МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

НАКАЗ

08.02. 2019 м. Київ № 93

Зареєстровано в Міністерстві юстиції України
"22" квітня 2019 р.
за № 418/33389
Керівник реєструючого органу _____
підпис

Про затвердження Інструкції щодо практик чи процедур проектування, дослідження, введення в експлуатацію, експлуатації та технічного обслуговування (супроводження) автоматизованих систем централізованого оповіщення

Відповідно до пункту 4 частини другої статті 17, статті 19 Кодексу цивільного захисту України, пунктів 9 та 10 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 року № 733, пункту 4 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, з метою проведення реконструкції (створення) автоматизованих систем централізованого оповіщення про загрозу або виникнення надзвичайних ситуацій

НАКАЗУЮ:

1. Затвердити Інструкцію щодо практик чи процедур проектування, дослідження, введення в експлуатацію, експлуатації та технічного обслуговування (супроводження) автоматизованих систем централізованого оповіщення, що додається.

2. Управлінню взаємодії з Державною службою України з надзвичайних ситуацій МВС (Скакун В. О.) забезпечити подання цього наказу на державну реєстрацію до Міністерства юстиції України в установленому порядку.

3. Цей наказ набирає чинності з дня його офіційного опублікування.

Міністр **А. Б. Аваков**

ЗАТВЕРДЖЕНО
Наказ Міністерства внутрішніх справ України
08 лютого 2019 року № 93

Зареєстровано в Міністерстві юстиції України
"12" квітня 2019 р.
за № 418/33389
Керівник реєструючого органу _____
підпис

ІНСТРУКЦІЯ
щодо практик чи процедур проектування, дослідження, введення в експлуатацію, експлуатації та технічного обслуговування (супроводження) автоматизованих систем централізованого оповіщення

І. Загальні положення

1. Ця Інструкція встановлює вимоги щодо проектування, дослідження, введення в експлуатацію, експлуатації та технічного обслуговування (супроводження) автоматизованих систем централізованого оповіщення.

Ця Інструкція призначена для використання постійно діючими органами управління цивільного захисту на регіональному та місцевому рівнях в процесі реалізації проектних рішень щодо технічної реконструкції (створення) місцевих та територіальних автоматизованих систем централізованого оповіщення, а також для підготовки приймальної документації, методик попередніх (у процесі верифікації), приймальних (у процесі валідації) та експлуатаційних випробувань.

2. Терміни, що використовуються у цій Інструкції, вживаються у значеннях, наведених у Кодексі цивільного захисту України, Законах України «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах» та «Про основні засади забезпечення кібербезпеки України».

ІІ. Основні вимоги до процесу проектування автоматизованої системи централізованого оповіщення

1. Вимоги до автоматизованої системи централізованого оповіщення:

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.

2. Вимоги до сумісності:

1) 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;

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

3. Вимоги до конструкції:

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

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

3) 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;

4) 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.

4. Вимоги до програмного забезпечення:

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

2) 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;

3) 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;

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

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

5. Вимоги до інформаційного забезпечення та інформаційної взаємодії:

1) 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;

2) 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;

3) 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;

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

5) 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;

6) 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;

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

6. Вимоги до інформаційної безпеки і захисту інформації:

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

2) 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;

3) 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;

4) 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;

5) 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);

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

7) 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;

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

9) 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».

7. 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:

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;

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;

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.

8. Вимоги до кінцевих технічних пристроїв оповіщення населення:

1) 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;

2) безвідмовність, ремонтопридатність, спроможність виконувати необхідні функції в будь-який момент часу;

3) забезпечення резервним електроживленням з метою збереження працездатності кінцевих технічних пристроїв у разі відключення централізованого енергопостачання або відмови первинного електроживлення;

4) 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 ніж 30 хвилин;

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

6) кінцеві технічні пристрої, що використовуються в системі централізованого оповіщення, повинні мати виданий у встановленому

законодавством порядку документ про підтвердження відповідності вимогам нормативних документів у сфері телекомунікацій.

9. 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.

Проекти будівництва та реконструкції автоматизованих систем централізованого оповіщення мають передбачати заходи щодо резервування каналів та ліній зв'язку (у тому числі бездротового) 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.

III. Уведення в експлуатацію та експлуатація автоматизованої системи централізованого оповіщення

1. Основні заходи та/або роботи щодо введення в експлуатацію автоматизованої системи централізованого оповіщення:

навчання персоналу й перевірка його здатності забезпечити функціонування автоматизованої системи централізованого оповіщення;

комплектація системи відповідно до проектної документації;

монтаж технічних засобів і засобів телекомунікацій;

автономне пусконалагодження технічних та програмних засобів і комплексна перевірка функціонування системи в цілому для проведення приймальних випробувань.

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.

3. Контроль стану елементів системи:

1) 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 мають 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 обслуговувального персоналу технічних засобів автоматизованої системи централізованого оповіщення та її елементів (компонентів, частин) не є обов'язковою;

2) види технічного обслуговування та тривалість технічного обслуговування автоматизованої системи централізованого оповіщення визначаються відповідно до нормативних документів з питань технічного обслуговування;

3) документація на технічне обслуговування автоматизованої системи централізованого оповіщення визначається відповідно до нормативних документів з питань технічного обслуговування.

06. Супровід системи:

1) супровід програмних засобів відповідно до нормативних документів з питань застосування процесів життєвого циклу програмного забезпечення включає коригувальний супровід, адаптивний супровід, супровід із вдосконалення, профілактичний супровід;

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.

Начальник Управління взаємодії з Державною службою України з надзвичайних ситуацій Міністерства внутрішніх справ України **В. О. Скакун**