ПЛАН-КОНСПЕКТ

для проведення заняття в системі службової підготовки із середнім та старшим начальницьким складом (Групи №1,2) Вищого професійного училища Львівського державного університету безпеки життєдіяльності (м. Вінниця)

Вид підготовки: профільна підготовка

Тема № 17 Автоматизовані системи управління і комп'ютерні мережі та їх практичне використання в управлінні органами та підрозділами цивільного захисту

Навчальна мета: Ознайомити із основними автоматизованими системи управління і комп'ютерні мережі та їх практичне використання в управлінні органами та підрозділами цивільного захисту

Час: 1 год.

Місце проведення : лекційний зал

Метод проведення : Лекція.

Навчально-матеріальне забезпечення: 1.Кодекс цивільного захисту України;

Нормативно-правові акти та література:

1 Автоматизовані системи управління та зв'язок: курс лекцій / Уклад. Л.В. Борисова, О.В. Закора, А.Б. Фещенко. – Х : НУЦЗУ, 2018. – 282 с.

2. Бурляй І.В., Джулай О.М., Орел Б.Б. Системи радіозв'язку та їх застосування оперативно-рятувальною службою: посібник з дисципліни «Основи електроніки та зв'язок». – Черкаси: Черкаський інститут пожежної безпеки ім. Героїв Чорнобиля МНС України, 2007. – 224 с.

3. Поповський В.В. Основи теорії телекомунікаційних систем: підручник. – Харків: ХНУРЕ, 2018. – 368 с.

4. В. О. Собина, Д. В. Тарадуда, М. М. Піксасов, Л. В. Борисова, О. В. Закора, А. Б. Фещенко, М.В. Маляров, Д. Л. Соколов. Дослідження проблем функціонування системи зв'язку ДСНС, використання засобів телекомунікацій та інформатизації в системі ДСНС, шляхів їх розвитку із застосуванням сучасних телекомунікаційних та інформаційних технологій, Звіт про НДР: № держреєстрації 0119U001009, Х. : НУЦЗУ, 2020. – 85 с. URL: http://ndr.dsns.gov.ua/?p=7135.

5. Микитишин А.Г. Комп'ютерні мережі. Навч. посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник – Львів, «Магнолія 2006», 2013. – 256 с.

6. Про затвердження Положення про функціональну підсистему «Система управління силами та засобами цивільного захисту» єдиної інформаційної системи Міністерства внутрішніх справ Наказ; МВС України від 20.04.2023 № 326

Порядок проведення заняття:

1. **Організаційні заходи** – 2 хв.:
- перевірка присутніх; оголошення теми і мети заняття.

2. Викладення матеріалу теми. - 50 хв.

Питання, які вивчатимуться:

Автоматизовані системи управління в ДСНС

ПИТАННЯ № 1 АВТОМАТИЗОВАНІ СИСТЕМИ УПРАВЛІННЯ В ДСНС

Наразі в підрозділах ДСНС функціонують оперативно-координаційні центри, до яких надходять повідомлення від громадян про надзвичайні ситуації за номером «101». Повідомлення обробляють диспетчери та направляють за вказаними адресами необхідну кількість сил та засобів. Введення нових Центрів управління дозволить автоматизувати процеси обробки повідомлень від громадян. Нові алгоритми роботи, оновлена апаратна складова та програмне забезпечення дозволять суттєво скоротити час відправки рятувальних підрозділів на надзвичайну подію. До того ж підвищать оперативні можливості рятувальників у ліквідації пожеж та наслідків надзвичайних подій.

У межах програми заплановано обладнати пожежно-рятувальну техніку GPS-трекерами та планшетами, що будуть під'єднанні до системи Центрів управлінн. Рятувальники через планшети зможуть користуватись загальною базою даних. Зокрема, прокладати найкоротші маршрути до місць надзвичайних подій, користуватися картками та планами пожежогасіння, схемами вододжерел, мати останню інформацію щодо протипожежного стану об'єктів.

Диспетчери Центрів управління зможуть відслідковувати всю рятувальну техніку, що слідує або працює на місцях надзвичайних подій та координувати дії оперативно-рятувальних підрозділів за допомогою нового програмного забезпечення.





1. Система управління силами та засобами цивільного захисту

Про затвердження Положення про функціональну підсистему «Система управління силами та засобами цивільного захисту» єдиної інформаційної системи Міністерства внутрішніх справ Наказ; МВС України від 20.04.2023 № 326

1.1 Система управління силами та засобами цивільного захисту (СУСЗ) – це інтегрована інформаційно-комунікаційна система, що забезпечує збирання, зберігання, використання, передачу, захист інформації про сили та засоби цивільного захисту, об'єкти, на яких існує загроза виникнення надзвичайних ситуацій, пожеж та інших небезпечних подій, у тому числі об'єкти підвищеної небезпеки, надзвичайні ситуації, небезпечні події, у тому числі пожежі, а також іншої інформації, необхідної для керування силами та засобами цивільного захисту, а також оперативно-диспетчерського управління ними.

Адміністратором СУСЗ є визначена власником СУСЗ установа, що належить до сфери управління ДСНС і забезпечує:

реалізацію заходів з інформаційного, технічного і програмно-технологічного функціонування СУСЗ;

визначення порядку та правил управління інформаційною безпекою, політики та підходів до управління ризиками;

відповідно до компетенції надання, обмеження, припинення користувачам доступу до СУСЗ у випадках, передбачених цим Положенням та іншими нормативно-правовими актами, визначеними законодавством;

здійснення заходів зі створення, підтримки та технічного адміністрування інформаційно-комунікаційних засобів, програмних та апаратних компонентів, що використовуються для забезпечення функціонування СУСЗ;

реалізацію інформаційної взаємодії та інтеграцію з іншими реєстрами, електроними інформаційними ресурсами, засобами центральної підсистеми єдиної інформаційної системи Міністерства внутрішніх справ (далі - ЦП ЄІС МВС);

організацію впровадження та вдосконалення програмно-апаратних засобів ведення СУСЗ;

збереження та захист інформації від втрати, знищення, незаконної обробки та незаконного доступу до інформації, що міститься в ресурсах СУСЗ;

організація заходів із створення, упровадження, забезпечення функціонування та адміністрування ресурсів СУСЗ;

здійснення заходів із кібербезпеки;

виконання інших завдань, визначених законодавством, для ефективного функціонування СУСЗ.

Комплексна система захисту інформації забезпечує захист інформації в СУСЗ шляхом здійснення комплексу технічних, криптографічних, організаційних та інших заходів і використання засобів захисту інформації, спрямованих на недопущення блокування доступу до інформації, несанкціонованого доступу та/або її модифікації

Обробка та захист інформації в СУСЗ здійснюються відповідно до вимог Законів України «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних» та інших нормативно-правових актів.

1.2. Загальні вимоги до формування електронних інформаційних ресурсів

1. *Для функціонування СУСЗ* та її складових частин використовуються власні та залучені із ЦП ЄІС МВС підсистеми, модулі, сервіси, інформаційні ресурси.

2. *До архітектури СУСЗ* входять:

сховище даних – програмно-технічні комплекси, які складаються із серверів баз даних та програмного забезпечення, призначені для безперервної обробки та зберігання інформації, ведення та зберігання системних журналів аудиту роботи користувачів СУСЗ, системних журналів реєстрації роботи програмних засобів і журналів аудиту засобів безпеки;

ервери застосувань – програмно-технічні комплекси, які складаються із серверів та програмного забезпечення, призначених для безперервного функціонування програмних засобів обробки інформації в інтерактивному режимі реального часу, архівування та синхронізації інформації, записування та зберігання системних журналів аудиту приймання та передачі інформації, реєстрації роботи програмних засобів і журналів аудиту засобів безпеки;

шлюзові сервери – програмно-технічні комплекси, які складаються із серверів та програмного забезпечення, призначених для забезпечення захисту інформації під час її приймання та передачі до сховища даних, а також для запобігання можливості блокування доступу до програмно-апаратних ресурсів СУСЗ;інші сервери та електронне комунікаційне обладнання, які можуть використовуватися для виконання завдань та функцій СУСЗ у процесі його функціонування;

автоматизовані робочі місця користувачів СУСЗ – робочі місця, обладнані програмно-технічними засобами доступу до відповідних програмно-інформаційних комплексів, призначені для забезпечення користувачам можливості обробляти інформацію відповідно до наданих прав;

автоматизовані робочі місця адміністратора СУСЗ – робочі місця, обладнані технічними засобами та програмним забезпеченням, призначеними для моніторингу системних журналів реєстрації роботи програмних засобів, аналізу порушень у роботі СУСЗ, налагодження параметрів, необхідних для забезпечення стабільної роботи програмних та технічних засобів СУСЗ;

комплексна система захисту інформації – взаємопов’язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації в СУСЗ.

3. *Інформація, що обробляється* в СУСЗ, повинна відповідати форматам, визначеним для електронних інформаційних ресурсів єдиної інформаційної системи Міністерства внутрішніх справ (ЄІС МВС), та узгодженим показникам для їх автоматизованої обробки, використання та надання суб’єктам СУСЗ в уніфікованому вигляді, а також єдиним правилам її класифікації та кодифікації шляхом використання відповідних класифікаторів, кодифікаторів та уніфікованих довідників.

4. *У СУСЗ вноситься інформація*:

від заявників, отримана за допомогою засобів зв’язку, повідомлень користятувачів мобільного застосунку «Служба порятунку 101», автоматизованих систем охоронно-пожежної сигналізації;

про надзвичайні ситуації, небезпечні події, у тому числі пожежі;

про сили та засоби цивільного захисту, відомчої пожежної охорони, пожежно-рятувальних підрозділів для забезпечення місцевої та добровільної пожежної охорони, що можуть залучатися до ліквідації пожежі, наслідків надзвичайної ситуації, небезпечної події, їх місцезнаходження, географічні координати, відображення на цифрових електронних картах районів виїзду;

ро об’єкти, на яких є загроза виникнення надзвичайних ситуацій, пожеж та інших небезпечних подій, у тому числі об’єкти підвищеної небезпеки, їх місцезнаходження, географічні координати, відображення на цифрових електронних картах, плани та картки пожежогасіння на об’єкти з їх описовою інформацією та характеристиками, сили та засоби цивільного захисту, що можуть залучатися до ліквідації наслідків надзвичайних ситуацій, пожеж та небезпечних подій на цих об’єктах;

про місцезнаходження/географічні координати (геолокація) джерел водопостачання;

про розпорядження та інші документи, пов’язані з керуванням силами та засобами цивільного захисту;про спеціалізовані служби цивільного захисту та їх дії в ході ліквідації наслідків надзвичайної ситуації, небезпечної події;

про плани та картки пожежогасіння на об’єкти інфраструктури з їх описовою інформацією та характеристиками та сили і засоби цивільного захисту, що залучаються до ліквідації наслідків надзвичайної ситуації, небезпечної події;

з місця події про хід ліквідації наслідків надзвичайної ситуації, небезпечної події (короткі повідомлення керівника гасіння пожежі про послідовність дій на місці ліквідації наслідків надзвичайної ситуації, небезпечної події, розпорядження керівника гасіння пожежі про необхідність залучення додаткових сил та засобів, інших екстрених служб);

про захисні споруди цивільного захисту;

про вибухонебезпяяяяечні предмети;

про укладення та дострокове припинення дії договорів страхування відповідальності за шкоду, яка може бути заподіяна третім особам унаслідок надзвичайних ситуацій, небезпечних подій, у тому числі пожеж та аварій на території та/або об’єктах нерухомості;

про організації, що проводять аудит пожежної та техногенної безпеки, та експертів у сфері пожежної та техногенної безпеки;

інша інформація, яка обробляється ДСНС у межах виконання покладених на неї завдань.

5. *Унесення інформації в СУСЗ та її зміна здійснюються користувачами СУСЗ*, права доступу яких дозволяють здійснити відповідну дію, за допомогою технічних засобів та програмних комплексів СУСЗ.

6. У разі виявлення факту *внесення користувачем СУСЗ недостовірної інформації* та/або неправомірного поширення користувачем СУСЗ інформації з

обмеженим доступом, яка міститься в СУСЗ, такий користувач (за відповідним зверненням володільця СУСЗ) обмежується в доступі або позбавляється доступу до СУСЗ.

7. *Строки зберігання інформації,* що обробляється в СУСЗ, установлюються згідно із законодавством.

8. *Обробка електронних документів* у СУСЗ здійснюється відповідно до вимог законодавства про електронні документи та електронний документообіг. На всі електронні документи, о вносяться, формуються, приймаються в СУСЗ, накладається кваліфікований електронний підпис та/або електронна печатка.

9. Під час *обробки інформації в СУСЗ* повинна зберігатися її цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації, спотворення чи знищення, зокрема шляхом накладення кваліфікованого електронного підпису та/або електронної печатки.

10. *Інформація, що обробляється* в СУСЗ, може бути змінена уповноваженою особою суб'єкта СУСЗ, якій у встановленому порядку надано право доступу до інформації в СУСЗ, за допомогою технічних засобів та програмних комплексів СУСЗ у разі виявлення факту введення недостовірної інформації, а також в інших випадках, передбачених законодавством.

Інформація, що внесеа та зберігається в СУСЗ і зазнала будь-яких змін, зберігається в новій версії відповідного інформаційного об'єкта. Зберігається також інформація про всі внесені зміни. Видалення чи знищення інформації із СУСЗ можливе лише у випадках, передбачених законодавством.

1.3. Порядок доступу до інформації в СУСЗ

1. Доступ до публічної інформації у формі відкритих даних СУСЗ реалізується через сервіси на офіційних веб-сайтах ДСНС без електронної ідентифікації особи.

2. Доступ фізичних, юридичних осіб до інформації про них в електронній формі, що обробляється в СУСЗ, здійснюється з використанням засобів електронної ідентифікації особи засобами ЦП ЄІС МВС, що відповідають вимогам законодавства.

3. Суб'єкти СУСЗ, уповноваженим особам яких надано доступ до СУСЗ, для реалізації своїх повноважень зобов'язані негайно, але не пізніше двох робочих днів із дня припинення виконання користувачем СУСЗ своїх повноважень, письмово повідомити адміністратора СУСЗ про необхідність блокування доступу до СУСЗ такого користувача.

4. Користувачі СУСЗ зобов'язані дотримуватися визначеного МВС порядку роботи з електронними інформаційними ресурсами ЄІС МВС та використовувати отриману інформацію відповідно до законодавства.

5. Доступ користувачів СУСЗ до автоматизованих робочих місць СУСЗ здійснюється із застосуванням засобів електронної ідентифікації, що відповідають вимогам законодавства, у межах реалізації своїх повноважень.

6. Обсяг прав доступу, який надається користувачу СУСЗ, визначається відповідним суб'єктом СУСЗ з урахуванням вимог законодавства. Про будь-яку дію щодо інформації в СУСЗ, а також про користувача СУСЗ, який учинив відповідну дію, автоматично робиться унікальний запис у системному журналі аудиту роботи користувачів СУСЗ, який зберігається відповідно до положень, визначених у вимогах до комплексної системи захисту інформації.

7. Право перегляду інформації в СУСЗ належить виключно користувачам СУСЗ (у межах їх прав доступу) з використанням для здійснення такого доступу засобів електронної ідентфікації, крім публічної інформації у формі відкритих даних.

8. Розголошення персональних даних про особу забороняється, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Власник СУСЗ та адміністратор СУСЗ уживають у межах компетенції відповідних заходів для забезпечення зберігання, запобігання несанкціонованому доступу та поширенню інформації із СУСЗ.

3.4. Автоматизовані системи централізованого оповіщення цивільного захисту, їх класифікація, організація та принципи застосування

Відповідно до Положення про організацію оповіщення про загрозу виникнення або виникненя надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту від 27 вересня 2017 р. № 733:

автоматизована система оповіщення – сукупність алгоритмів дій, процесів (заходів), технологій, а також організаційно і технічно поєднаних програмних і технічних засобів електронних комунікацій, засобів обробки та передачі (відображення) інформації, що забезпечують своєчасне доведення сигналів та інформації з питань цивільного захисту до органів виконавчої влади, органів місцевого самоврядування, органів управління і сил цивільного захисту, підприємств, установ, організацій та населення в разі загрози виникнення або під час виникнення надзвичайних ситуацій;

інформування населення у сфері цивільного захисту – доведення органами управління цивільного захисту за допомогою медіа, каналів мовлення або ефірних багатоканальних електронних комунікаційних мереж, а також з використанням Інтернету, засобів операторів мобільного зв'язку та інших технічних засобів відомостей про надзвичайні ситуації, що прогнозуються або виникли, з визначенням їх класифікації, меж поширення і наслідків, про способи та методи захисту від них, а також про свою діяльність з питань цивільного захисту, в тому числі з урахуванням особливостей оповіщення осіб з фізичними, психічними, інтелектуальними та сенсорними порушеннями.

Класифікація:

загальнодержавна автоматизована система централізованого оповіщення – автоматизована система оповіщення, призначена для оповіщення оперативно-чергових (чергових, диспетчерських) служб центральних органів

виконавчої влади, що створюють функціональні підсистеми єдиної державної системи

цивільного захисту, обласних, Київської та Севастопольської міських держадміністрацій, а також оперативно-чергових служб центрів управління в надзвичайних ситуаціях територіальних органів ДСНС;

локальна система оповіщення – автоматизована система оповіщення на об'єкті підвищеної небезпеки, гідротехнічній споруді або гідроелектростанції напірного типу (крім Дніпровського та Дністровського каскадів), продуктопроводі (крім магістральних аміако-, нафто- та газопроводів), призначена для оповіщення персоналу об'єкта та населення в разі загрози виникнення та під час иникнення надзвичайних ситуацій, внаслідок яких зона можливого ураження (катастрофічного затоплення) також досягає територій інших об'єктів або заселених територій;

місцева автоматизована система централізованого оповіщення – автоматизована система оповіщення, призначена для оповіщення населення, осіб керівного складу місцевих органів виконавчої влади, органів місцевого самоврядування, а також чергових (диспетчерських) служб підприємств, установ та організацій незалежно від форми власності на території відповідної адміністративно-територіальної одиниці (району, територіальної громади);

об'єктова система оповіщення – автоматизована система оповіщення на об'єкті з масовим перебуванням людей, призначена для оповіщення персоналу об'єкта та населення, яке перебуває на його території, в разі загрози виникнення та під час виникненнянадзвичайних ситуацій, внаслідок яких зона можливого ураження не виходить за територію об'єкта;

спеціальна система оповіщення – автоматизована система оповіщення, яка створюється на таких об'єктах, як гідротехнічні споруди Дніпровського та Дністровського каскадів, атомні електростанції, магістральні аміакопроводи, нафто- та газопроводи, і призначена для оповіщення персоналу об'єкта та населення в разі загрози виникнення або під час виникнення надзвичайних ситуацій на об'єкті та в зонах можливої дії уражаючих факторів;

територіальна автоматизована система централізованого оповіщення – автоматизована система оповіщення, призначена для оповіщення осіб керівного складу і чергових служб відповідних місцевих органів виконавчої влади, органів місцевого самоврядування, а також чергових (диспетчерських) служб підприємств, установ, організацій та населення через місцеві автоматизовані системи централізованого оповіщення та інші системи оповіщення;

За рівнями системи оповіщення згідно до Кодексу Цивільного Захисту України у Розділі IV «Захист населення і територій від надзвичайних ситуацій» (ст.30) поділяються на загальнодержавну автоматизовану систему централізованого оповіщення, територіальні автоматизовані системи централізованого оповіщення, місцеві автоматизовані системи централізованого оповіщення, а також спеціальні, локальні та об'єктові системи оповіщення, систем циркулярного виклику. Ці системи забезпечують оповіщення і подальше інформування:

чергових служб міністерств та інших центральних органів виконавчої влади по службових телефонах;

чергових служб місцевих органів виконавчої влади;

чергових аварійно-рятувальних служб.

Спеціальні системи оповіщення створюються і функціонують:

на атомних електростанціях;

на гідротехнічних спорудах Дніпровського та Дністровського каскадів та в зонах їх можливого катастрофічного затоплення;

на магістральних продуктопроводах.

Спеціальні системиоповіщення передбачають взаємодію з відповідними територіальними та місцевими автоматизованими системами централізованого оповіщення. Електронні комунікаційні послуги для потреб автоматизованих систем централізованого оповіщення надаються операторами електронних комунікацій на договірних засадах.

Між об'єктами, де функціонують спеціальні, локальні та об'єктові системи оповіщення, та оперативно-черговою (черговою) службою місцевих органів виконавчої влади (органів місцевого самоврядування) керівником об'єкта організовується безпосередній телефонний зв'язок.

Готовність систем оповіщення забезпечено шляхом:

організація цілодовового чергування відповідних служб;

налагодження телефонного зв'язку чергових служб потенційно небезпечних підпримств, зона ураження яких може поширюватися на заселені території або території інших підприємств, установ, організацій з оперативно-черговою службою пункту управління облдержадміністрації, чергових служб органів МВС в містах та районах області;

завчасна підготовка персоналу чергових служб до дій у надзвичайних ситуаціях;

впровадження автоматизованих систем оповіщення з використанням сучасних технологій;

проведення якісного експлуатаційно-технічного обслуговування апаратури оповіщення та інших технічних засобів зв'язку та оповіщення.

Забороняється зняття та відключення телекомунікаційних мереж, абонентських ліній, через які здійснюється запуск електросирен, демонтувати вуличні гучномовці без погодження з відповідними органами Департаменту.

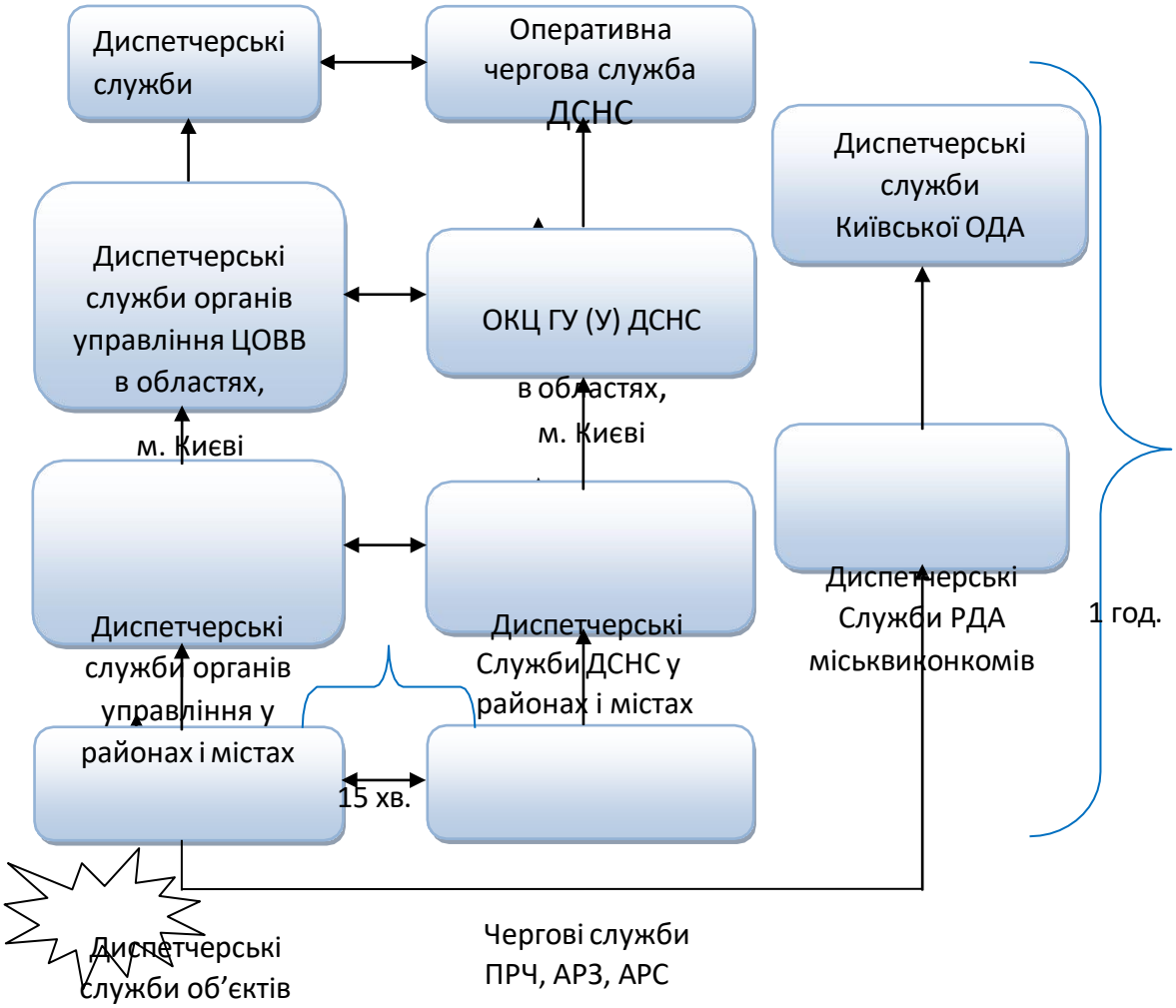
Порядок дій оперативно-чергових (чергових, диспетчерських) служб центральних та місцевих органів виконавчої влади, а також центрів управління мережами операторів електронних комунікацій, провайдерів програмної послуги, телерадіоорганізацій, засобів масової інформації незалежно від форми власності, які долучаються до оповіщення та інформування населення, під час передачі сигналів оповіщення та інформування населення визначається законодавством, зокрема положеннями про системи оповіщення, планами у сфері цивільного захисту.

Одним із головних способів оповіщення населення про небезпеку та шляхи рятування від дії їх вражаючих чинників є передача повідомлень по всіх мережах зв'язку, радіомовлення, через зовнішні гучномовці, а також через місцеві

радіомовні і телевізійні станції в разі їх наявності.

Система оповіщення на всіх рівнях Єдиної Державної Системи запобігання і реагування на НС техногенного та природного характеру – це організаційно-технічне об'єднання (організаційно-технічну систему) оперативних чергових служб органів управління ЦЗ, спеціальної апаратури управління і засобів оповіщення, а також каналів (ліній зв'язку), які забезпечують передачу команд управління і мовної інформації при НС. Системи централізованого оповіщення (СЦО) регіонального рівня є основною ланкою системи оповіщення в Україні.

Завданням СЦО регіонального рівня є оповіщення посадових осіб і сил місцевого і об'єктового рівнів та їх посадових осіб, а також населення, яке проживає на території, на яку поширюється дія СЦО цього рівня. Інформація, яка доводиться до органів управління і посадових осіб, має оперативний характер, а до населення доводиться інформація про характер і масштаби загрози та про дії людей в умовах НС. СЦО регіонального рівня мають забезпечувати як циркулярне, так і вибіркове включення СЦО місцевого і об'єктового рівня, а також оповіщення населення, яке проживає на території, яку охоплює система оповіщення цього рівня. Управління СЦО місцевого рівня може здійснюватися безпосередньо від оперативної чергової служби у місті або через чергового зміни вузла зв'язку міста.



НС

Рис. 47 – Схема проходження інформації від об’єкта де виникла НС

Використання цих систем в комплексі з існуючими мережами операторів мобільного зв'язку, які покривають практично всю територію України, зробить можливим розгорання мережі з глобальним оповіщенням практично 100 % населення і дозволить виконати наступні завдання:

побудувати мережу оповіщення населення і спеціальних структур;

організувати мережу оповіщення з мінімальними інфраструктурними витратами;

утворити простір поширення сигналів оповіщення незалежно від конкретного оператора та/або телекомунікаційної мережі;

здійснювати вибіркове оповіщення за територіальним розташуванням зони потенційної надзвичайної ситуації;

персоналізувати повідомлення для різних органів, таких як ДСНС, МВС та ін.;

здійснювати оповіщення зі встановленням пріоритетів за важливістю і формувати інструкції групам для їх негайного виконання;

проводити контроль і управління ситуацією щодо оповіщення; оперативно використовувати і спрямовувати необхідні ресурси для локалізації аварій, катастроф або будь-яких інших подій.

При розробці нових систем оповіщення населення про виникнення надзвичайних ситуацій необхідно передбачати автоматизовані системи досліджень (наземних, авіаційних, радарних, супутникових), систем збору та передачі даних із застосуванням сучасних засобів зв'язку, автоматичної обробкиданих спостережень і видачі актуальної інформації, сучасне доведення інформації до населення впровадженням сучасних інноваційних технологій.

Для управління суб'єктами забезпечення цивільного захисту у разі загрози виникнення або виникнення надзвичайних ситуацій використовуються ресурси електронних комунікаційних мереж загального користування, державної системи урядового зв'язку та Національної системи конфіденційного зв'язку.

1. Автоматизовані системи раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення населення (СРВНСО) (ДБН В.2.5-76:2014)

Автоматизована система класу «людино-машина», у якій суміщено автоматичні процеси виявлення загрози виникнення НС, спостереження та оброблення інформації щодо поточного стану об'єктів та будівель, інженерних споруд, мереж, що розташовані на територіях з ризиком прояву небезпечних природних явищ і процесів, оперативне надання користувачам фактичної та прогнозованої інформації, а також оповіщення (за необхідності) працівників та керівників об'єкта, відповідальних за стан техногенної безпеки, посадових осіб органів виконавчої влади та місцевого самоврядування і населення при безпосередній участі людини-оператора.

СРВНСО повинна виконувати такі функції:

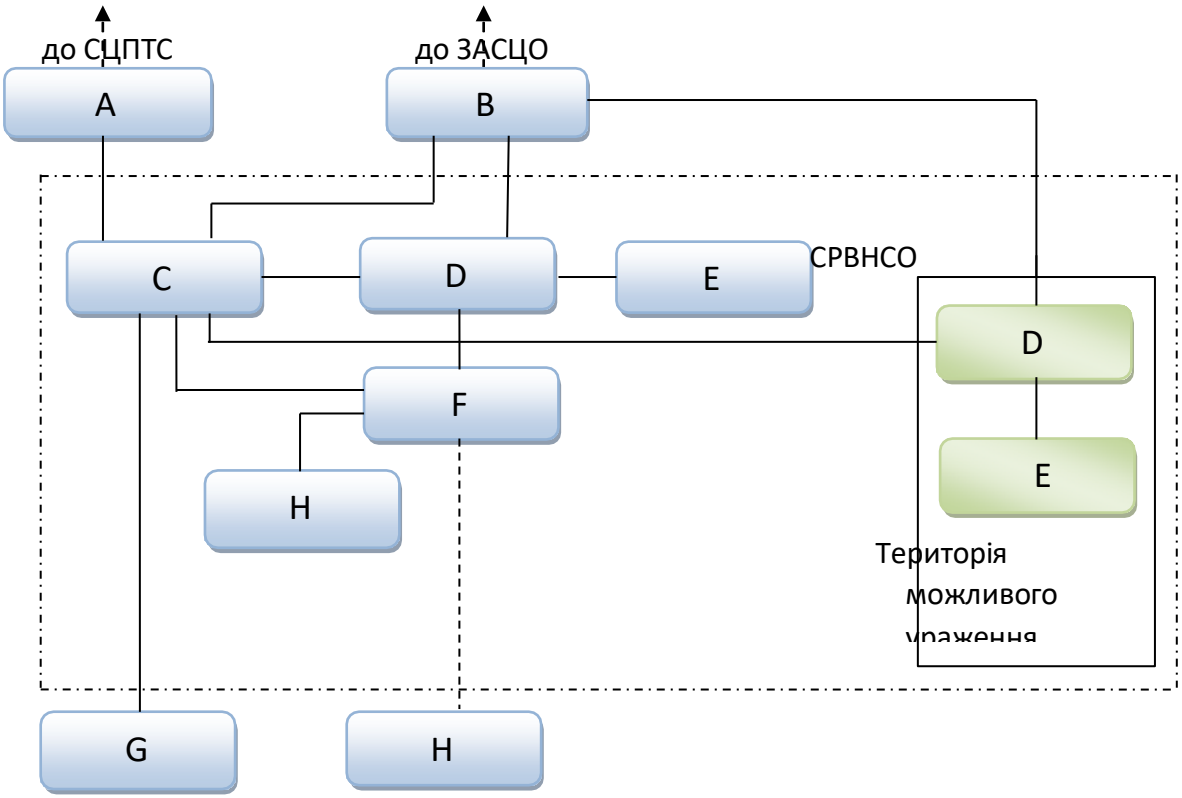
безперервно отримувати дані від джерел первинної інформації;

контролювати в реальному вимірі часу відповідність поточних (граничних) значень параметрів проектним режимам технологічного процесу об'єкта та (або) унормованим значенням параметрів джерел НС природного характеру;

інформувати працівників, відповідальних за функціонування технологічного обладнання, щодо виявлених фактів досягнення докритичних та критичних значень параметрів, які контролюють;

інформувати посадових осіб, які відповідають за стан техногенної безпеки об’єкта, про факти досягнення критичних значень параметрами, які контролюють.

Структурна схема СРВНСО наведена на рис. 48.



СЦПТС	Система централізованого пожежного та техногенного спостереження
ЗАСЦО	Загальнодержавна автоматизована система централізованого оповіщення
A – ПЦС	Пульт централізованого спостереження
B – ТАСЦО	Територіальна автоматизована система централізованого оповіщення
C – ПК	Пульт керування СРВНСО
D – ПО	Пристрій оповіщення
E – КТЗІО	Кінцеві технічні засоби інформування та оповіщення
F – КП	Комунікаційний пристрій
H	Джерела первинної інформації
G	Суміжні системи забезпечення безпеки

Рис. 48 – Структурна схема СРВНСО

СРВНСО отримує від оператора СРВНСО підтвердження прийняття сигналів про досягнення параметрами, які контролюються, докритичних та критичних значень, а також сигналів про спрацьовування ручних оповіщувачів. За відсутності підтвердження СРВНСО автоматично виконує інформування відповідальних посадових осіб по підприємству.

СРВНСО автоматично формує та за командою оператора СРВНСО передає до ПЦС тривожне сповіщення щодо виявлення загрози або виникнення НС разом із ідентифікатором електронної картки аварії, з можливістю отримання від ПЦС сигналу підтвердження його прийняття.

СВНСО та суміжні системи повинні програмно і апаратно суміщатись із ієрархічними структурами вищого рівня та між собою.

Інформаційна підтримка дій повинна здійснюється шляхом автоматизованого визначення та візуалізації певного сценарію розвитку НС. Сукупність усіх можливих сценаріїв розвитку НС зберігається у базі даних АРМ оператора СРВНСО у вигляді електронних карток аварії, які містять інформацію з оперативної частини планів локалізації і ліквідації аварії.

У разі відсутності підтвердження з боку ПЦС факту отримання тривожного сповіщення СРВНСО здійснює автоматичне телефонне з’єднання з оперативно-диспетчерською службою відповідного аварійно-рятувального підрозділу, на який відповідно до плану локалізації і ліквідації аварії покладено оперативне реагування на НС, з подальшою передачею тривожного мовного повідомлення, що містить ідентифікатор електронної картки аварії.

Джерелом первинної інформації для СРВНСО є існуючі на підприємстві технологічні датчики і сигналізатори промислової автоматики, що входять до складу систем протиаварійного захисту та автоматизованих систем керування технологічними процесами.

Комунікаційні пристрої забезпечують виконання таких функцій:

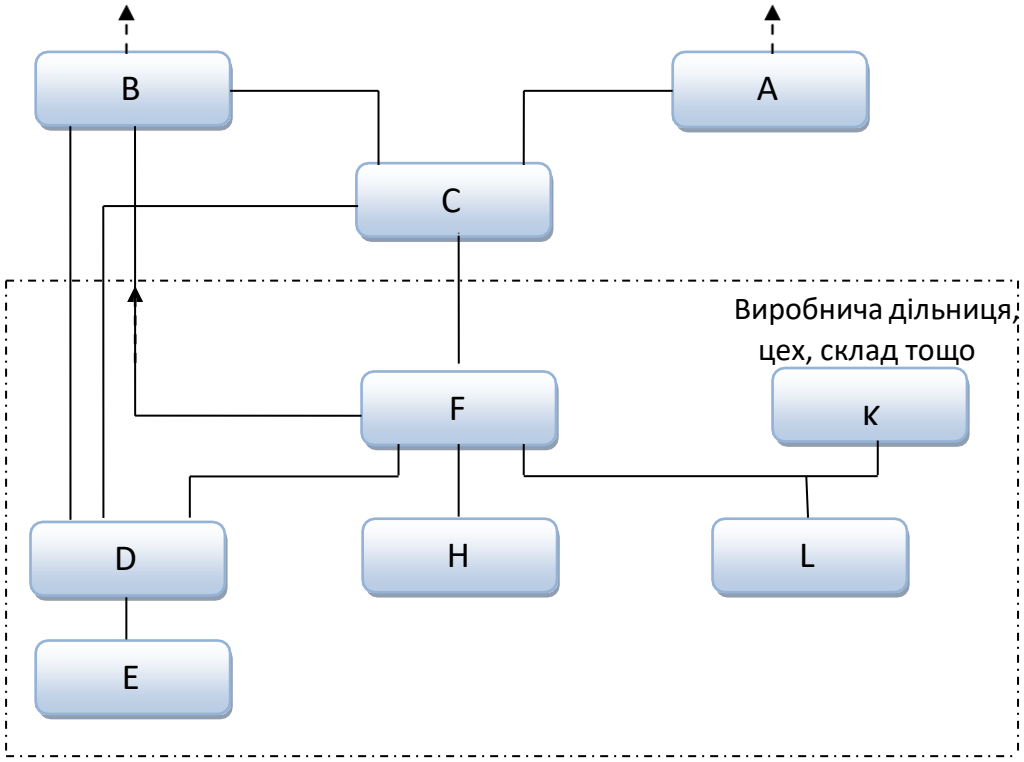
самодіагностування працездатності;

отримання даних від ДПІ щодо поточного стану джерел техногенної та (або) природної небезпеки, обробку отриманої інформації;

інформування респондентів щодо результатів оброблення інформації;

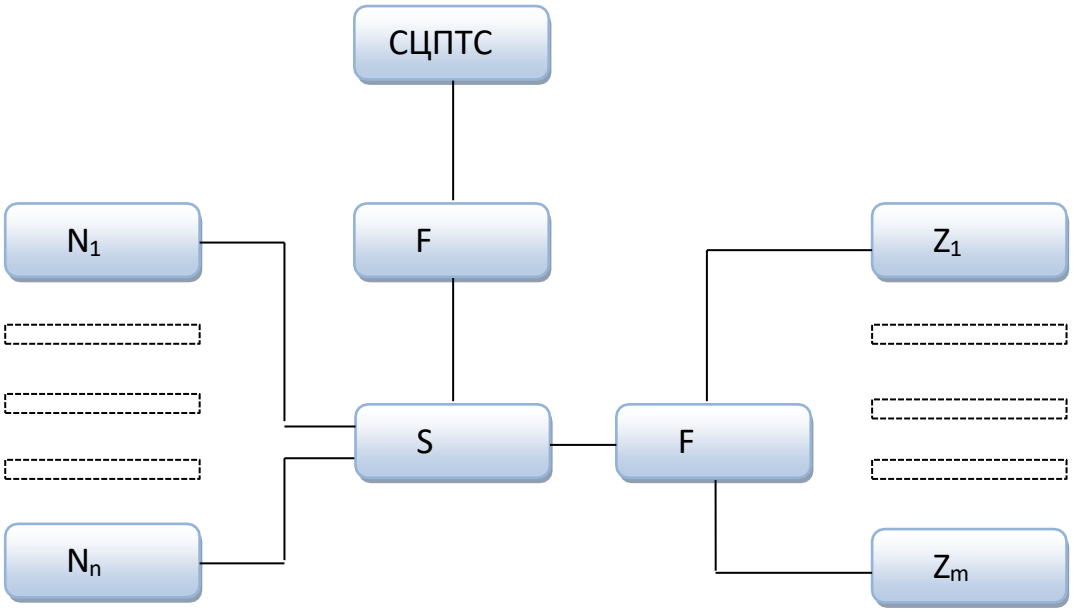
прийняття та виконання команд, що надходять від пульту керування СРВНСО;

формування архівного журналу.



СЦПТС	Система централізованого пожежного та техногенного спостереження
ЗАСЦО	Загальнодержавна автоматизована система централізованого оповіщення
А – ПЦС	Пульт централізованого спостереження
В – ТАСЦО	Територіальна автоматизована система централізованого оповіщення
С – ПК	Пульт керування
D – ПО	Пристрій оповіщення
Е – КТЗІО	Кінцеві технічні засоби інформування та оповіщення
– КП	Комунікаційний пристрій
Н – ДПІ	Джерела первинної інформації
К – ПДП	Пристрій дистанційного пуску
L – УЛНСРС	Установки локалізації/ліквідації НС на ранній стадії

Рис. 49 – Структурна схема установок локалізації/ліквідації НС на ранній стадії



СЦПТС	Система централізованого пожежного та техногенного спостереження
F	Комунікаційний пристрій
N – АРМ	Автоматизоване робоче місце оператора ПЦС
Z – СРВНСО	Автоматизовані системи раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення населення
S	Сервер

Рис. 50 – Пульт централізованого спостереження за СРВНСО

Канали зв'язку між СРВНСО, їх складовими та суміжними системами організовують з урахуванням забезпечення їх функціонування протягом часу, необхідного для виявлення НС, інформування та оповіщення, вжиття невідкладних заходів щодо ліквідування НС та їх наслідків, перш за все - евакуювання людей із зони НС.

2. Забезпечення функціонування апаратури і технічних засобів автоматизованих систем централізованого оповіщення та зв'язку, контроль за їх станом

Експлуатаційно-технічне обслуговування апаратури і технічних засобів оповіщення та технічних засобів електронних комунікацій – комплекс організаційно-технічних заходів щодо технічного обслуговування, поточного ремонту, планування експлуатації, а також здійснення контролю за забезпеченням надійного функціонування апаратури і технічних засобів оповіщення та технічних засобів електронних комунікацій.

Технічне обслуговування автоматизованих систем оповіщення здійснюється підготовленим технічним персоналом органу виконавчої влади (органу місцевого самоврядування), підприємства (установи, організації), на які покладено

створення автоматизованої системи оповіщення або на договірних засадах суб'єктами господарювання, що надають послуги у сфері електронних комунікацій (інформаційних технологій) відповідно до законодавства.

Контрольні перевірки готовності автоматизованих систем оповіщення здійснюються оперативно-черговими (черговими, диспетчерськими) службами пунктів управління всіх рівнів шляхом передачі контрольних сигналів управління та отримання підтвердження їх виконання в автоматичному (автоматизованому) режимі з періодичністю не менше одного разу на добу.

У разі виявлення несправностей апаратури і технічних засобів оповіщення та технічних засобів електронних комунікацій загальнодержавної (територіальної або місцевої) автоматизованої системи централізованого оповіщення органом виконавчої влади (органом місцевого самоврядування), що здійснює управління системою, та суб'єктом господарювання, що здійснює технічне обслуговування зазначеної апаратури і технічних засобів, негайно вживаються заходи до усунення несправностей.

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