етапі проектування.

2) Вимоги до інформаційного забезпечення та інформаційної взаємодії:

реалізація автоматизованою системою централізованого оповіщення інформаційної взаємодії між складовими частинами програмно-технічного комплексу системи, із автоматизованими системами централізованого оповіщення інших рівнів та іншими інформаційними системами єдиної державної системи цивільного захисту за допомогою спеціального програмного забезпечення;

покладення в основу побудови інформаційного забезпечення таких принципів:

спадкоємність із використання накопиченої інформації у функціонуючих системах оповіщення;

мінімізація дублювання з уведення (приймання) і накопичення даних в інформаційній базі даних;

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

простота і зручність доступу до інформації;

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

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

захист від недостовірної і несанкціонованої інформації;

перешкодостійке кодування і захист інформації від руйнування і несанкціонованого доступу;

регламентація доступу до інформаційних даних з різним рівнем доступу, а також часу зберігання документованої інформації;

у всіх випадках багаторазового введення або прийняття інформації передбачення заходів із запобігання розбіжностям та недостовірності інформації, а також із сигналізації про істотну розбіжність інформації в різних складових частинах програмно-технічного комплексу автоматизованої системи централізованого оповіщення;

передбачення заходів з виділення корисних складових інформації під час введення і первинної обробки сигналів (команд) оповіщення;

дотримання під час кодування інформації таких основних вимог:

відповідність набору мнемонічних знаків і їх колірного кодування набору, який прийнятий для автоматизованої системи централізованого оповіщення, і відображення функціонального технологічного вмісту;

кодування нормальної, попереджувальної, аварійної та недостовірної інформації різними кольорами, які не мають використовуватися з іншою метою (системні кольори);

для привернення уваги користувача виділення інформації, що має попереджувальний або аварійний характер, миготінням та супроводження її звуковими сигналами відповідного тону;

відображення недостовірної інформації кольором, який відрізняється від кольору основного фону або позначається миготливим символом;

лаконічність, вичерпність за змістом й однотипність за формою текстів повідомлень;

забезпечення інформаційної сумісності, сумісності взаємодії та інтеграції між автоматизованими системами централізованого оповіщення всіх рівнів шляхом створення єдиного інформаційного середовища на основі протоколу інформаційного обміну даними (взаємодії) прикладного рівня стеку інтернет-протоколу TCP/IP;

відповідність протоколу інформаційної взаємодії між автоматизованими системами централізованого оповіщення всіх рівнів вимогам нормативних документів з питань структури інформаційних повідомлень при управлінні в надзвичайних ситуаціях.

Загальні відомості щодо формату обміну даними наведено у додатку 2 до Рекомендацій.

8. Вимоги до інформаційної безпеки і захисту інформації:

надання доступу до функцій прикладних програм та інформації лише авторизованим користувачам з урахуванням їх службових повноважень, а також категорії інформації, яка запитується;

блокування спроб модифікації чи знищення інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з непідтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора;

вирішення технічних рішень авторизованого доступу до інформації наданням кодів (фізичних ключів або логічних паролів) доступу користувачам, забезпечення надання прав доступу користувачам на підставі авторизації, ідентифікації та автентифікації;

визначення таких категорій користувачів:

користувач — відповідальна особа за здійснення заходів згідно з функціональними обов'язками, яка пройшла навчання і допущена до роботи з відповідним автоматизованим робочим місцем, зокрема, черговий персонал оперативно-чергових (чергових, диспетчерських) служб;

адміністратор — уповноважена особа, яка пройшла навчання та уповноважена щодо:

перегляду або зміни конфігурації програмно-технічного комплексу та надання кодів доступу за типом (категорією) «користувач»;

перегляду статистичних даних журналів (архіву) за результатами дій користувачів системи за типом (категорією) «користувач»;

здійснення технічного обслуговування програмно-технічного комплексу автоматизованої системи централізованого оповіщення тощо;

розробник — особа, яка пройшла навчання та уповноважена щодо заміни (модифікації) технічних та/або програмних засобів;

впровадження таких рівнів доступу:

рівень доступу 1 — доступ необмеженого кола осіб, відповідальних за первинне реагування на повідомлення (лише статистичний перегляд цієї інформації без будь-якого втручання щодо її обробки);

рівень доступу 2 — доступ користувачів за категорією «користувач»;

рівень доступу 3 — доступ користувачів за категорією «адміністратор» (рівень доступу 3 виконується лише через рівень доступу 2);

рівень доступу 4 — доступ користувачів за категорією «розробник» (рівень доступу 4 виконується лише через рівень доступу 3);

надання прав авторизованого доступу до інформаційного ресурсу та функціонування у складі автоматизованої системи централізованого оповіщення програмним та технічним засобам автоматизованого робочого місця;

проведення авторизації, ідентифікації та автентифікації будь-якого програмного та/або технічного засобу автоматизованого робочого місця з використанням його унікального реєстраційного номера, який присвоюється програмному та/або технічному засобу для конкретного автоматизованого робочого місця;

розділення доступу до функцій прикладних програм програмно-технічного комплексу та інформаційного ресурсу як мінімум на чотири рівні;

створення для автоматизованої системи централізованого оповіщення, її інформаційних баз та сховищ даних (електронних архівів) комплексної системи захисту інформації з підтвердженою відповідністю згідно із Законом України «Про захист інформації в інформаційно-телекомунікаційних системах».

9. Вимоги до автоматизованого робочого місця:

1) забезпечення за допомогою функціональних можливостей прикладних програм автоматизованого робочого місця ефективного виконання користувачами автоматизованої системи централізованого оповіщення таких етапів дій (рисунок 6):

перший етап — сприйняття вхідної інформації (повідомлень, сигналів, команд, документів) щодо оповіщення;

другий етап — оцінка інформації;

третій етап — прийняття рішення про дії на основі аналізу інформації;

четвертий етап — виконання прийнятого рішення шляхом певних дій або надання відповідних розпоряджень (команд);

п’ятий етап — контроль за результативністю виконання прийнятих рішень;

Рисунок 6. Етапи дій користувача АРМ

2) забезпечення екранними інтерфейсами засобів відображення інформації (дисплеї, спеціальні табло) автоматизованого робочого місця можливості швидкого та безпомилкового сприйняття інформації для її оцінки та прийняття правильного рішення (рисунок 7);

Рисунок 7. Приклад АРМ

3) розташування важливої інформації, яка вимагає прийняття рішення, в межах оптимальної для сприйняття зони відображення;

4) відображення аварійної інформації (про відмови, несправності, збої) та другорядної, яка використовується періодично, поза межами оптимальної зони відображення;

5) об'єднання способів і засобів ведення діалогу користувача з прикладним програмним забезпеченням в уніфіковані сценарії з максимальним використанням ієрархій меню;

6) отримання користувачем повідомлень про наявність помилок у вигляді попереджувальної (звукової та візуальної) сигналізації за допомогою програмного контролю помилкових дій (відображення повідомлення про наявність помилки і її характер в контрольному рядку або на спеціальній ділянці екрану автоматизованого робочого місця);

7) забезпечення органів управління інтерфейсу користувача, випадковий вплив на які неприпустимий, спеціальним захистом, зняття якого потребує виконання не менше двох дій;

8) забезпечення автоматизованого робочого місця таким мінімальним набором функцій:

автоматизоване вибіркове або за пріоритетом передавання оперативної інформації (повідомлень, сигналів, команд, документів) щодо оповіщення;

підготовка та автоматизоване вибіркове або за пріоритетом у будь-якому напрямку передавання формалізованої та/або неформалізованої інформації (повідомлень, документів) про загрозу виникнення, виникнення надзвичайної ситуації (залежно від її рівня: державного, регіонального, місцевого) та оперативної інформації про стан обстановки під час ліквідації наслідків надзвичайної ситуації для її аналізу, прийняття рішень, оповіщення та інформування населення;

введення вручну за допомогою сенсомоторних пристроїв (маніпулятор «миша», клавіатура) текстової та/або символьної (алфавітно-цифрової) інформації;

автоматичне та/або автоматизоване приймання та реєстрація інформації (повідомлень, сигналів, команд, документів);

автоматичне та/або автоматизоване підтвердження приймання інформації (повідомлень, сигналів, команд, документів);

візуальна та/або звукова попереджувальна сигналізація про підтвердження (непідтвердження) приймання переданої інформації;

індикація контролю технічного стану автоматизованого робочого місця і каналів обміну даними (візуальна та/або звукова попереджувальна сигналізація);

індикація контролю технічного стану прикінцевих технічних засобів оповіщення та інформування населення і каналів обміну даними з ними (візуальна та/або звукова попереджувальна сигналізація);

перегляд задокументованої (запротокольованої) вхідної та/або вихідної інформації (повідомлень, сигналів, команд, документів) з можливістю формування друкованих звітів;

підготовка формалізованих статистичних звітів та інших документів.

9) врахування в проектних рішеннях за узгодженням із Замовником вимог та рекомендацій до ергономіки та технічної естетики АРМ таких 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 ПЗ);

ДСТУ ISO 9241-14 (вимоги до діалогових меню);

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

Остаточні вимоги обґрунтовуються Замовником та узгоджуються з Розробником у процесі проектування.

10. Кінцеві технічні пристрої оповіщення населення

1) У Рекомендаціях термін «кінцеві технічні пристрої оповіщення» визначає комплекси технічних пристроїв, що призначені для своєчасного доведення звукових, візуальних сигналів та інформаційних повідомлень про небезпеку при загрозі виникнення або виникненні надзвичайній ситуації до людей, які можуть знаходиться або знаходяться в небезпеці.

2) Вимоги до кінцевих технічних пристроїв оповіщення населення:

автоматизоване або автоматичне приведення сигнальних технічних пристроїв (електросирени, спеціальні звукові системи на основі гучномовців, спеціальні світлові джерела візуальних сигналів) протягом 3 секунд з моменту надходження відповідної команди в режим функціонування за призначенням;

безвідмовність, ремонтопридатність, спроможність виконувати необхідні функції в будь-який момент часу (кінцеві технічні пристрої, які можуть застосовуватися у системах оповіщення населення, повинні відповідати вимогам до безпеки національного стандарту — ДСТУ EN 60950-1);

забезпечення резервним електроживленням з метою збереження працездатності кінцевих технічних пристроїв у разі відключення централізованого енергопостачання або відмови первинного електроживлення (Технічні засоби електроживлення кінцевих технічних пристроїв оповіщення, що мають бути визначені в проектних рішеннях, повинні відповідати вимогам Технічного регламенту низьковольтного електричного обладнання, затвердженого постановою Кабінету Міністрів України від 16 грудня 2015 р. № 1067);

забезпечення резервним джерелом електроживлення працездатності кінцевих технічних пристроїв оповіщення в черговому режимі протягом 24 годин та в режимі передавання сигналів оповіщення протягом подвоєного часу евакуації, але не менше 30 хвилин;

забезпечення кінцевих технічних пристроїв оповіщення автоматичними зарядними пристроями, якщо як резервне джерело електроживлення використовуються акумуляторні батареї (автоматичні зарядні пристрої мають забезпечувати зарядку акумуляторів до 80 % їх максимальної місткості протягом не більше 24 годин, свинцево-кислотні батареї мають бути обладнані пристроями обмеження їх повного розряджання відповідно до рекомендацій виробника);

кінцеві технічні пристрої, що використовуються в системі централізованого оповіщення, повинні відповідати Орієнтовному переліку нормативних документів у сфері телекомунікацій, що визначають технічні вимоги до кінцевого обладнання, яке призначене для з'єднання з пунктом закінчення телекомунікаційної мережі, затвердженому наказом Адміністрації Держспецзв'язку від 26.01.2018 № 38.

11. Телекомунікаційна мережа

1) Для потреб автоматизованих систем централізованого оповіщення використовуються ресурси телекомунікаційних мереж загального користування, Національної телекомунікаційної мережі, державної системи урядового зв'язку та Національної системи конфіденційного зв'язку.

2) Проекти будівництва та реконструкції автоматизованих систем централізованого оповіщення мають передбачати заходи щодо резервування каналів та ліній зв'язку (у тому числі безпроводового) для здійснення управління технічними засобами оповіщення, а проектні рішення – встановлення спеціальних технічних засобів для переривання трансляції програм мовлення з метою передавання сигналів та інформації через програми теле- та радіомовлення.

VIII. Експлуатація АСЦО

1. Експлуатація — це стадія життєвого циклу АСЦО, на якій реалізується, підтримується і відновлюється її якість. Експлуатація системи включає в себе використання її за призначенням, технічне обслуговування, супровід і ремонт.

Важливим елементом експлуатації АСЦО є визначення режимів її функціонування.

2. Режими роботи автоматизованої системи централізованого оповіщення:

штатний режим (основний режим роботи) — забезпечення безперервного виконання всіх функцій системи незалежно від режимів функціонування єдиної державної системи цивільного захисту (повсякденне функціонування, підвищена готовність, надзвичайна ситуація, надзвичайний стан);

режим відновлення після збоїв, відмов (аварійний режим) — відновлення функціонування на основі змішаного резервування (проектні рішення мають передбачати автоматичне відновлення функціонування основних елементів системи без порушення працездатності в цілому);

режим технічного обслуговування (адміністративний, сервісний режим) — проведення заходів щодо супроводу, технічного обслуговування, подальшого вдосконалення та модифікації;

режим навчання персоналу.

Технологічні та технічні умови реалізації режимів функціонування АСЦО обґрунтовуються Розробником та погоджуються Замовником на етапі проектування.

3. Контроль стану елементів системи

1) Мають бути реалізовані наступні критерії реалізації моніторингу та контролю (далі — моніторинг) стану елементів (компонентів) програмно-технічного комплексу системи:

повна готовність до виконання покладених функцій;

обмежена здатність щодо виконання покладених функцій;

збій або відмова.

2) У разі виникнення аварійних ситуацій або помилок у роботі програмно-технічного комплексу автоматизованої системи централізованого оповіщення інструменти контролю зберігають повний набір інформації, необхідної користувачеві і розробникові для ідентифікації проблеми (знімки екранів, коди помилки (збою), поточний стан пам’яті та файлової системи програмних засобів).

3) Компоненти інструментів контролю:

забезпечують виявлення непрацездатності власних технічних та програмних засобів, які входять до складу елементів (компонентів) програмно-технічного комплексу автоматизованої системи централізованого оповіщення та засобів інформаційного обміну, сумісності і взаємодії;

контролюють канали обміну даними з мережевими телекомунікаційними засобами, які використовуються для передавання/приймання сигналів (команд) оповіщення (як мінімум, фізичне пошкодження внутрішніх каналів обміну даними має бути визначено та розпізнано).

4) У разі несправності каналів обміну даними генерується та подається інформація про їх несправність, а також генерується застережна сигналізація.

5) активація засобів безперервного контролю прикладних програм супроводжується відповідними повідомленнями та застережною сигналізацією.

4. Збереження інформації у разі відмов та збоїв

1) Програмно-технічний комплекс системи:

стійкий до хибних дій користувача (помилки в діях персоналу не повинні призводити до відмов (збоїв) у роботі);

забезпечує гарантований контроль вхідної та вихідної інформації;

забезпечує регламентований час відновлення після відмови (збою).

2) Інформація зберігається у разі:

збою або відмови технічних засобів;

збою або відключення електроживлення;

відмови каналів обміну даними;

збою або відмови операційної системи;

збою або відмови прикладної програми.

3) Прикладні програми:

виконують функції автоматичного дублювання і резервування даних;

відновлюють своє функціонування у разі коректного перезапуску технічних засобів зі збереженням усіх даних.

4) У разі збою або відключення електроживлення апаратних засобів, що призводить до перезавантаження операційної системи і прикладної програми, відновлення прикладної програми відбувається після перезапуску операційної системи і запуску виконуваного файлу прикладної програми. Дані конфігурацій прикладної програми у такому разі не втрачаються.

5) Для відновлення даних і прикладної програми з резервної копії використовуються засоби автоматичного та/або ручного резервного копіювання й архівації, які входять до складу програмних засобів. Для скорочення об’єму копійованих даних забезпечується копіювання лише змін з попереднього копіювання, періодичність повного копіювання даних обґрунтовується на етапі проектування.

6) Передбачається можливість відновлення даних за допомогою їх повторного введення або імпорту (для даних із зовнішніх систем, що отримуються автоматично).

5. Технічне обслуговування системи

1) Вимоги до технічного обслуговування:

проведення комплексу робіт з підтримки цілодобового функціонування автоматизованої системи централізованого оповіщення в усіх режимах;

забезпечення справного стану програмно-технічних засобів під час їх використання за призначенням та необхідних показників надійності протягом усього строку експлуатації;

постійна присутність обслуговуючого персоналу технічних засобів автоматизованої системи централізованого оповіщення та її елементів (компонентів, частин) не є обов'язковою.

2) Види технічного обслуговування, види діяльності щодо технічного обслуговування та тривалість технічного обслуговування автоматизованої системи централізованого оповіщення визначаються відповідно до нормативних документів з питань технічного обслуговування (ДСТУ EN 13306).

3) Документація на технічне обслуговування автоматизованої системи централізованого оповіщення визначається відповідно до нормативних документів з питань технічного обслуговування (ДСТУ EN 13460).

6. Супровід системи

1) Супровід програмних засобів відповідно до нормативних документів з питань застосування процесів життєвого циклу програмного забезпечення відповідно до ДСТУ ISO/IEC 14764 включає:

коригувальний супровід — модифікація програмних засобів після передачі Замовнику Розробником (Постачальником) для коригування виявлених проблем (невідповідностей, помилок, збоїв) з метою приведення у відповідність зі встановленими вимогами;

адаптивний супровід — модифікація програмних засобів на етапі експлуатації для забезпечення продовження використання із заданою ефективністю (з точки зору потреб Замовника) у зміненому оточенні, що породжує нові вимоги до системи;

супровід із вдосконалення — модифікація програмних засобів на етапі експлуатації для підвищення його ефективності або зручності супроводу;

профілактичний супровід — модифікація програмних засобів на етапі експлуатації з метою виявлення та коригування наявних прихованих помилок для запобігання прояву цих помилок при експлуатації;

2) Роботи із супроводу програмних засобів проводяться для вирішення таких завдань:

усунення збоїв;

поліпшення дизайну інтерфейсів користувачів;

реалізація розширень функціональних можливостей;

створення інтерфейсів інформаційної взаємодії з іншими (зовнішніми) інформаційними системами;

адаптація програмних засобів для можливості роботи на іншій технічній платформі (або оновленій платформі), застосування нових системних можливостей, функціонування в середовищі оновленої телекомунікаційної мережі тощо;

виведення окремого прикладного програмного забезпечення з експлуатації.

7. Навчання персоналу

У режимі навчання персоналу забезпечується робота АСЦО паралельно з іншими режимами (штатний режим, режим технічного обслуговування і режим відновлення після збоїв).

Крім цього, у такому режимі повинен забезпечуватися захист від несанкціонованого втручання та некваліфікованих дій користувачів, що може привести до пошкодження інформації (даних) або складати загрозу її (їх) цілісності.

Повинна забезпечуватися коректна обробка даних, викликана неправильними діями користувачів, неправильним форматом або неприпустимими значеннями вхідних даних. У вказаних випадках користувачам повинно видаватися відповідне повідомлення з поверненням прикладної програми у стан, що передував неправильній (неприпустимій) команді або некоректному введенню даних.

Начальник управління
оповіщення, телекомунікацій
та інформаційних технологій
Департаменту організації
заходів цивільного захисту
ДСНС України **Владислав КРАВЧЕНКО**