

# 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

«СЛУЖБА ЗВ'ЯЗКУ»

№ держреєстрації 0119U001009

Звіт про НДР: 85 с., 2 рис., 27 джерел.

Об'єктом дослідження є організація зв'язку та інформатизації в ДСНС України у повсякденній діяльності та під час ліквідації надзвичайних ситуацій (НП).

Мета роботи – дослідження організації функціонування системи зв'язку ДСНС, застосуванням сучасних телекомунікаційних та інформаційних технологій, забезпечення кібербезпеки і кіберзахисту.

Методи дослідження – методи аналізу, аналогії, порівняння та систематизації.

Ключові слова: організація зв'язку, телекомунікаційний простір, система оповіщення, цифрова телекомунікаційна мережа.

Керівник роботи к.т.н., доцент В.О. Собина.

Відповідальний виконавець к.т.н., Д.В. Тарадуда.

Виконавці: к.т.н., доцент М.М. Піксов, к.ю.н., доцент Л.В. Боросова, к.т.н., доцент О.В.

Закора, к.т.н., доцент А.Б. Фещенко, к.т.н., доцент М.В. Маляр, к.т.н., доцент Д.Л. Соколов.

**ПОЛОЖЕННЯ**

**з організації зв'язку та інформатизації в ДСНС України**

(проект)

## **ЗМІСТ**

### **ВСТУП**

#### **1. СФЕРА ЗАСТОСУВАННЯ**

#### **2. НОРМАТИВНІ ПОСИЛАННЯ**

#### **3. ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ**

#### **4. ЗАГАЛЬНІ ПОЛОЖЕННЯ**

Організація телекомунікаційних систем та інформаційних технологій у ДСНС України

4.2 Служба зв'язку у ДСНС України

Призначення і завдання телекомунікацій

Призначення і завдання інформатизації

Технічний захист інформації

Кіберзахист та організація протидії кіберзагрозам

#### **5. ОРГАНІЗАЦІЯ ЗВ'ЯЗКУ В ДСНС УКРАЇНИ**

5.1 Організація каналів і мереж зв'язку

5.1.1 Радіозв'язок

5.1.2 Радіорелейний зв'язок

Супутниковий зв'язок

5.1.4 Проводовий зв'язок

5.2 Організація зв'язку у підрозділах ДСНС України

5.3 Організація зв'язку при взаємодії з органами управління інших міністерств, відомств і

служб

5.4 Організація зв'язку при ліквідації наслідків надзвичайних ситуацій

5.4.1 Особливості організації зв'язку при застосуванні морських (річкових) суден та проведенні підводних робіт

5.4.2 Особливості організації зв'язку під час проведення рятувальних робіт з ліквідації надзвичайних ситуацій в гірських районах

Організація зв'язку при застосуванні авіації

5.4.4 Організація зв'язку в метрополітенах і підземних об'єктах

5.5 Відновлення зв'язку і готовності підрозділів зв'язку

#### **ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ В ДСНС УКРАЇНИ**

6.1. Організація телефонного зв'язку

6.2. Організація роботи телекомунікаційної мережі

6.3 Організація відеоконференцзв'язку

6.4 Система оповіщення особового складу

6.5 Система контролю управління доступом

#### **ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДСНС УКРАЇНИ**

Організаційні заходи стосовно впровадження програмного забезпечення та його облік

7.2 Організація роботи електронної поштової системи

7.3. Система оперативно-диспетчерського управління (СОДУ)

7.4 Організація адміністрування телекомунікаційних систем та інформаційних технологій

#### **СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ**

8.1 Види робіт з ТЗІ, які можуть виконуватися підрозділами ТЗІ

8.1.1 Організація діяльності підрозділів ТЗІ

8.1.2 Умови та порядок надання повноважень на проведення робіт з технічного захисту інформації

8.2 Створення та впровадження комплексних систем захисту інформації

8.3 Створення та впровадження комплексів технічного захисту інформації

8.4 Організація заходів протидії кіберзагрозам

#### **СЛУЖБА ЗВ'ЯЗКУ ГАРНІЗОНУ**

9.1 Загальні положення

9.2 Структура служби зв'язку гарнізону

9.3 Структурні підрозділи зв'язку гарнізону

**ОРГАНІЗАЦІЯ ЕКСПЛУАТАЦІЇ ЗАСОБІВ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ  
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

10.1 Введення в експлуатацію телекомунікаційних систем та інформаційних технологій

10.2 Введення в експлуатацію технічних засобів

10.3 Введення в експлуатацію програмних засобів

10.4 Технічне обслуговування (супровід) телекомунікаційних систем та інформаційних технологій

10.5 Зберігання телекомунікаційного обладнання та засобів інформатизації

10.6 Контроль за станом систем, технічних і програмних засобів

**Додатки**

Додаток А. Умовні позначення та скорочення

Додаток Б. Основні документи, що регламентують діяльність підрозділів ДСНС з питань телекомунікацій та інформаційних технологій

Додаток В. Типові схеми телекомунікаційних мереж

Додаток Г. Типові журнали

Додаток Д. Правила ведення радіообміну

У даному Положенні викладено основні принципи з організації зв'язку, телекомунікаційних систем та інформаційних технологій, порядок використання засобів зв'язку, телекомунікаційних систем та інформаційних технологій, їх технічної експлуатації в підрозділах апарату ДСНС України, територіальних органах, підрозділах центрального підпорядкування, закладах освіти, підприємствах, організаціях та установах сфери управління ДСНС, підрозділи ДСНС, які не підпорядковуються безпосередньо апарату ДСНС.

## **1. СФЕРА ЗАСТОСУВАННЯ**

Положення є керівним документом з організації зв'язку, телекомунікаційних систем та інформаційних технологій в системі ДСНС та поширюється на підрозділи центрального апарату ДСНС, територіальні органи, підрозділи центрального підпорядкування, заклади освіти, підприємства, організації та установи сфери управління ДСНС, підрозділи ДСНС, які не підпорядковуються безпосередньо апарату ДСНС.

Положення визначає структуру підрозділів телекомунікаційних систем та інформаційних технологій сфери управління ДСНС, їх завдання, підпорядкованість, взаємодію з іншими підрозділами, порядок використання засобів телекомунікацій та інформатизації, а також основні положення з організації технічної експлуатації засобів телекомунікацій та інформатизації.

Положення встановлює порядок функціонування телекомунікаційних систем та інформаційних технологій, організацію зв'язку, використання засобів зв'язку в системі ДСНС у повсякденній діяльності та під час ліквідації наслідків НС (НП).

## **2. НОРМАТИВНІ ПОСИЛАННЯ**

У цьому документі є посилання на нормативні документи, які наведені у Додатку Б. Нормативні документи, посилання на які зроблено нижче, є нормативно-правовими, які регламентують вимоги у зазначеній сфері діяльності. У разі датованих посилань застосовують лише зазначене видання. У разі недатованих посилань треба користуватися останнім виданням документа, на який зроблено посилання (разом із будь-якими змінами до нього).

### 3. ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

**ВЦТМ** (відомча цифрова телекомунікаційна мережа ДСНС) – логічна цілісна мультисервісна багаторівнева телекомунікаційна мережа, яка здійснює взаємодію із загальнодержавними телекомунікаційними мережами спеціального зв'язку та загального користування і включає в себе сукупність технічних засобів й обладнання телекомунікаційної мережі доступу і транспортної телекомунікаційної мережі для забезпечення інформаційної взаємодії між суб'єктами ВЦТМ як у мирний час, так і в особливий період;

**Готовність**– здатність телекомунікаційних систем та інформаційних технологій забезпечити управління силами цивільного захисту ДСНС у будь-яких умовах оперативної обстановки в встановлені строки;

**Дозвіл**– документ, що надає право на виконання робіт з технічного захисту інформації для власних потреб;

**Достовірність**– це ступінь вірності відтворення переданих повідомлень на пунктах прийому;

**Доступність** – здатність телекомунікаційних систем та інформаційних технологій забезпечувати посадовим особам органів управління та черговому персоналу пунктів управління різних рівнів можливість користування достовірними інформаційними ресурсами при дотриманні встановлених пріоритетів і прав доступу до них, способів встановлення зв'язку і отримання інформації та забезпеченням суворого дотримання режимів роботи засобів телекомунікацій та інформатизації;

**Засоби інформатизації**– електронні обчислювальні машини, організаційна техніка, програмне, лінгвістичне та інше забезпечення, інформаційні системи або їх окремі елементи, інформаційні мережі і мережі зв'язку, що використовуються для реалізації інформаційних технологій;

**Зв'язок в ДСНС України** – процес приймання, передавання, розподілу та надання відповідної інформації з метою забезпечення ефективного керування системою управління ДСНС силами цивільного захисту у всіх режимах функціонування (режимах повсякденної діяльності, підвищеної готовності і надзвичайної ситуації), що реалізується адміністративним ресурсом ДСНС за допомогою сукупності телекомунікаційних мереж та технічних засобів зв'язку;

**Інформатизація в ДСНС України** – сукупність взаємопов'язаних організаційних, правових і науково-технічних процесів, що спрямовані на створення умов ефективного функціонування системи управління силами цивільного захисту ДСНС в режимах повсякденної діяльності, підвищеної готовності і надзвичайної ситуації на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки;

**Інформаційна система** – автоматизована система, комп'ютерна мережа або система зв'язку;

**Інформаційний ресурс** – сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо);

**Інформаційні ресурси ДСНС** відносять до державних інформаційних ресурсів, що підлягають захисту відповідно до порядку визначеному законодавством України шляхом впровадженням комплексу технічних, організаційних та інших заходів спрямованих на недопущення блокування інформації, несанкціонованого ознайомлення з нею та/або її модифікації;

**Інформація** – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

**Інформація з обмеженим доступом** – інформація, що становить державну або іншу передбачену законом таємницю, а також службова та конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України «Про доступ до публічної інформації», та інша конфіденційна інформація, вимога щодо захисту якої встановлена законом;

**Інцидент кібербезпеки**– подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами,



створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

**Кібератака**– спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

**Кібербезпека**– захищеність життєвоважливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

**Кіберзахист**– сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

**Кінцеве обладнання** – обладнання, призначене для з'єднання з пунктом закінчення телекомунікаційної мережі з метою забезпечення доступу до телекомунікаційних послуг;

**Комплекс ТЗІ** – сукупність організаційних, інженерних і технічних заходів та засобів, призначених для захисту від витоку інформації з обмеженим доступом технічними каналами на об'єктах інформаційної діяльності;

**Критична інформаційна інфраструктура**– сукупність об'єктів критичної інформаційної інфраструктури;

**Локальна телекомунікаційна мережа** – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень будь-якого виду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням у межах в межах адміністративної будівлі (комплексу адміністративних будівель) суб'єкта ВЦТМ;

**Мобільність** – здатність телекомунікаційних систем та інформаційних технологій у встановлені строки змінювати структуру відповідно до оперативної обстановки на об'єктах інформаційної діяльності.

**Надзвичайна ситуація у телекомунікаційних мережах**–порушення функціонування телекомунікаційних мереж внаслідок впливу чинників техногенного, природного, соціально-політичного або воєнного характеру чи інших чинників, що призвели або можуть призвести до виходу з ладу значної частини ресурсів, засобів телекомунікацій, перевантаження телекомунікаційних мереж, втрати енергопостачання тощо;

**Надзвичайний режим управління**– режим оперативно-технічного управління телекомунікаційними мережами, який встановлюється на час дії надзвичайної ситуації у телекомунікаційних мережах;

**Надійність** – здатність телекомунікаційних систем та інформаційних технологій забезпечити безперервне управління аварійно-рятувальними підрозділами у будь-яких умовах надзвичайних ситуацій;

**Національна телекомунікаційна мережа**– сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформаційних ресурсів,

забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам;

**Об'єкт інформаційної діяльності** – будівлі, приміщення, транспортні засоби чи інші інженерно-технічні споруди, функціональне призначення яких передбачає обіг інформації з обмеженим доступом;

**Об'єкт критичної інформаційної інфраструктури**– комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури;

**Оперативно-технічне управління телекомунікаційними мережами**– контроль за функціонуванням телекомунікаційних мереж і проведення організаційно-технічних заходів з управління телекомунікаційними мережами з метою забезпечення їх сталого та якісного функціонування;

**Підрозділ ТЗІ** – підрозділ, призначений для виконання робіт з технічного захисту інформації у системі ДСНС відповідно до повноважень, наданих ДСНС згідно з Дозволом на проведення робіт з технічного захисту інформації для власних потреб;

**Прихованість (таємність)** – здатність телекомунікаційних систем та інформаційних технологій обмеження несанкціонованого доступу до схем організації телекомунікацій, переданої інформації й засобів телекомунікації та інформатизації;

**Пропускна спроможність** – це можливість телекомунікаційних систем та інформаційних технологій забезпечити своєчасність передачі та обробки заданих потоків інформації;

**Рухомий (мобільний) зв'язок**– електровз'язок із застосуванням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися в межах усіх пунктів закінчення телекомунікаційної мережі, зберігаючи єдиний унікальний ідентифікаційний номер мобільної станції;

**Сервіси ВЦТМ** – сукупність телекомунікаційних послуг, які надаються за допомогою ВЦТМ;

**Система оперативно-технічного управління телекомунікаційними мережами (СОТУТМ)** – сукупність технічних засобів, центрів управління, у тому числі персоналу, для забезпечення сталого функціонування телекомунікаційних мереж в умовах надзвичайних ситуацій, надзвичайного та воєнного стану;

**Телекомунікаційні системи та інформаційні технології**– складова системи управління силами цивільного захисту, що є сукупністю взаємопов'язаних структурних підрозділів ДСНС, мереж та засобів телекомунікацій та інформатизації різного призначення, які діють узгоджено щодо завдань, місця, часу та використовуються. Розгортаються або створюються за планом для вирішення завдань забезпечення управління силами цивільного захисту;

**СКУД (система контролю і управління доступом)** – сукупність програмно-апаратних технічних засобів контролю і засобів управління, що мають на меті обмеження і реєстрацію входу-виходу об'єктів (людей, транспорту) на заданій території через «точки проходу»: двері, ворота, КПП;

**СОДУ (система оперативно-диспетчерського управління)** – це організаційно-технічне поєднання програмно-технічного комплексу чергової оперативно-диспетчерської служби, програмно-технічних комплексів підпорядкованих підрозділів, оперативно-координаційного центру, підрозділів (вузлів) технічного забезпечення центру телекомунікаційних систем та інформаційних технологій;

**Суб'єкт ВЦТМ** – територіальні органи, заклади освіти, установи та підприємства, які підпорядковуються ДСНС;

**Телекомунікаційна мережа** – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням;

**Телекомунікаційна система** – сукупність технічних і програмних засобів, призначених для

обміну інформацією шляхом передавання (випромінювання) або приймання сигналів, знаків, звуків, рухомих чи нерухомих зображень тощо;

**Телекомунікації (електрозв'язок)** – передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах;

**Технічний захист інформації (ТЗІ)**– діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації;

#### **4. ЗАГАЛЬНІ ПОЛОЖЕННЯ**

##### **Організація телекомунікаційних систем та інформаційних технологій у ДСНС України**

Організація телекомунікаційних систем та інформаційних технологій має відповідати вимогам чинних нормативно-правових актів. Перелік основних нормативних документів стосовно телекомунікаційних систем та інформаційних технологій розміщено на Порталі обстеження ІТ-систем органів виконавчої влади.

Мова інтерфейсу програмних продуктів і документації інформаційних систем – українська, а у разі відсутності україномовного інтерфейсу – англійська.

За можливості створення телекомунікаційних систем та інформаційних технологій цілком або виконання частини етапів зі створення без залучення сторонніх організацій підрозділи ДСНС можуть виступати не тільки як замовники, але й як виконавці.

Створення і впровадження нових телекомунікаційних систем та інформаційних технологій у ДСНС відбувається за погодженням зі структурним підрозділом, що відповідає за напрям інформаційні технології в апараті ДСНС. Телекомунікаційні системи та інформаційні технології створюються та впроваджуються за обґрунтованим поданням підрозділу для забезпечення підвищення ефективності виконання покладених на нього завдань. Необхідність створення телекомунікаційних систем та інформаційних технологій визначає керівник підрозділу.

Вимоги до телекомунікаційних систем та інформаційних технологій формуються і визначаються відповідним структурним підрозділом або робочою групою (за необхідністю), за участю представників відповідних структурних підрозділів, до компетенції яких належать завдання її створення і застосування за призначенням.

Технічне завдання розробляється за необхідністю, відповідно до чинного законодавства, рекомендацій національних стандартів і встановленої практики визначеної виконавцем робіт на основі узгоджених із замовником вимог до телекомунікаційних систем та інформаційних технологій.

Усі програмні, програмно-технічні (зокрема, вихідний код програмних засобів і команди компілятора, алгоритми, структури і формати даних тощо) та організаційні (регламенти, вимоги, інструкції, обмеження тощо) проектні рішення, які можуть застосовуватися для підтримки потрібного рівня експлуатаційних характеристик (якості) в процесі експлуатації й супроводу телекомунікаційних систем та інформаційних технологій, мають бути узгоджені, затверджені та передані замовнику виконавцем робіт (розробником) у задокументованому вигляді, необхідному для опису повної сукупності прийнятих проектних рішень і достатньому для їхнього незалежного використання (без звернення до розробника). Застосування недокументованих рішень заборонено.

Телекомунікаційні системи та інформаційні технології вводяться в експлуатацію наказом керівника підрозділу, в якому зазначаються підрозділи, які використовують телекомунікаційні системи та інформаційні технології, та визначаються відповідальні за її технічний супровід, а також затверджується відповідна нормативна документація телекомунікаційних систем та інформаційних технологій.

##### **4.2 Служба зв'язку в ДСНС**

Основними призначенням служби зв'язку ДСНС відповідно до галузевого спрямування діяльності є організація та забезпечення надійним зв'язком органів управління та сил

Оперативно-рятувальної служби цивільного захисту в умовах загрози виникнення і виникнення НС (НП), здійснення контролю за організацією та виконанням заходів щодо підтримання у готовності автоматизованих систем централізованого оповіщення про загрозу або виникнення НС (НП) для оповіщення центральних та місцевих органів виконавчої влади, органів управління та сил цивільного захисту в мирний час та в особливий період.

Основними завданнями служби є:

у режимі повсякденного функціонування:

підготовка та здійснення контролю за готовністю підрозділів служби до дій за призначенням, їх забезпечення;

організація проведення навчання фахівців, які входять до складу спеціалізованої служби;

підтримання в готовності техніки і майна спеціального призначення для виконання завдань, покладених на спеціалізовану службу в мирний час та особливий період;

організація надійного зв'язку центральними та місцевими органами виконавчої влади, органами управління та силами цивільного захисту;

організація та здійснення заходів щодо контролю готовності автоматизованих систем централізованого оповіщення про загрозу або виникнення НС(НП);

у режимі підвищеної готовності:

здійснення заходів щодо контролю підтримання в готовності автоматизованих систем централізованого оповіщення про загрозу або виникнення НС (НП) для забезпечення оповіщення центральних та місцевих органів виконавчої влади, органів управління та сил цивільного захисту, а також координація діяльності із забезпечення інформування населення про загрозу виникнення НС(НП) та дії в умовах такої ситуації; приведення в готовність спеціалізованої служби, залучення в разі потреби додаткових сил і засобів;

організація надійного зв'язку центральними та місцевими органами виконавчої влади, органами управління та силами цивільного захисту;

у режимі НС (НП):

здійснення заходів щодо контролю підтримання в готовності автоматизованих систем централізованого оповіщення про загрозу або виникнення НС (НП) для забезпечення оповіщення центральних та місцевих органів виконавчої влади, органів управління та сил цивільного захисту, а також координація діяльності із забезпечення інформування населення про загрозу виникнення НС (НП) та дії в умовах такої ситуації; приведення в готовність спеціалізованої служби, залучення в разі потреби додаткових сил і засобів;

здійснення заходів з переведення спеціалізованої служби до функціонування в умовах НС (НП);

підготовка пропозицій щодо проведення спеціальних робіт і заходів з цивільного захисту за напрямом галузевого спрямування діяльності спеціалізованої служби та їх забезпечення під час ліквідації наслідків НС (НП) і управління підрозділами спеціалізованої служби, що залучаються до таких робіт та заходів;

організація взаємодії з органами управління та силами цивільного захисту функціональних і територіальних підсистем, їх ланок, які залучаються до ліквідації наслідків НС (НП);

організація надійного зв'язку центральними та місцевими органами виконавчої влади, органами управління та силами цивільного захисту.

#### **4.3 Призначення і завдання телекомунікацій**

Найважливішими завданнями телекомунікацій у ДСНС є:

забезпечення оперативного та якісного прийому і передачі інформації про НС (НП);

забезпечення стійкого і безперервного зв'язку для управління силами та засобами при виконанні завдань за призначенням;

організація взаємодії та передачі інформації з іншими центральними органами виконавчої влади та місцевого самоврядування;

забезпечення передачі інформації як між апаратом ДСНС, його територіальними підрозділами, підприємствами, організаціями та установами сфери управління ДСНС, так і всередині них між окремими структурними підрозділами та їх співробітниками.

#### **4.4 Призначення і завдання інформатизації**

Упровадження інформаційних технологій (ІТ) в діяльність підрозділів ДСНС відбувається шляхом автоматизації процесів управління діяльністю ДСНС, оперативного рішення завдань щодо забезпечення пожежної та техногенної безпеки, адміністративно-господарської діяльності і реалізується через засоби інформатизації, що забезпечує рішення завдань за призначенням.

Основним призначенням упровадження ІТ у ДСНС є автоматизація обробки інформації за напрямками діяльності ДСНС.

Основним завданням ІТ у ДСНС є:

автоматизація системи оперативно-диспетчерського управління;  
впровадження та підтримка функціонування системи електронного документообігу;  
автоматизація основних напрямків адміністративно-управлінської діяльності (матеріально-технічне забезпечення, фінансово-господарська діяльність, і т.д.);  
підтримка функціонування Інтернет-ресурсів ІТС та ТС в ДСНС.

Інформаційні технології повинні забезпечувати:

взаємодію інформаційних потоків усіх рівнів;  
збереження цілісності інформаційних баз даних;  
оперативність та достовірність інформації;  
ефективне й надійне функціонування інформаційних систем та захист від несанкціонованого доступу та кіберзахист.

#### **Технічний захист інформації**

Організаційно-технічні принципи, порядок здійснення заходів із технічного захисту інформації, порядок контролю в цій сфері, характеристики загроз для інформації, норми та вимоги з технічного захисту інформації, порядок атестації та експертизи комплексних систем захисту інформації та комплексів технічного захисту інформації визначаються нормативно-правовими актами, прийнятими в установленому порядку відповідними органами.

До об'єктів ТЗІ належить інформація, вимога щодо захисту якої встановлена законом. До об'єктів захисту в телекомунікаційних системах та інформаційних технологіях відноситься програмне забезпечення, що призначене для обробки цієї інформації. Організаційно-технічні принципи, порядок здійснення заходів щодо ТЗІ, порядок контролю у цій сфері, характеристики загроз для інформації, норми та вимоги з ТЗІ визначаються нормативно-правовими актами з питань ТЗІ.

Дія Положення про технічний захист інформації у Державній службі України з надзвичайних ситуацій не поширюється на системи і засоби, що базуються на криптографічних методах захисту інформації.

Організація заходів протидії технічним розвідкам у ДСНС України регламентується нормативними документами Державної служби спеціального зв'язку та захисту інформації України. Комплекси системи захисту інформації на об'єктах інформаційної діяльності від витоку технічними каналами створюються власними силами та із залученням організацій, що мають відповідні ліцензії (дозволи).

Під час розроблення і впровадження заходів з ТЗІ використовуються засоби, дозволені Державною службою спеціального зв'язку та захисту інформації України для застосування та включені до відповідних переліків.

Організація технічного захисту інформації в органах ДСНС, щодо яких здійснюється ТЗІ, покладається на їх керівників.

Підрозділи ТЗІ органів та підрозділи ДСНС здійснюють організацію, методичне забезпечення та контроль за впровадженням в органах та підрозділах ДСНС заходів ТЗІ.

#### **4.6 Кіберзахист та організація протидії кіберзагрозам**

Комунікаційні системи, які використовуються у ДСНС, відносяться до критичної інформаційної інфраструктури і є об'єктами кіберзахисту.

Об'єктами кібербезпеки є сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; об'єкти критичної інфраструктури.

Об'єктами кіберзахисту є комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси; об'єкти критичної інформаційної інфраструктури; комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Здійснення заходів із забезпечення кібербезпеки покладається на відповідні структурні підрозділи.

Структурні підрозділи, які відповідають у межах своєї компетенції за забезпечення кібербезпеки:

- здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

- здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

- здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

- розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

- забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління;

- здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.

Закон України «Про основні засади забезпечення кібербезпеки України» не поширюється на діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення».

### **ОРГАНІЗАЦІЯ ЗВ'ЯЗКУ В ДСНС УКРАЇНИ**

#### **5.1 Організація каналів і мереж зв'язку ДСНС**

Для забезпечення управління силами цивільного захисту ДСНС телекомунікаційні системи та інформаційні технології ДСНС повинні мати високий рівень готовності, мобільності, доступності, надійності, оперативності, достовірності, необхідної пропускну здатності та скритності передачі інформації.

Центральний та резервний вузли відомчої цифрової телекомунікаційної мережі ДСНС (ВЦТМ) належать до сфери відповідальності ДСНС України. На резервному центральному вузлі ВЦТМ здійснюється резервування сервісів ВЦТМ і створено резервний центр обробки даних.

Територіальні органи, підрозділи центрального підпорядкування, заклади освіти, підприємства, організації та установи сфери управління ДСНС виступають окремими вузлами ВЦТМ 1-го рівня (далі – окремі вузли ВЦТМ) і мають власну IP-адресацію, визначену відповідним наказом ДСНС. Фіксована IP-адресація поширюється на підрозділи ДСНС, розташовані в населених пунктах будь-якого типу та їх районах. Підрозділи ДСНС, які не підпорядковуються безпосередньо апарату ДСНС, виступають окремими вузлами 2-го рівня.

ВЦТМ поєднує як самостійні підмережі територіальних органів, підрозділів центрального підпорядкування, закладів освіти, підприємств, організацій та установ сфери управління ДСНС (далі – окремі вузли ВЦТМ) із центральними вузлами ВЦТМ, так і може надавати можливість здійснювати обмін даними між окремими вузлами ВЦТМ без залучення обладнання центральних вузлів ВЦТМ.

Канали зв'язку між вузлами ВЦТМ будуються на базі:  
каналів зв'язку ДСНС;

каналів зв'язку операторів (провайдерів) телекомунікацій, що надають послуги з доступу до мережі Інтернет та мають чинні атестати відповідності системи захисту, видані Державною службою спеціального зв'язку та захисту інформації України;

державних каналів зв'язку спеціального призначення – національна телекомунікаційна мережа, телекомунікаційна мережа спеціального призначення тощо.

Доступ до ВЦТМ підрозділів, які підпорядковані територіальним органам ДСНС, здійснюється через територіальні органи ДСНС.

Схему організації ВЦТМ наведено у додатку В.

Окремим способом підключення до ВЦТМ виступає під'єднання через відомчий VPN сервер. VPN виступає складовою ВЦТМ.

Правила побудови мережі в окремих вузлах ВЦТМ відзначаються відповідними наказами. Мережа Wi-Fi має бути розгорнута в окремому сегменті.

### **5.1.1 Радіозв'язок**

Радіозв'язок у системі зв'язку ДСНС організовується в КХ та УКХ діапазонах, використовується супутниковий зв'язок та пристрої радіодоступу до телекомунікаційних мереж відповідно до наказів та Інструкцій МВС та ДСНС України.

У ДСНС використовуються цифрові та аналогові системи радіозв'язку. Пріоритет надається розвитку та впровадженню систем цифрового радіозв'язку.

Радіозв'язок є найважливішим засобом, який спроможний забезпечити безперервним управлінням підрозділами ОРС ЦЗ.

Відомчий УКХ радіозв'язок під час ліквідації наслідків НС (НП) є основним видом оперативного зв'язку.

Радіомережі та радіонапрямки КХ діапазону призначені для забезпечення передачі оперативної інформації до головної радіостанції (ДСНС України) щодо ліквідації НС (НП) та отримання команд управління силами та засобами. Радіостанції ДСНС при забезпеченні радіозв'язку в КХ діапазоні застосовують міжнародні (офіційні) позивні.

Основними способами організації радіозв'язку є радіонапрямок та радіомережа.

Системи радіозв'язку використовують основні режими обміну інформацією: симплексний, дуплексний та напівдуплексний.

Радіозв'язок ведеться державною мовою відповідно до правил ведення радіообміну. Типові схеми організації радіозв'язку наведені в додатку В.

При роботі в КХ діапазоні ведеться окремий апаратний журнал (Додаток Г).

Правила ведення радіообміну наведено у додатку Д.

Ведення радіообміну в підрозділах повинні бути записані та архівовані за допомогою програмно-апаратних комплексів.

### **5.1.2 Радіорелейний зв'язок**

Радіорелейний зв'язок організовується для резервування провідних каналів зв'язку від місця ліквідації надзвичайної ситуації до територіальної підсистеми.

Радіорелейні засоби зв'язку в ДСНС можуть застосовуватись як самостійно, так і для створення комбінованих ліній зв'язку спільно з іншими засобами зв'язку для резервування каналів зв'язку. Радіорелейні засоби зв'язку в ОРС ЦЗ організовуються по напрямках.

Під час побудови радіорелейного зв'язку враховується:

можливість перехоплення передач та створення завад;

необхідність старанного вибору місць установки станцій;

залежність стійкості роботи зв'язку від направленості антен кожної станції та від рельєфу місцевості.

### **5.1.3 Супутниковий зв'язок**

Організація супутникового зв'язку в ДСНС здійснюється згідно відповідних наказів та Інструкції МВС та ДСНС України.

Залежно від виду наданих послуг системи супутникового зв'язку діляться на:  
системи пакетної передачі даних (доставка циркулярних повідомлень, автоматизованого збору даних про стан різних об'єктів, у тому числі транспортних засобів, тощо);  
системи радіотелефонного зв'язку;  
системи AVLS для визначення місцезнаходження (координат) абонента.

Дозвіл на використання каналу супутникового зв'язку надає ДСНС України, враховуючи пропозиції начальників (уповноважених фахівців) підрозділів телекомунікацій та інформаційних технологій територіальних органів та підрозділів ДСНС. Начальники підрозділів телекомунікацій та інформаційних технологій територіальних органів та підрозділів ДСНС України забезпечують роботу комплексу супутникового зв'язку.

#### **5.1.4 Проводовий зв'язок**

Проводовий зв'язок у ДСНС забезпечується по кабельних та повітряних лініях загальнодержавної та відомчих мереж зв'язку, а також по польовим кабельним лініям, прокладеним під час проведення аварійно-рятувальних та інших невідкладних робіт в зоні НС(НП).

Для забезпечення роботи каналів проводового зв'язку використовуються:  
лінійні та кабельні споруди;  
ресурси національної телекомунікаційної мережі;  
ресурси телекомунікаційної мережі загального користування;  
мережі некомутованих (виділених) телефонних ліній для зв'язку з службами взаємодії та критично важливими об'єктами інфраструктури;  
ресурси відомчої цифрової телекомунікаційної мережі ДСНС.

#### **5.2 Організація зв'язку у підрозділах ДСНС**

Організація зв'язку визначається схемою та планом, які затверджені керівником територіального підрозділу (Додаток В).

Для забезпечення управління створюється відомча система зв'язку, яка представляє собою сполучення систем зв'язку ДСНС України, органів і підрозділів ОРС ЦЗ, спеціалізованих формувань та аварійно-рятувальних загонів ОРС ЦЗ.

Система зв'язку будується завчасно. У період приведення ОРС ЦЗ в готовність до дій за призначенням вона нарощується за рахунок сил, засобів та додаткових каналів зв'язку органів і підрозділів ОРС ЦЗ та підрозділів провайдерів та операторів телекомунікацій, які забезпечують надання каналів та послуг в сфері телекомунікацій.

#### **5.3 Організація зв'язку при взаємодії з органами управління інших міністерств, відомств і служб**

Взаємодія з органами управління, силами і засобами територіальних органів ДСНС України та іншими спеціалізованими формуваннями Єдиної Державної системи цивільного захисту (далі – ЄДСЦЗ), здійснюється відповідно до інструкцій взаємодії затверджених спільними наказами.

#### **Організація зв'язку при ліквідації наслідків надзвичайних ситуацій**

Основним видом зв'язку при ліквідації наслідків НС (НП) є радіозв'язок. Зв'язок організовується за рішенням керівника органу управління (підрозділу) ОРС ЦЗ відповідно до схеми організації зв'язку.

За рішенням керівника ліквідації наслідків надзвичайних ситуацій залучається спеціалізована служба зв'язку ЄДСЦЗ.

Залежно від рівня НС (НП) визначаються необхідні технічні засоби телекомунікацій, які доповнюють діючі системи зв'язку ДСНС рухомими (мобільними) засобами, що дозволяють забезпечити управління підрозділами на марші та безпосередньо в зоні НС (НП).



Під час визначення масштабів НС (НП), за потреби розгортання ППУ з метою забезпечення ефективного управління силами та засобами, залученими до ліквідації наслідків НС (НП), і своєчасного інформування керівництва, залучаються додаткові технічні засоби зв'язку.

Мережі операторів рухомого (мобільного) зв'язку застосовуються за умови його наявності.

На місці ліквідації НС (НП) організується радіомережа керівника органу управління (підрозділу) ОРС ЦЗ у складі радіостанції керівника органу управління (підрозділу) – головна радіостанція та начальників підпорядкованих, приданих та взаємодіючих підрозділів – кореспонденти радіомережі.

Схеми організація зв'язку при ліквідації наслідків надзвичайних ситуацій наведені в Додатку В.

### **.1 Особливості організації зв'язку при застосуванні морських (річкових) суден та проведенні підводних робіт**

Організація зв'язку й взаємодії по пошуку й порятунку людей, що терплять лихо на морі й водних басейнах України, здійснюється на підставі Плану взаємодії органів управління і сил, які залучаються до реагування на надзвичайні ситуації державного рівня на водних об'єктах, у якому визначається порядок організація управління, зв'язку, оповіщення і взаємодії.

Безпосередньо у проведенні пошуково-рятувальних операцій на морі й водних басейнах беруть участь пошуково-рятувальні підрозділи, спеціалізовані пошуково-рятувальні морські і повітряні судна (пошуково-рятувальні одиниці), виділені учасниками взаємодії, а також інші морські і повітряні судна, що знаходяться в районі або поблизу району лиха, що діють як самостійно, так і спільно один з одним.

Екіпаж пошуково-рятувального повітряного судна по радіо, а за відсутності радіозв'язку – за допомогою встановлених візуальних сигналів здійснює спрямування кораблів та малих (маломірних) суден у зону НС (НП).

Зв'язок при проведенні підводних робіт організується підрозділами водолазно-рятувальних робіт, що виконують аварійно-рятувальні підводні роботи. Для зв'язку керівника робіт із ліквідації наслідків НС (НП) з рятувальниками, що працюють під водою, використовуються засоби телефонного й гідроакустичного зв'язку.

### **.2 Особливості організації зв'язку під час проведення рятувальних робіт з ліквідації надзвичайних ситуацій в гірських районах**

Основою організації зв'язку в гірських районах становить радіозв'язок.

Виходячи з умов обстановки, засоби радіозв'язку доцільно встановлювати на вершинах пагорбів і схилів, використовувати ретранслятори радіозв'язку, розміщені так само на вершинах. При виборі місця розгортання радіо- й радіорелейних станцій враховувати можливість обвалів, утвору лавин, селєвих потоків та ін. Розміщення засобів радіозв'язку в районах, які можуть бути затоплені при розливі рік, і в місцях гірських водойм, що висохли, не допускається.

### **.3 Організація зв'язку при застосуванні авіації**

Управління повітряними суднами, що здійснюють ліквідацію наслідків НС (НП), здійснюється керівником з ліквідації наслідків НС (НП) через координатора дій авіації з використанням УКХ радіостанції авіаційного діапазону.

### **.4 Організація зв'язку в метрополітенах і підземних об'єктах**

Для забезпечення зв'язку в підземних спорудах, в умовах не проходження радіохвиль, використовується телефонна мережа зв'язку об'єкта, УКХ радіозв'язок з використанням ретрансляторів зв'язку, гучномовний зв'язок, й гірничорятувальне обладнання зв'язку.

Підрозділ ОРС ЦЗ ДСНС в зоні НС(НП) організує прямий проводований зв'язок між штабом з ліквідації наслідків НС(НП) і місцем проведення аварійно-рятувальних робіт, радіозв'язок з використанням ретрансляторів. За необхідністю зв'язок з місцем НС (НП) може

забезпечуватися з використанням засобів мобільного зв'язку. Для організації взаємодії між пожежними-рятувальниками та рятувальниками в зоні НС (НП) використовуються індивідуальні засоби радіозв'язку в комплексі із портативними ретрансляторами.

#### **Відновлення зв'язку і готовності підрозділів зв'язку**

Начальник служби зв'язку залучає всі необхідні сили та засоби на відновлення зв'язку, а також звертається до центру управління телекомунікаційними мережами.

## **6. ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ В ДСНС УКРАЇНИ**

### **6.1. Організація телефонного зв'язку**

Телефонний зв'язок розподіляється на стаціонарний, мобільний, супутниковий та IP-телефонію.

Телефонний зв'язок використовується для забезпечення оперативного та адміністративно-господарського управління.

Стаціонарний телефонний зв'язок організовується шляхом надання телекомунікаційних послуг операторами телекомунікацій та доступу до мережі телефонного зв'язку загального користування.

Корпоративна система мобільного зв'язку організовується шляхом надання телекомунікаційних послуг операторами мобільного зв'язку. При наявності покриття місцевості операторами мобільного зв'язку, де відбувається ліквідація наслідків НС (НП), мобільний зв'язок є одним із видів прийому та передачі інформації.

Система IP-телефонії функціонує на базі телекомунікаційних систем.

Розмови та переговори по телефонних лініях екстрених викликів повинні бути записані та архівовані за допомогою програмно-апаратних комплексів.

Перелік телефонних номерів, порядок запису, зберігання та видачі інформації затверджується відповідними наказами керівників підрозділів.

### **6.2. Організація роботи телекомунікаційної мережі**

Для забезпечення управління створюється відомча ІТС ДСНС, яка представляє собою сполучення ІТС ДСНС України, органів і підрозділів ЦЗ, спеціалізованих формувань та аварійно-рятувальних загонів ОРС ЦЗ.

Телекомунікаційна мережа територіального (структурного) підрозділу складається із:  
лінійних та кабельних споруд;

телекомунікаційної мережі загального користування;

мереж операторів телекомунікацій для обслуговування абонентів особливо важливих об'єктів, систем централізованого нагляду і абонентів відомчих автоматичних телефонних станцій;

каналів телефонного зв'язку номерів екстрених викликів;

каналівнекомутованих (прямих) телефонних ліній, призначених для зв'язку чергової частини з пунктами зв'язку частин;

мереж операторів телекомунікацій мобільного зв'язку;

Типові схеми організації телекомунікаційної мережі наведені в додатку В.

### **6.3 Організація відеоконференцзв'язку**

Одним з видів обміну та доведення інформації в підрозділах ДСНС є відеоконференцзв'язок. Організація відеоконференцзв'язку здійснюється за рішенням керівництва ДСНС, а для територіального підрозділу (органу) за рішенням керівника цього підрозділу.

Технічний супровід відеоконференцзв'язку здійснюється відповідними фахівцями.

### **6.4 Система оповіщення особового складу**

Для оповіщення особового складу в підрозділах застосовуються автоматизовані системи оповіщення.

Для забезпечення оповіщення підрозділів та особового складу розробляються та відпрацьовуються відповідні схеми оповіщення.

Телекомунікаційні системи оповіщення особового складу поділяються на:

гучномовні телекомунікаційні системи оповіщення особового складу для безпосереднього оповіщення особового складу в адмінбудівлях, будівлях та прилеглий території підрозділу;

автоматизовані телекомунікаційні системи оповіщення особового складу на

телефоніфікованого зв'язку та мобільні телефони.

Оповіщення здійснюється за рішенням керівника підрозділу.

## **6.5 Система контролю управління доступом**

СКУД повинна забезпечувати управління доступом на задану територію (кого, в який час і на яку територію пропускати), ідентифікацію особи (транспортного засобу), яка (який) має доступ на задану територію.

За технічної можливості СКУД може вести базу даних особового складу (працівників)/відвідувачів, облік робочого часу, інтеграцію з системою безпеки, наприклад:

з системою відеоспостереження для суміщення архівів подій систем, передачі системі відеоспостереження повідомлень про необхідність стартувати запис тощо;

з системою охоронної сигналізації, для обмеження доступу в приміщення, які стоять на охороні, або для автоматичного зняття і постановки приміщень на охорону.

Ідентифікатор є базовим елементом системи контролю доступом, що зберігає код, який служить для визначення прав («ідентифікації») власника (Touchmemory, безконтактна картка, RFID-мітка, біометричні ознаки людини (відбиток пальця, малюнок сітківки або райдужної оболонки ока, тривимірне зображення обличчя).

Мережевий контролер СКУД повинен об'єднуватись в єдину систему з іншими контролерами або комп'ютером для можливості централізованого контролю і управління.

Рішення про надання доступу може прийматися як контролером, так і програмним забезпеченням головного комп'ютера. Об'єднання контролерів в мережу здійснюється за допомогою промислового інтерфейсу RS-485 або локальної мережі Ethernet.

Програмне забезпечення СКУД не є обов'язковим елементом системи контролю доступу і використовується в разі, коли потрібна обробка інформації о проходах, побудова звітів, управління та збору інформації в процесі роботи системи. Пріоритетом використання програмного забезпечення СКУД є WEB-орієнтоване програмне забезпечення.

## ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДСНС УКРАЇНИ

### 7.1 Організаційні заходи стосовно впровадження програмного забезпечення та його облік

У системі ДСНС структурні підрозділи (або визначені посадові особи) за напрямом телекомунікаційних систем та інформаційних технологій відповідають за дотримання вимог законодавства з питань правової охорони комп'ютерних програм під час їх придбання, встановлення, використання, обліку та інвентаризації.

У системі ДСНС використання не ліцензійного програмного забезпечення заборонено. У системі ДСНС пріоритетним є використання комп'ютерних програм вільного використання.

Користувач отримує доступ до тих видів інформаційних ресурсів, використання яких в повній мірі забезпечує виконання ним своїх службових обов'язків через комп'ютер, котрий має унікальне ім'я в локальній мережі.

Перелік комп'ютерних програм, які дозволені для встановлення на серверах та комп'ютерах користувачів системи ДСНС, зокрема, що знаходиться на позабалансовому обліку затверджується відповідними наказами ДСНС. Використання інших комп'ютерних програм має відбуватися за погодженням із підрозділом, що відповідає за напрямом інформаційних і телекомунікаційних технологій апарату ДСНС.

Обробка та зберігання особистої інформації на службових засобах обчислювальної техніки заборонено.

Облік програмного забезпечення здійснюється відповідно до вимог нормативних документів в електронному вигляді.

### 7.2 Організація роботи електронної поштової системи

Відомча електронна поштова система ДСНС застосовується для обміну службовими документами каналами телекомунікаційних мереж ДСНС, а також мережею Інтернет.

До складу Відомчої електронної поштової системи входить центральний поштовий сервер апарату ДСНС та власні поштові сервери головних управлінь (управлінь) ДСНС України в областях та м. Києві, які побудовано на базі серверного програмного забезпечення, рекомендованого для використання апаратом ДСНС, та функціонують на під доменах dsns.gov.ua.

Відповідальні за адміністрування серверів, що входять до складу Відомчої поштової системи, визначаються внутрішніми наказами відповідних підрозділів ДСНС.

Відомча поштова система використовується в інформаційних цілях, у тому числі з метою інформування, організації роботи, забезпечення внутрішніх та зовнішніх комунікацій.

Обмін електронними повідомленнями в ДСНС та з зовнішніми адресатами здійснюється лише з використанням електронних поштових скриньок в домені dsns.gov.ua.

Закладам освіти, Державному центру сертифікації ДСНС України та Українському гідрометеорологічному центру дозволяється здійснювати обмін електронними повідомленнями в ДСНС та з зовнішніми адресатами з поштових скриньок у під доменах edu.uata доменах dcs.gov.ua, meteo.gov.ua відповідно.

### 7.3. Система оперативно-диспетчерського управління

СОДУ призначена для максимальної автоматизації основних функцій оперативно-диспетчерського управління та є інтегруючим інформаційним програмно-технічним комплексом для створення єдиної геоінформаційної системи (далі – ГІС) управління та моніторингу з можливістю передачі інформації в реальному часі від чергових підрозділів до СІЗ;

СОДУ повинна забезпечувати:

надійний прийом, передачу, реєстрацію, обробку і аналіз всієї інформації, яка відноситься до службово-оперативної діяльності, управління підпорядкованими силами постійної готовності та взаємодію з іншими диспетчерськими службами екстреного виклику;

ведення інформаційних баз даних і формування інформаційних та статистичних звітів.

Задачі управління силами та засобами повинні вирішуватися на основі оперативної взаємодії диспетчерів СОДУ. Функції підсистеми і відповідні програмні комплекси повинні бути розподілені між сервером СОДУ, автоматизованими робочими місцями диспетчерів оперативно-диспетчерської служби та автоматизованими робочими місцями диспетчерів ПЗЧ.

#### **7.4 Організація адміністрування систем телекомунікацій та інформатизації**

Завдання організації адміністрування систем телекомунікацій та інформатизації призначені для виконання таких функцій:

- підтримка функціонування програмного забезпечення та телекомунікаційного обладнання системи;

- інформаційної безпеки та цілісності даних;

- кібербезпеки;

- організації та підтримки інформаційної взаємодії;

- надання допомоги користувачам системи.

Основними елементами адміністрування є сервер, телекомунікаційна мережа та комп'ютери користувачів. Для виконання робіт з адміністрування ІТС наказом керівника підрозділу визначається структурний підрозділ (фахівець), який виконує функції адміністратора. До його обов'язків входить технічна підтримка функціонування ІТС згідно регламенту, проведення профілактичних заходів, організація резервування ІТС та періодичне формування резервних копій даних, проведення заходів із кіберзахисту ІТС, забезпечення функціонування засобів телекомунікації.

Рекомендовано виконати розмежування рівнів доступу адміністраторів мережевого обладнання таким чином:

- надання адміністраторам центрального вузла ДСНС повного доступу до мережевого обладнання у центральному вузлі ДСНС та в регіональних підрозділах для можливості моніторингу мережі та своєчасного виявлення ризиків;

- надання адміністраторам регіональних підрозділів ДСНС обмеженого рівня доступу до мережевого обладнання, еквівалентного рівню базової конфігурації обладнання;

Рекомендовано здійснювати безпосереднє підключення до необхідних пристроїв лише за допомогою захищених протоколів.

## **8.СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ**

Напрямки захисту інформації формуються виходячи із конкретних особливостей інформаційної системи як об'єкту захисту. Виходячи з типової структури ІС і історично складених висновків робіт по захисту інформацією, можна виділити наступні напрямки:

- захист об'єктів інформаційних систем;
- захист процесів, процедур і програм обробки інформації;
- захист каналів зв'язку;
- пригнічення побічних електромагнітних наведень;
- управління системою захисту.

Забезпечення діяльності щодо заходів технічного захисту інформації досягається:

створенням комплексних систем захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах ДСНС на об'єктах інформаційної діяльності ДСНС;

забезпечення сталого функціонування впроваджених в експлуатацію комплексних систем захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах ДСНС на об'єктах інформаційної діяльності ДСНС.

### **8.1 Види робіт з ТЗІ, які можуть виконуватися підрозділами ТЗІ**

Розроблення, впровадження, випробування, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є акустичні поля.

Розроблення, впровадження, випробування, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є електромагнітні поля та електричні сигнали.

Розроблення, впровадження, випробування, супроводження комплексів технічного захисту інформації в інформаційних системах, інформаційних технологій із захистом інформації від несанкціонованого доступу.

Виявлення та блокування витоку мовної та видової інформації через закладні пристрої на об'єктах інформаційної діяльності.

#### **8.1.1 Організація діяльності підрозділів ТЗІ**

У системі ДСНС роботи з технічного захисту інформації проводяться підрозділами ТЗІ відповідно до Дозволу на проведення робіт з технічного захисту інформації для власних потреб, наданого ДСНС у встановленому порядку, та повноважень на проведення відповідних видів робіт відповідно до наказу ДСНС. Роботи з технічного захисту інформації у системі ДСНС також можуть проводити організації, які мають ліцензію на проведення відповідних видів робіт з технічного захисту інформації та спеціальний дозвіл на

проведення діяльності, пов'язаної з державною таємницею.

Повноваження підрозділу ТЗІ на проведення відповідних видів робіт з ТЗІ надаються наказом ДСНС.

Координацію, облік проведених робіт та контроль за діяльністю підрозділів ТЗІ підрозділів здійснює Управління зв'язку та оповіщення ДСНС .

Основні завдання, функції, обов'язки та відповідальність підрозділу ТЗІ визначаються Положенням про підрозділ ТЗІ, яке затверджується керівником підрозділу.

Впровадження заходів ТЗІ в підрозділі, до складу якої входить Підрозділ ТЗІ, організовується керівником підрозділу.

Безпосередній контроль за виконанням завдань підрозділом ТЗІ покладається на керівника підрозділу зв'язку та інформатизації підрозділу.

Організація заходів ТЗІ у центральному апараті ДСНС здійснюється Управлінням.

Інструментальний контроль виконання вимог та норм технічного захисту інформації на об'єкті інформаційної діяльності (далі – ОІД), де розроблено та впроваджено підрозділом ТЗІ комплекс технічного захисту інформації, може здійснюватися Центром ТЗІ Вузла зв'язку та

автоматизації ДСНС.

### **8.1.2 Умови та порядок надання повноважень на проведення робіт з технічного захисту інформації**

Для одержання повноважень підрозділу ТЗІ на проведення окремих видів робіт або усього зазначеного переліку необхідно мати:

Призначених наказом керівника підрозділу спеціалістів для проведення обраних видів робіт, які мають повну чи базову вищу освіту за напрямом підготовки «Інформаційна безпека» або інженерно-технічну освіту фахового спрямування, відповідного обраному виду роботи, з додатковою підготовкою на курсах перепідготовки та підвищення кваліфікації фахівців з питань ТЗІ чи стажем роботи у галузі ТЗІ за обраним видом роботи не менше 3 років, а також мають оформлені у встановленому порядку допуски до державної таємниці.

Нормативно-правові акти та нормативні документи з технічного захисту інформації, необхідні для проведення обраних видів робіт.

Повірені в установленому порядку засоби вимірювань і контролю (як власні, так і залучені на договірних засадах), а також засоби ЕОТ в обсязі, що забезпечує проведення обраних видів робіт.

Приміщення, у яких впроваджено і атестовано комплекси ТЗІ та інформаційні системи з впровадженою КСЗІ з підтвердженою відповідністю.

Спеціальний дозвіл на провадження діяльності, пов'язаної з державною таємницею.

Окреме приміщення, в якому розміщується начальницький склад та працівники, а також апаратура підрозділу ТЗІ і забезпечується обмежений доступ сторонніх осіб.

Начальницький склад та працівники підрозділу ТЗІ повинні знати методики та порядок виконання робіт з ТЗІ відповідно до вимог нормативних документів та уміти застосовувати наявну апаратуру і обладнання. Методичний супровід підвищення кваліфікації начальницького складу та працівників підрозділу ТЗІ забезпечується Управлінням.

За умов виконання зазначених вимог підрозділ ТЗІ, подає до ДСНС заяву про надання повноважень на проведення робіт з ТЗІ.

Після отримання заяви ДСНС перевіряє відомості, що містяться у поданих матеріалах, створені умови для проведення заявлених видів робіт, підготовленість начальницького складу і працівників підрозділу ТЗІ та приймає рішення про надання повноважень на виконання заявлених видів робіт або надає рекомендації щодо усунення виявлених недоліків і термін наступної перевірки.

### **8.2 Створення та впровадження комплексних систем захисту інформації**

Етапи побудови КСЗІ необхідно пройти в рівній кількості для всіх і кожного окремо напрямків (з врахуванням всіх основ). Виділяють наступні етапи побудови КСЗІ:

визначення інформаційних ресурсів (ІР), які підлягають захисту;

виявлення всієї можливої кількості загроз безпеки ІР, які підлягають захисту;

проведення оцінки чутливості і ризиків для ІР, які підлягають захисту, при виявленні великої кількості загроз;

розробка проекту (плану) системи захисту інформації, знижуючого за вибраним критерієм ризику для ІР, які підлягають захисту, при виявленні великої кількості загроз.

реалізація проекту (плану) захисту інформації;

визначення якості реалізації системи захисту;

здійснення контролю функціонування і управління системою захисту.

Аналіз стану і уточнення вимог до СЗІ об'єднує складові блоків основи, напрямки, етапи за принципом один з одним.

### **8.3 Створення та впровадження комплексів технічного захисту інформації**

Захист інформації з обмеженим доступом при автономному використанні на ОІД пристроїв обробки інформації здійснюється шляхом створення комплексу ТЗІ, який складається



із сукупності:

організаційних заходів захисту від несанкціонованих дій з інформацією (для захисту конфіденційної інформації, що є власністю держави або вимога щодо захисту якої встановлена законом);

організаційних заходів захисту від несанкціонованих дій з інформацією та технічних засобів захисту інформації від витоку технічними каналами за наявності можливості створення таких каналів (для захисту інформації, що становить державну таємницю).

За результатами спеціального дослідження приймається рішення про необхідність встановлення активних та/або пасивних засобів захисту. Після цього проводиться оцінка захищеності ІЗОД від витоку технічними каналами на об'єкті ЕОТ (атестація комплексу ТЗІ).

Організаційні заходи захисту від несанкціонованих дій з інформацією при автономному використанні пристроїв обробки інформації:

встановлення порядку користування ПАВ;

встановлення порядку використання зовнішніх пристроїв пам'яті в ПАВ;

визначення та встановлення обов'язків осіб, що користуються ПАВ та здійснюють контроль за користуванням ПАВ;

встановлення порядку фізичного захисту ОІД, де функціонує ПАВ;

визначення та встановлення змісту і порядку контролю за користуванням ПАВ.

#### **8.4 Організація заходів протидії кіберзагрозам**

За рекомендаціями Державної служби спеціального зв'язку та захисту інформації України з метою запобігання кіберінцидентам і сприяння підвищенню рівня кіберзахисту електронних ресурсів та систем необхідно:

Провести аудит запроваджених заходів захисту та рівня інформаційної безпеки систем у цілому.

Провести роз'яснювальну роботу з працівниками, які користуються службовою електронною поштою, щодо правил та вимог безпеки, особливо в частині, що стосується вхідних листів (повідомлень).

Заборонити відкриття вкладень у підозрілих повідомленнях (листах від адресатів, щодо авторства яких виникають сумніви та зобов'язати користувачів службової електронної пошти негайно повідомляти про такі листи адміністратора безпеки.

Зобов'язати користувачів службової електронної пошти провести її ревізію на предмет виявлення листів, що мають вкладення «MoF critical IT needs\_eng.xls», «Додаток №2.xls», заборонивши їх відкриття, та невідкладно повідомляти про наявність таких листів адміністратора безпеки.

Заборонити використання приватної електронної пошти для цілей службової діяльності.

Заборонити використання точок публічного доступу до Інтернет для входу до службової електронної пошти.

Адміністраторам безпеки рекомендовано звести до мінімуму мережеву активність усіх пристроїв систем управління з Інтернет, ужити заходів до дотримання вимог із сегментування, не допускати циркуляції технологічної інформації поза межами адміністративного сегмента мережі.

Для організації віддаленого доступу використовувати лише безпечні методи (наприклад, такі технологічні рішення, як VPN).

Для унеможливлення проведення атак типу Man-in-the-Middle з використанням техніки обладнання. Для цього здійснити прив'язку MAC-адрес АРМ до конкретного інтерфейсу комутатора, цим самим заборонивши підключення сторонніх пристроїв.

Передбачити моніторинг та фіксацію (журналювання) подій, які мають відношення до інформаційної безпеки (доступ до баз даних, адміністративний доступ до обладнання тощо).

Запровадити політику, що потребує використання лише надійних паролів.

Провести рекомендоване виробником оновлення програмного забезпечення, щоб запобігти вже виявленим уразливостям.

Контролювати створення аккаунтів на рівні адміністраторів системи.

Здійснити зміну авторизаційних даних до критично важливих вузлів системи, попередньо перевіряючи їх на наявність процесів, які можуть скомпрометувати дані.

Проводити постійний аналіз вхідного/вихідного Інтернет-трафіку.

Проводити аналіз лог-файлів мережевого та серверного обладнання на наявність у них відомостей про аномальну активність (доступ до системи із систем, які перебувають поза адміністративним сегментом мережі; наявність нелегітимних авторизаційних даних).

Здійснювати перевірку ПЕОМ адміністраторів мережі та критично важливих вузлів системи на наявність підозрілих процесів і програм (наприклад: системних служб, що запускаються не зі стандартного розташування; програм, що не мають цифрового підпису виробника, тощо).

Дотримуватися організації заходів протидії кіберзагрозам у відповідності до рекомендацій Національного стандарту України ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки.

# СЛУЖБА ЗВ'ЯЗКУ ГАРНІЗОНУ

## 9.1 Загальні положення

Відповідальним за зв'язок є начальник управління територіального органу ДСНС, а безпосередня організація та забезпечення зв'язку покладається на начальника служби зв'язку гарнізону.

Начальник служби зв'язку гарнізону ОРС ЦЗ призначається наказом начальника гарнізону ОРС ЦЗ із осіб начальницького складу, які мають спеціальну підготовку за фахом, є посадовою особою гарнізону, підпорядковується начальнику (заступнику начальника) гарнізону ОРС ЦЗ, а під час виконання оперативних дій – керівнику ліквідації наслідків надзвичайної ситуації, керівнику гасіння пожежі і несе відповідальність за організацію зв'язку, постійну готовність до використання технічних засобів.

## 9.2 Структура служби зв'язку гарнізону

Головною організуючою і керівною ланкою в організації телекомунікаційних систем та інформаційних технологій в гарнізонах ДСНС України (ГУ(У) ДСНС в областях) є відділ(сектор) телекомунікацій, інформаційних технологій та Системи 112 (відділ, сектор), що організовує всі основні види зв'язку. Відділ (сектор) створюється в усіх ГУ(У) ДСНС і є самостійним структурним підрозділом в складі ГУ(У) ДСНС.

Основним підрозділом, який відповідає за технічну експлуатацію телекомунікаційних систем та інформаційних технологій в гарнізонах ДСНС України (ГУ(У) ДСНС в областях), є Центр оперативного зв'язку телекомунікаційних систем та інформаційних ресурсів (ЦОЗ).

Центр створюється в усіх ГУ(У) ДСНС області і функціонально підпорядковується начальнику відділу (сектору) телекомунікацій, інформаційних технологій та Системи 112 ГУ(У) ДСНС області.

До складу Центру входять підрозділи телекомунікацій, інформаційних технологій, підрозділ захисту інформації, радіотехнічного контролю та кіберзахисту, підрозділ технічного забезпечення.

## 9.3 Структурні підрозділи зв'язку гарнізону

В апаратах ГУ(У) ДСНС в областях та місті Києві створюються посади начальників відділів (секторів), або помічників начальників Управлінь з питань телекомунікаційних систем та інформаційних технологій (в залежності від штатної чисельності територіальних органів). Штатна чисельність секторів становить не менше двох посад.

Для виконання завдань щодо забезпечення діяльності ГУ(У) та його підпорядкованих підрозділів за напрямками оперативного зв'язку, телекомунікаційних систем, інформаційних технологій, технічного захисту інформації, технічного забезпечення та обслуговування засобів телекомунікацій і обчислювальної техніки в територіальних органах ДСНС України створюються центри оперативного зв'язку, телекомунікаційних систем та інформаційних технологій (ЦОЗ, ТС та ІТ), а також відділення зв'язку (ВЗ АРЗ СП) та майстерні по ремонту засобів зв'язку аварійно-рятувальних загонів спеціального призначення.

До складу ЦОЗ, ТС та ІТ входить не менше двох відділів чисельністю не менше 5 посад, а також відділення чисельністю не менше 3 посад та сектори чисельністю не менше 2 посад.

Посада заступника начальника ЦОЗ поєднується з посадою начальника відділу інформаційних технологій, а при чисельності ЦОЗ, ТС та ІТ 17 посад і більше вводиться додаткова п

о Виконання обов'язків начальника польового вузла зв'язку покладається на начальника відділу телекомунікаційних систем ЦОЗ, ТС та ІТ або на заступника начальника ЦОЗ, ТС та ІТ, при його наявності.

д

а

з

а

с

т

у

## **10.ОРГАНІЗАЦІЯ ЕКСПЛУАТАЦІЇ ЗАСОБІВ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

Організація та контроль технічної експлуатації телекомунікаційного обладнання та засобів інформатизації в територіальних органах ДСНС покладається на підрозділи зв'язку та телекомунікації (підрозділів, відповідальних за організацію зв'язку і технічну експлуатацію телекомунікаційних систем) ДСНС, посадових осіб, відповідальних за організацію зв'язку і технічну експлуатацію телекомунікаційних систем в ДСНС.Персональну відповідальність за експлуатацію телекомунікаційного обладнання та засобів інформатизації несе безпосередньо користувач.

### **10.1 Введення в експлуатацію телекомунікаційних систем та інформаційних технологій**

Стадія введення в дію телекомунікаційних систем та інформаційних технологій включає: підготовчі роботи до введення телекомунікаційних систем та інформаційних технологій в дію (реалізація проектних рішень щодо організаційної структури системи, інсталяція програмних засобів, монтаж технічних засобів і ліній зв'язку, пусконаладжувальні роботи та автономна перевірка технічних і програмних засобів, комплексна перевірка працездатності телекомунікаційних систем та інформаційних технологій), що здійснює виконавець (постачальник);

комплектацію системи відповідно до проектної документації (придбання та постачання необхідних для реалізації проектних рішень технічних і програмних засобів тощо);

підготовку персоналу (навчання персоналу і перевірку його здатності забезпечити функціонування системи згідно з програмою підготовки персоналу), яку здійснює виконавець (постачальник);

проведення попередніх випробувань (виконавцем проекту згідно з програмою і методикою випробувань з наданням результатів випробувань замовнику під час передачі проекту);

проведення дослідної експлуатації згідно з розпорядчим документом у визначені терміни, за підсумками якої складається акт, що затверджується керівником підрозділу;

проведення приймальних випробувань відповідною комісією (випробування на відповідність проектних рішень технічному завданню згідно з програмою та методикою приймальних випробувань) з оформленням акта, в якому зазначаються підрозділи, які використовують телекомунікаційні системи та інформаційні технології, та визначаються відповідальні за її технічний супровід, а також затверджується відповідна нормативна документація за напрямом телекомунікаційних систем та інформаційних технологій.

### **10.2 Введення в експлуатацію технічних засобів**

Введення телекомунікаційного обладнання в експлуатацію здійснюється комісією, яка створюється в підрозділах ДСНС. При введенні в експлуатацію стаціонарних телекомунікаційних об'єктів або споруд (в тому числі реконструйованих) до складу комісії включаються представники підрядних проектних, будівельних і монтажних організацій. Участь співробітників підрозділу зв'язку та телекомунікацій ДСНС у роботі комісії є обов'язковою. Комісія складає відповідні документи (формуляр) із зазначенням заводських номерів, року випуску і місця установки на введення в експлуатацію.

Час введення в експлуатацію телекомунікаційного обладнання не повинно перевищувати тридцяти днів з моменту їх надходження в підрозділ ДСНС, за винятком коли потрібне проведення комплексу будівельно-монтажних і пусконаладжувальних робіт.

Інформацію про введення в експлуатацію, зміні категорії, модернізації або списання телекомунікаційного обладнання записуються в формулярі із зазначенням документа та дати. Записи завіряються підписом матеріально відповідальної особи працівника зв'язку та телекомунікації, або майстерні.

Контроль за правильність ведення формулярів, та їх зберігання покладається на підрозділи за напрямом телекомунікаційних систем та інформаційних технологій, які відповідають за телекомунікаційне обладнання, а при їх відсутності – на посадових осіб, відповідальних за організацію зв'язку і технічну експлуатацію телекомунікаційного обладнання ДСНС.

У разі втрати формуляра його дублікат відновлюється на підставі рішення начальника служби зв'язку, після проведення службової перевірки за фактом його втрати.

Монтаж телекомунікаційного обладнання проводиться силами співробітників підрозділів зв'язку та телекомунікації, або підрядних організацій відповідно до експлуатаційно-технічної документації.

Облік телекомунікаційного обладнання здійснюється співробітниками підрозділів зв'язку, та телекомунікації або посадовими особами, відповідальними за організацію зв'язку і технічну експлуатацію телекомунікаційного обладнання ДСНС. Дозволяється вести облік в електронному вигляді.

Розподіл телекомунікаційного обладнання між підрозділами ДСНС проводиться на підставі наказів ДСНС. Закріплення обладнання за співробітниками підрозділів, проводиться безпосередньо в підрозділі отримувача майна, згідно внутрішніх розпорядчих документів. Дані про закріплення телекомунікаційного обладнання заносяться в формуляр обладнання.

Порядок видачі телекомунікаційного обладнання, що знаходиться на зберіганні, визначається нормативно-правовими актами ДСНС, що регламентують організацію їх роботи.

### **10.3 Введення в експлуатацію програмних засобів**

Придбання комп'ютерних програм здійснюється лише в разі відсутності аналогів комп'ютерних програм вільного користування та за погодженням із підрозділом, що відповідає за напрям інформаційних і телекомунікаційних технологій апарату ДСНС.

Прикладне програмне забезпечення має бути ліцензійним, по можливості з розширеною підтримкою та обслуговуванням. У разі використання вільного прикладного програмного забезпечення джерелом для його завантаження має виступати офіційний сайт розробника з установленим та дійсним на момент завантаження SSL-сертифікатом.

Не допускається використання програмного забезпечення, якщо розробник знаходиться у переліку фізичних чи юридичних осіб, до яких державою Україна вжито обмежувальних заходів (санкцій).

Установлення програмного забезпечення на комп'ютерах користувачів у системі ДСНС виконують виключно фахівці підрозділів за напрямом телекомунікаційних систем та інформаційних технологій.

Підрозділи ДСНС повинні передбачати заходи з виводу з експлуатації програмного забезпечення, яке вже не підтримується з боку розробника.

Для здійснення внутрішнього електронного документообігу в ДСНС має використовуватися відкритий формат документів (ODF – OpenDocumentFormat).

У разі відправлення документів за межі ДСНС за необхідності вони можуть бути конвертовані (якщо є змога) у формат, який потрібен отримувачу.

Облік програмного забезпечення здійснюють підрозділів за напрямом телекомунікаційних систем та інформаційних технологій.

### **10.4 Технічне обслуговування (супровід) та регламентні роботи телекомунікаційних систем та інформаційних технологій**

Технічне обслуговування та проведення регламентних робіт телекомунікаційних систем та інформаційних технологій виконується згідно річного план-графіку який розробляється посадовою особою відповідальною за напрям телекомунікацій та інформатизації та затверджується начальником служби зв'язку.

Стадія технічного обслуговування та супроводу телекомунікаційних систем та інформаційних технологій включає:

гарантійне технічне обслуговування (здійснення робіт з усунення на безоплатній основі виконавцем проектних робіт недоліків, виявлених під час експлуатації телекомунікаційних систем та інформаційних технологій протягом установлених гарантійних термінів і внесення необхідних змін до технічної документації);

післягарантійне технічне обслуговування (комплекс робіт з підтримки цілодобового справного функціонування телекомунікаційних систем та інформаційних технологій протягом усього строку експлуатації);

супровід телекомунікаційних систем та інформаційних технологій (модифікація програмних та/або програмно-технічних засобів телекомунікаційних систем та інформаційних технологій після передачі замовнику виконавцем (постачальником) робіт для коригування виявлених проблем, виявлення та коригування наявних прихованих помилок для запобігання прояву цих помилок під час експлуатації або забезпечення продовження використання телекомунікаційних систем та інформаційних технологій із заданою ефективністю).

За необхідністю для супроводу та післягарантійного технічного обслуговування телекомунікаційних систем та інформаційних технологій на договірній основі можуть залучатися сторонні організації.

### **Зберігання телекомунікаційного обладнання та засобів інформатизації**

Облік, зберігання, порядок перевірки, введення в експлуатацію, технічне обслуговування телекомунікаційного обладнання та засобів інформатизації, що знаходяться на довготривалому зберіганні визначається окремими розпорядчими документами.

На всі інформаційні ресурси в підрозділі має вестись інформаційна картка за формою. За щорічне оновлення і зберігання інформаційних карток на телекомунікаційні системи та інформаційні технології відповідає підрозділ з напрямку телекомунікацій та інформатизації. Інформаційні картки мають бути в актуальному стані і зберігатися в електронній формі.

При зберіганні телекомунікаційного обладнання та засобів інформатизації повинні виконуватися наступні заходи:

- правильне утримання і використання приміщень складів;
- ретельний і кількісний прийом обладнання, яке поступило на зберігання, їх матеріальний облік з повнотою запису всіх даних про обладнання;
- створення умов, що забезпечують якісне зберігання для кожного виду техніки відповідно до технічних вимог;
- своєчасне проведення технічного обслуговування;

Телекомунікаційне обладнання та засоби інформатизації зберігаються в комплекті поставки. Розукомплектування і роздільне зберігання обладнання допускаються лише за клопотанням начальника служби зв'язку та дозволом начальника територіального підрозділу.

### **Контроль за станом систем, технічних і програмних засобів**

Контроль за станом систем, технічних і програмних засобів покладається на структурний підрозділ, що відповідає за напрям інформаційних і телекомунікаційних технологій, або на визначених керівником посадових осіб, які користуються у своїй діяльності телекомунікаційні системи та інформаційні технології.

**Умовні позначення та скорочення**

- АРЗ СП – аварійно-рятувальний загін спеціального призначення  
АРІНР – аварійно-рятувальні та інші невідкладні роботи  
ВЦТМ – відомча цифрова телекомунікаційна мережа ДСНС  
ЕОТ – електронно-обчислювальна техніка  
ЗТІ – засоби телекомунікацій та інформатизації  
ІзОД – інформація з обмеженим доступом  
ІР - інформаційні ресурси  
ІТ – інформаційні технології  
ІТС – інформаційно-телекомунікаційна система  
КХ - короткохвильовий зв'язок  
Національний центр – Національний центр оперативно-технічного управління телекомунікаційними мережами  
НП - небезпечна подія  
НС - надзвичайна ситуація  
ОІД – об'єкт інформаційної діяльності  
ОЧС – оперативно-чергові служби апарату ДСНС, її органи та підрозділи  
ПАВ – пристрій обробки інформації, що використовується автономно (пристрій автономного використання)  
ПАК - програмно-апаратний комплекс  
ПЕОМ – персональна електронно-обчислювальна машина  
ППУ – пересувний пункт управління  
СЗІ - система захисту інформації  
СОТУТМ – Система оперативно-технічного управління телекомунікаційними мережами  
ТЗІ – технічний захист інформації  
ТС – телекомунікаційні системи  
УКХ – ультракороткохвильовий зв'язок  
ЦОЗ – центр оперативного зв'язку ДСНС

## Пункти управління



Пункт управління з цивільного захисту України



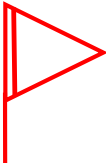
Пункт управління центрального органу виконавчої влади (ПУ), (ЗПУ) – запасний пункт управління



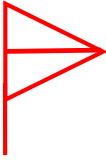
Пункт управління ГУ(У)ДСНС в областях та м. Київ



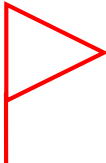
Пункт управління спеціального регіонального центру швидкого реагування, координаційного аварійно-рятувального центру, спеціальних формувань ДСНС



Пункт управління з цивільного захисту (ЦЗ) адміністративного району



Пункт управління з цивільного захисту (ЦЗ) міста (району міста)



Пункт управління аварійно-рятувального загону спеціального призначення ГУ (У)ДСНС



Пункти управління пожежно-рятувальної частини (позаштатних невоєнізованих формувань ЦЗ)



Пункт управління підрозділу аварійно-рятувальних, спеціалізованих, піротехнічних, пошукових та інших робіт





Пункт управління аварійно-рятувальної групи

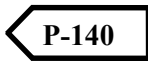
### Системи зв'язку та телекомунікацій



- 1 - польовий (рухомий); 2 - стаціонарний незахищений; 3 - стаціонарний захищений
- 4 - опорний (201 – номер вузла); 5 – допоміжний
- 6- контролю безпеки зв'язку



- 1 - радіостанція на кораблі
- 2 - радіостанція на літаку
- 3 - радіостанція на вертольоті



на бронетранспортері усередині знака вказується тип апаратної зв'язку

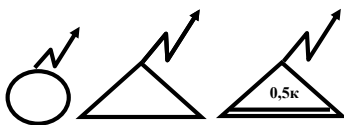


Стаціонарні вузли зв'язку державної мережі

- 1 - стаціонарний незахищений
- 2 - стаціонарний захищений

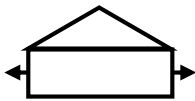


- 1 - радіоприймач (у середині символу – тип приймача);
- 2 - радіоретранслятор стаціонарний
- 3 - радіоретранслятор рухомий



Радіостанції

- 1 – переносна; 2 – радіостанція рухома(у середині символу - потужність передавача); 3 – радіостанція стаціонарна (у середині символу - потужність передавача)



Вузол фельд'єгерсько - поштового зв'язку (ФПЗ) із зазначенням дійсного найменування



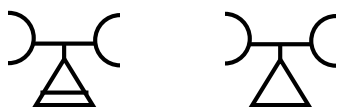
Станція ФПЗ із зазначенням дійсного найменування



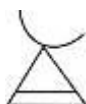
Комутатор



Шлюз

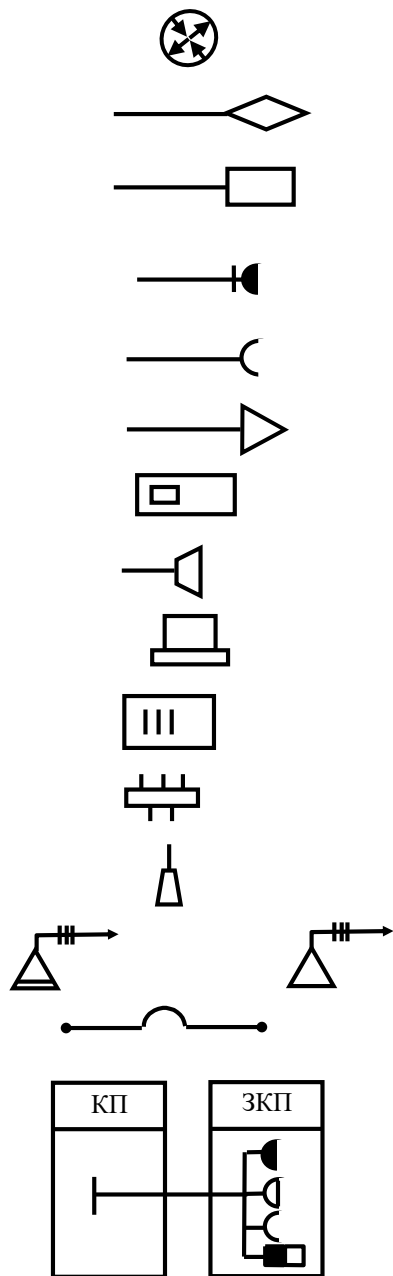


- 1 - Радіорелейна станція стаціонарна
- 2 - Радіорелейна станція рухома



Станція супутникового зв'язку:

- 1 – рухома
- 2 – стаціонарна



Маршрутизатор

Відкрита передача даних

Відкритий телеграфний зв'язок

Урядовий зв'язок

Відкритий телефонний зв'язок

Факсимільний зв'язок

Модем

Гучномовець

ПЕОМ

Сервер

Мережа Ethernet

Безпроводна точка доступу

1 - тропосферна станція стаціонарна

2 - тропосферна станція рухома

Комутація каналу

Телекомунікаційний напрямок з визначенням видів зв'язку;

## Основні документи, що регламентують діяльність підрозділів ДСНС з питань телекомунікацій та інформаційних технологій

Нормативно-правові акти:

Про державну таємницю : закон України від 21 січ. 1994 р. № 3855-XII / Відомості Верховної Ради України. – 1994. – № 16. – Ст. 93.

Про телекомунікації : закон України від 18 листоп. 2003 р. № 1280-IV / Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.

Про Національну програму інформатизації України : закон України від 4 лют. 1998 р. № 74/98-ВР / Відомості Верховної Ради України. – 1998. – № 27–28. – Ст. 181.

Про доступ до публічної інформації [Електронний ресурс] : закон України від 13 січ. 2011 р. № 2939-VI. – Режим доступу: <http://zakon.rada.gov.ua/laws/show/2939-17>.

Про Державну службу спеціального зв'язку та захисту інформації України : закон України від 23 лют. 2006 р. № 3475-IV / Відомості Верховної Ради України. – 2006. – № 30. – Ст. 258.

Про затвердження Положення про державний контроль за станом технічного захисту інформації [Електронний ресурс] : наказ Адміністрації Держ. служби спеціал. зв'язку та захисту інформації України від 16 трав. 2007 р. № 87. – Режим доступу: <http://zakon.rada.gov.ua/laws/show/v161007>.

Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади [Електронний ресурс] : постанова Кабінету Міністрів України від 10 верес. 2003 р. № 1433-п. <http://zakon.rada.gov.ua/laws/show/1433-2003-p>.

1 Про захист інформації в інформаційно-телекомунікаційних системах: закон України від 5 лип. 1994 р. № 80/94-ВР / Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.

3 Про захист персональних даних: закон України від 1 черв. 2010 р. № 2297-VI

Про інформацію : закон України від 2 жовт. 1992 р. № 2657-XII / Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

Про Національну програму інформатизації України : закон України від 4 лют. 1998 р. № 74/98-ВР / Відомості Верховної Ради України. – 1998. – № 27–28. – Ст. 181.

е Про основні засади забезпечення кібербезпеки України : закон України від 5 жовтня 2017 року № 2163-VIII XII / Відомості Верховної Ради України. – 2017. – № 45. – Ст. 403.

и

м ДСТУ

ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги

о ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки

т ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки

п ДСТУ ISO/IEC 27034-1:2017 (ISO/IEC 27034-1:2011; Cor 1:2014, IDT) Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 1. Огляд і загальні поняття

ДСТУ ETSI EG 202 057-2:2015 (ETSI EG 202 057-2:2011, IDT) Аспекти оброблення, передавання сигналів мовної інформації та забезпечення їхньої якості (STQ). Визначення і вимірювання важливих для споживача параметрів QoS. Частина 2. Послуги голосової телефонії, факсу групи 3 та передавання даних та коротких повідомлень (SMS) за допомогою модему

ДСТУ ETSI EG 202 057-4:2015 (ETSI EG 202 057-4:2008, IDT) Аспекти оброблення, передавання сигналів мовної інформації та забезпечення їхньої якості (STQ). Визначення і вимірювання важливих для споживача параметрів QoS. Частина 4. Доступ до «Інтернету»

ДСТУ ISO/IEC 27033-2:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 2. Настанови щодо проектування та реалізації безпеки мережі

ДСТУ ISO/IEC 27033-3:2016 Інформаційні технології. Методи захисту. Безпечність мережі. Частина 3. Еталонні мережеві сценарії. Загрози, методи проектування та проблеми керування

ДСТУ ISO/IEC 27033-4:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 4. Убезпечення комунікацій між мережами з використанням шлюзів безпеки

ДСТУ ISO/IEC 27033-5:2016 Інформаційні технології. Методи захисту. Безпечність мережі. Частина 5. Убезпечення комунікацій уздовж мереж із використанням віртуальних приватних мереж (VPNs)

ДСТУ EN 50600-1:2018 Інформаційні технології. Інфраструктура та устаткування центрів оброблення даних. Частина 1. Загальні положення

ДСТУ EN 50600-2-1:2018 Інформаційні технології. Інфраструктура та устаткування центрів оброблення даних. Частина 2-1. Будівлі та споруди центрів оброблення даних

ДСТУ EN 50600-2-2:2018 Інформаційні технології. Інфраструктура та устаткування центрів оброблення даних. Частина 2-2. Електропостачання

ДСТУ ISO/IEC 11801-1:2018 Інформаційні технології. Кабельні системи загальної призначеності для приміщень користувачів. Частина 1. Загальні вимоги

ДСТУ ISO/IEC 11801-2:2018 Інформаційні технології. Кабельні системи загальної призначеності для приміщень користувачів. Частина 2. Офісні приміщення

ДСТУ ISO/IEC 11801-5:2018 Інформаційні технології. Кабельні системи загальної призначеності для приміщень користувачів. Частина 5. Центри оброблення даних

ДСТУ 4113-2001 Апаратура оброблення інформації. Вимоги безпеки та методи випробування

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

ДСТУ EN 54-13:2014 Системи пожежної сигналізації. Частина 13. Вимоги щодо систем та оцінювання сумісності

ДСТУ-Н CEN/TS 54-14:2009 Системи пожежної сигналізації та оповіщення. Частина 14. Настанови щодо побудови, проектування, монтування, введення в експлуатацію, експлуатування і технічного обслуговування

ДБН, ДСН

ДБН В.2.5-23:2010 Інженерне обладнання будинків і споруд. Проектування електрообладнання об'єктів цивільного призначення

ДБН В.2.5-67:2013 Опалення, вентиляція та кондиціонування

ДБН В.2.5-56-2014 Системи протипожежного захисту

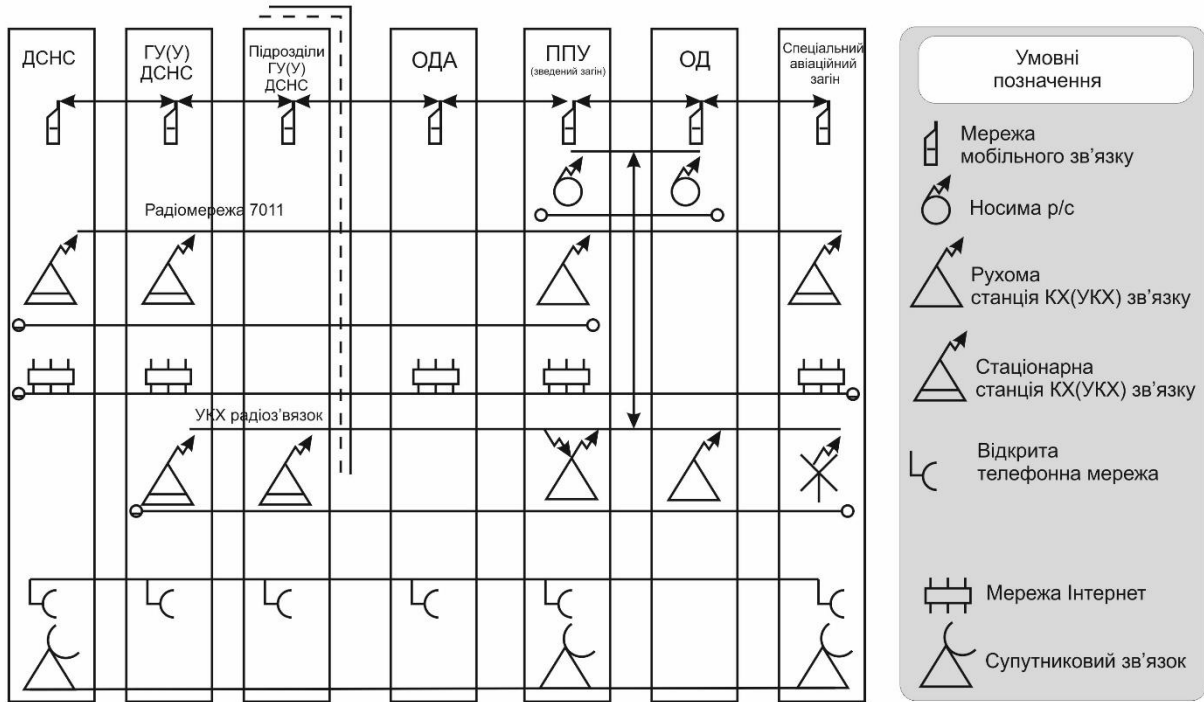
ДСН 3.3.6.042-99 Санітарні норми мікроклімату виробничих приміщень

Типові схеми

Типова схема організації зв'язку при ліквідації НС державного рівня

ЗАТВЕРДЖУЮ  
 Начальник ГУ(У) ДСНС України  
 у \_\_\_\_\_ області

СХЕМА  
 ОРГАНІЗАЦІЇ ЗВ'ЯЗКУ ПРИ ЛІКВІДАЦІЇ НС ДЕРЖАВНОГО РІВНЯ

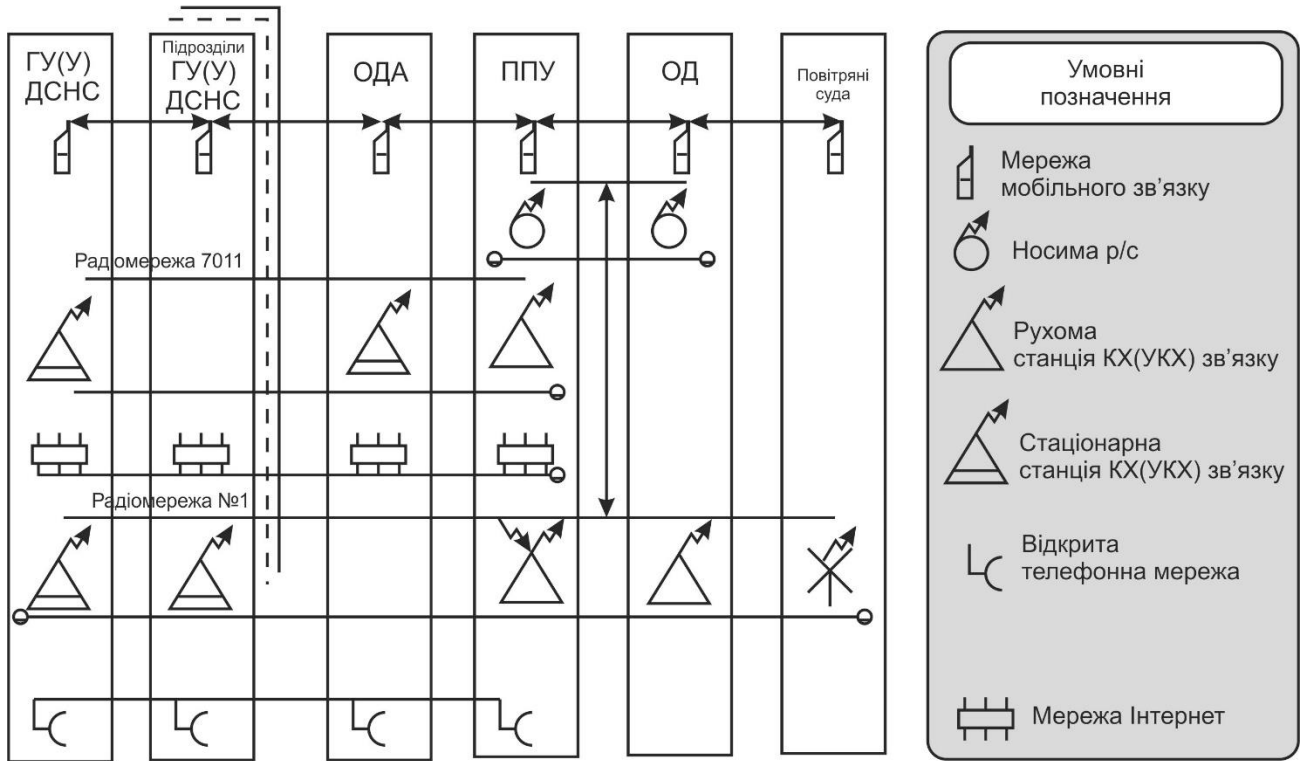


Начальник сектору (центру) \_\_\_\_\_

## Типова схема організації зв'язку при ліквідації НС регіонального рівня

ЗАТВЕРДЖУЮ  
Начальник ГУ(У) ДСНС України  
у \_\_\_\_\_ області

### СХЕМА ОРГАНІЗАЦІЇ ЗВ'ЯЗКУ ПРИ ЛІКВІДАЦІЇ НС РЕГІОНАЛЬНОГО РІВНЯ

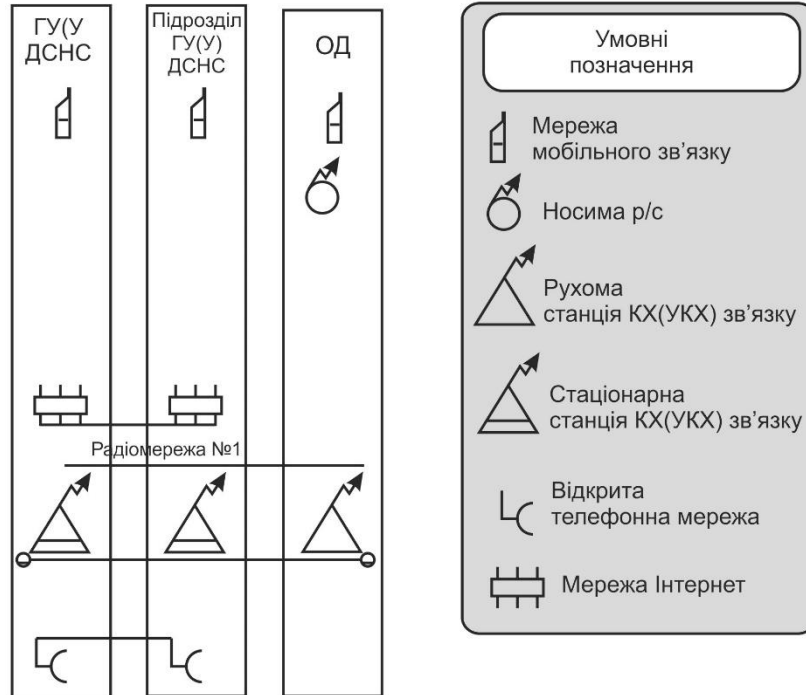


Начальник сектору (центру) \_\_\_\_\_

# Типова схема організації зв'язку при ліквідації НС місцевого рівня

ЗАТВЕРДЖУЮ  
Начальник ГУ(У) ДСНС України  
у \_\_\_\_\_ області

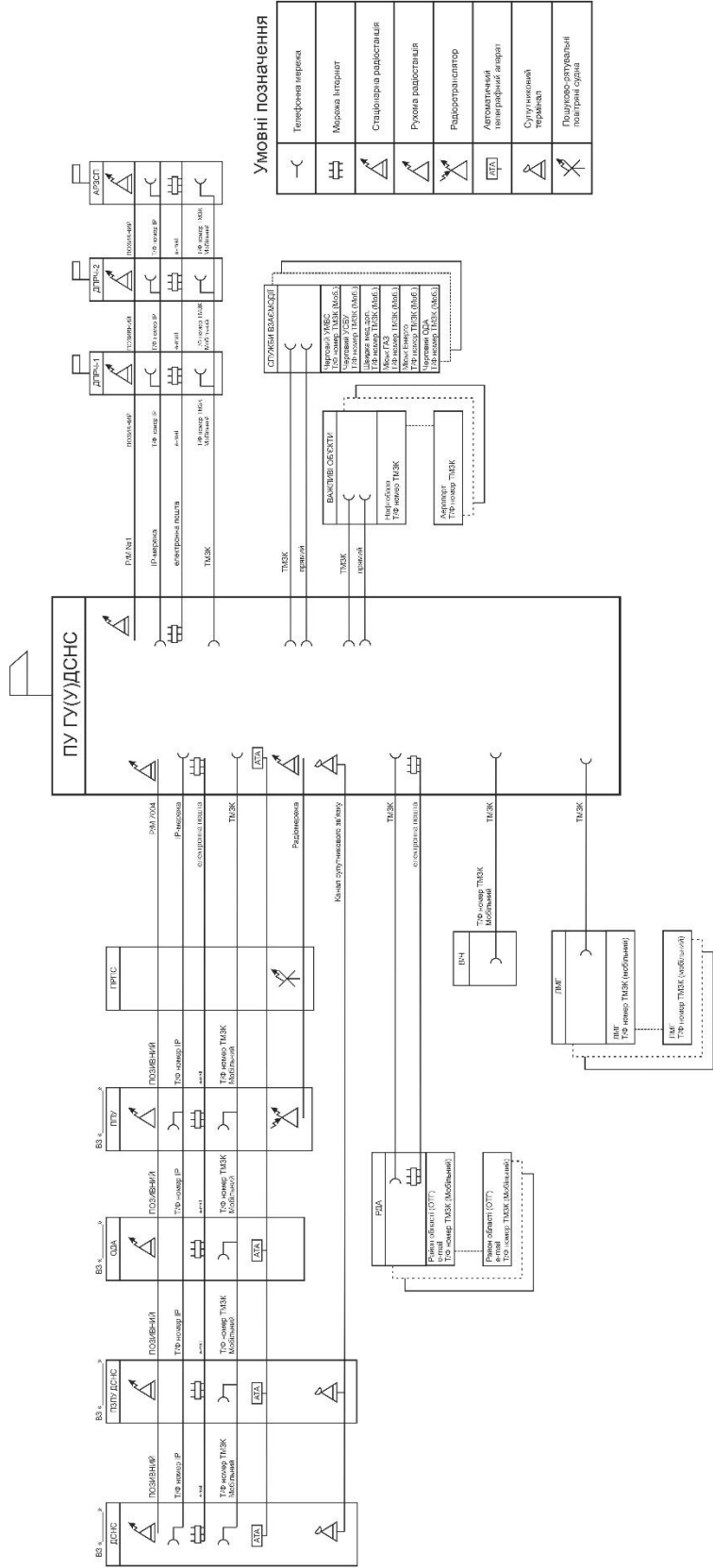
## СХЕМА ОРГАНІЗАЦІЇ ЗВ'ЯЗКУ ПРИ ЛІКВІДАЦІЇ НС МІСЦЕВОГО РІВНЯ



Начальник сектору (центру) \_\_\_\_\_

## **Типова схема оперативного зв'язку ГУ(У)ДСНС у області**





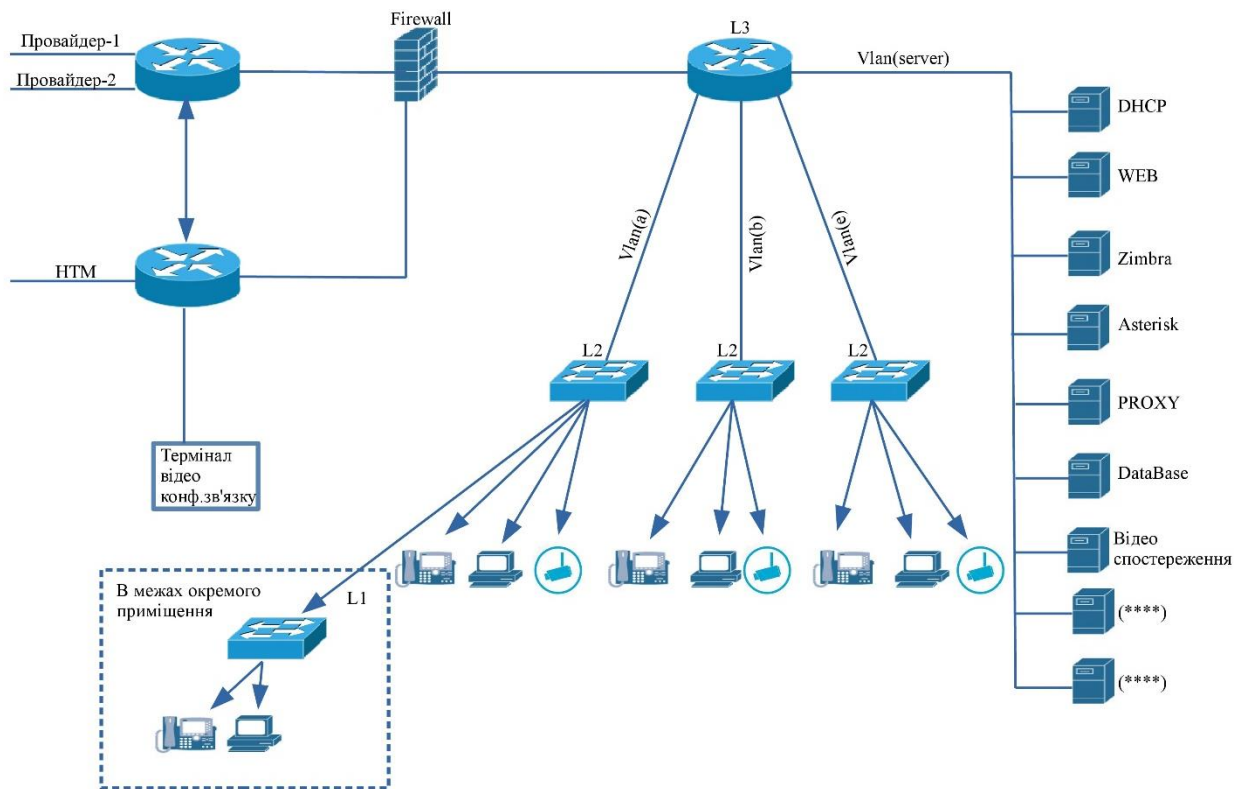
**УМОВНІ ПОЗНАЧЕННЯ**

	Телефонна мережа
	Мобільна Інтернет
	Стационарна радіостанція
	Рухлива радіостанція
	Радіостанція слотер
	Автоматичний телеграфічний апарат
	Ступінчастий термінал
	Портативний мобільний телефон

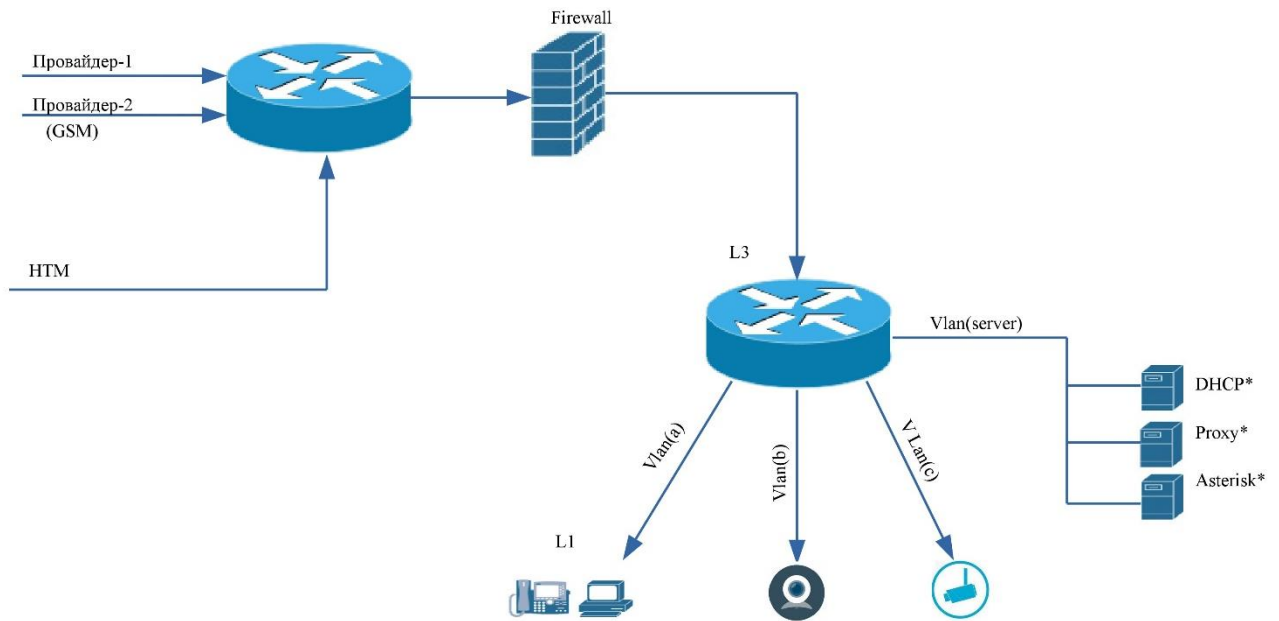
начальник сектору (центру)



## Типова схема локальної обчислювальної мережі територіальних органів ДСНС центрального підпорядкування



## Типова схема локальної обчислювальної мережі районних підрозділів



\*-за наявності (або використання ресурсів ГУ(У)Області)

**Схема структури служби зв'язку в ДСНС**  
(надасть Тарас Олексійович)

**АПАРАТНИЙ ЖУРНАЛ**

Дата	Час		Зміст запису (запис про відкриття і закриття зв'язку, з ким і яка велась робота текст прийнятих і переданих розпоряджень, приймання і здавання чергувань, перевірка зв'язку та інші відмітки)	Якість зв'язку	Хто передав або прийняв повідомлення (посада і прізвище)
	год.	хв.			

### Правила ведення радіообміну

Системи УКХ радіозв'язку використовують два основні режими обміну інформацією: симплексний та дуплексний, за необхідності – напівдуплексний.

Якщо передача і прийом повідомлень здійснюється по черзі, такий зв'язок називається симплексним. Якщо передача і прийом повідомлень здійснюється одночасно, такий зв'язок називається дуплексним.

Симплексний режим передбачає можливість почергової передачі та прийому інформації, змінюючи органами управління режим роботи засобу зв'язку (передача – прийом). При симплексному режимі радіообміну в каналі зв'язку використовується одна несуча частота.

Дуплексний режим передбачає можливість одночасної передачі і прийому інформації без маніпуляції органами управління засобу зв'язку. При дуплексному режимі радіообміну в каналі зв'язку використовуються дві несучі частоти. Це робиться для того, щоб приймач приймав тільки сигнали від передавача з протилежного пункту і не приймав сигнали власного передавача.

Напівдуплексний режим – стандарт голосового зв'язку із двостороннім радіоінтерфейсом і можливістю передачі сигналу одночасно тільки в одному напрямку. При напівдуплексному режимі вказана радіостанція автоматично переходить в режим постійної передачі інформації про обстановку навколо неї.

Встановлення радіозв'язку – це процес визначення і розпізнавання радіостанцій для проведення між ними радіообміну.

Процес радіообміну складається з наступних операцій:

- 1) підготовка радіостанції до роботи;
- 2) включення радіостанції;
- 3) виклик абонента;
- 4) передача радіограми;
- 5) закінчення радіообміну.

Радіообмін – це передача і прийом радіограм, сигналів, команд і ведення переговорів по радіо.

За змістом радіообмін поділяється на :

- оперативний;
- службовий.

Оперативний радіообмін включає передачу радіограм, сигналів, команд і оперативних повідомлень.

Службовий радіообмін проводиться з питань, пов'язаних з встановленням зв'язку, регулюванням радіоапаратури та забезпеченням роботи радіостанцій.

Якість зв'язку в радіомережі значною мірою залежить від дисципліни та дотримання правил радіообміну.

При передачі слід дотримуватись таких правил:

- 1) подумки сформулюйте повідомлення якомога більш чітко і коротко;
- 2) прослухайте, чи канал вільний від переговорів;
- 3) подайте тональний виклик (1–2 с);
- 4) натисніть кнопку ПЕРЕДАЧА і передавайте повідомлення.

Слід дотримуватись встановленого порядку ведення переговорів, користуватися лише встановленими позивними.

Радіообмін повинен бути лаконічним, містити мінімальну кількість слів і фраз, при цьому важлива інформація повторюється двічі.

При проведенні сеансу радіозв'язку категорично забороняється:

1. Називати посади, прізвища, імена та звання посадових осіб.
2. Вести особисті розмови.
3. Передавати відомості, що містять державну або службову таємницю.
4. Передавати відомості, що можуть розкрити суть оперативних заходів.
5. Використовувати під час передачі довільні радіопозивні.

6. Самовільно без дозволу керівництва вимикати радіостанцію.

7. Перевіряти канал зв'язку шляхом проведення переговорів.

Грубим порушенням правил радіообміну є невихід на зв'язок.

При використанні радіозв'язку для відкритої передачі дозволені наступні відомості:

1. Про стихійні лиха, нещасні випадки (крім особливо важливих об'єктів і кількість жертв).
2. Про ДТП (крім тих, у яких загинуло п'ять і більше людей, травмовано десять і більше людей).
3. Виклик працівників швидкої допомоги до місця пригоди.
4. Про технічний стан наявних засобів зв'язку і службового транспорту.
5. Про стан системи ОПС, електроживлення і телефонного зв'язку на об'єкті, що охороняється.
6. Про метеорологічні та дорожні умови.

Для передачі таємної інформації потрібно застосовувати кодові таблиці, які розробляються та затверджуються на місцях.

Порядок встановлення, перевірки якості зв'язку і передачі радіограм

Радіограми передаються в наступному порядку:

- 1) встановити перемикачем каналів необхідний робочий канал зв'язку;
- 2) встановити відповідним перемикачем тональний виклик;
- 3) включити радіостанцію (після включення радіостанція перебуває в режимі «Черговий прийом»);
- 4) встановити необхідний рівень гучності та шумоглушення;
- 5) шляхом прослуховування каналу зв'язку переконатися, що в даний момент радіообмін між іншими радіостанціями відсутній;
- 6) переключити радіостанцію в режим роботи «Посилка тонального виклику» та здійснити послідовно тональний виклик протягом 2–3 с;
- 7) переключити радіостанцію в режим «Передача» та викликати абонента голосом, наприклад: «Буквар 102, Буквар 102, я Буквар 101. Як мене чуєте? Прийом.»;
- 8) абонент повинен відповісти: «Буквар 101, Буквар 101, я Буквар 102. Чую Вас добре (якість зв'язку можна оцінювати за п'ятибальною шкалою). Прийом.»;
- 9) після цього зв'язок вважається встановленим і далі виконується передача радіограм. Передача радіограм повинна вестися неквапливо. Кожне слово слід вимовляти чітко, розбірливо, з правильними закінченнями та поставленим наголосом. Говорити треба голосно, але не кричати в мікрофон, тому що від галасу погіршується розбірливість і чіткість передачі;
- 10) закінчує радіообмін той абонент, який першим вийшов на зв'язок. Ознакою закінчення сеансу радіообміну служить фраза: «Буквар 102, Буквар 102, я Буквар 101. До зв'язку, відбій»;
- 11) після цього усі радіостанції, які беруть участь у радіообміні переходять у режим «Черговий прийом».

При передачі повідомлення всім (циркуляр) або кільком радіостанціям мережі оператор передає: «Увага всім, або Буквар 21, 22, 23, я Буквар. Приготуватися до прийому», повторює цю фразу ще раз, робить паузу і передає текст повідомлення двічі. Кореспонденти відповідають: «Буквар, я Буквар 21, Вас зрозумів. Буквар, я Буквар 22, Вас зрозумів» тощо.