УДК 621.391:007; 621.394/.396.019.3

КІБЕРПРОСТІР, УПРАВЛІННЯ ІНФРАСТРУКТУРОЮ, КІБЕРБЕЗПЕКА

С. В. Рибка, Є. В. Кільчицький, О. М. Післегін

Ми живемо в період, коли, на жаль, стало реальністю таке явище, як інформаційна війна, що уявляє собою міжнародне протиборство у кіберпросторі з метою проникнення в інформаційно – комунікаційні та інші інфраструктури, процеси та ресурси, що є критично важливими для держави і суспільства, з метою нанесення збитків або шкоди, підриву політичної, економічної та соціальної систем, масового психологічного впливу на населення для дестабілізації суспільства і держави, а також примушення держави приймати рішення в інтересах протиборчої сторони.

Сьогодні не існує однозначно визнаного міжнародним співтовариством визначення кіберпростору. Визначення, що використовуються як в офіційних документах, так і в публікаціях, великою мірою залежать від того, з якої точки зору розглядається кіберпростір.

Наприклад, в [13] кіберпростір визначено як складне середовище, яке не існує ні в якій фізичній формі, та виникає в результаті взаємодії людей, програмного забезпечення, інтернет – сервісів за допомогою технологічних пристроїв та мережевих зв'язків. У [12] застосоване таке визначення: «Кіберпростір – сфера діяльності в інформаційному просторі, утворена сукупністю комунікаційних каналів Інтернету та інших телекомунікаційних мереж, технологічної інфраструктури, що забезпечує їх функціонування, і будь-яких форм людської активності (особистості, організації, держави), здійснюваної за допомогою їх використання».

У цій статті ми пропонуємо визначення цього терміна з точки зору захисту інформаційно-комунікаційної інфраструктури, як невід'ємної складової частини тріади: інформація, інфраструктура, людська діяльність (див. рисунок 1).

Тріада – в філософії термін, що передає структурну триєдність або динамічну трифазність, якого-небудь процесу або явища [14].

Першим складником цієї тріади є **інформація у цифровому вигляді**: статичному (файли, реєстри, бази, архіви даних – електронні інформаційні ресурси) і динамічному (пакети, потоки, команди, запити тощо). Інформація (дані) створюється, обробляється, зберігається в автоматизованих системах та передається із застосуванням ресурсів складових частин **інформаційно-комунікаційної інфраструктури**, і подається (відображується) на термінальному обладнанні користувачів у графічному, текстовому, відео- або аудіо- вигляді.

Другим складником тріади виступає **інформаційно-комунікаційна інфраструктура** (див. рисунок 2), яка є сукупністю взаємоз'єднаних телекомунікаційних мереж загального користування (ТМЗК) фіксованого, мобільного, супутникового зв'язку, міжнародних магістральних транзитних

Рибка Сергій Володимирович – кандидат технічних наук, голова правління ПрАТ «Український інститут із проектування і розвитку інформаційно-комунікаційної інфраструктури «Діпрозв'язок»

Кільчицький Євген Васильович – кандидат технічних наук, перший заступник голови правління з наукової діяльності ПрАТ «Український інститут із проектування і розвитку інформаційно-комунікаційної інфраструктури «Діпрозв'язок»

Післегін Олександр Миколайович – радник голови правління ПрАТ «Український інститут із проектування і розвитку інформаційно-комунікаційної інфраструктури «Діпрозв'язок»

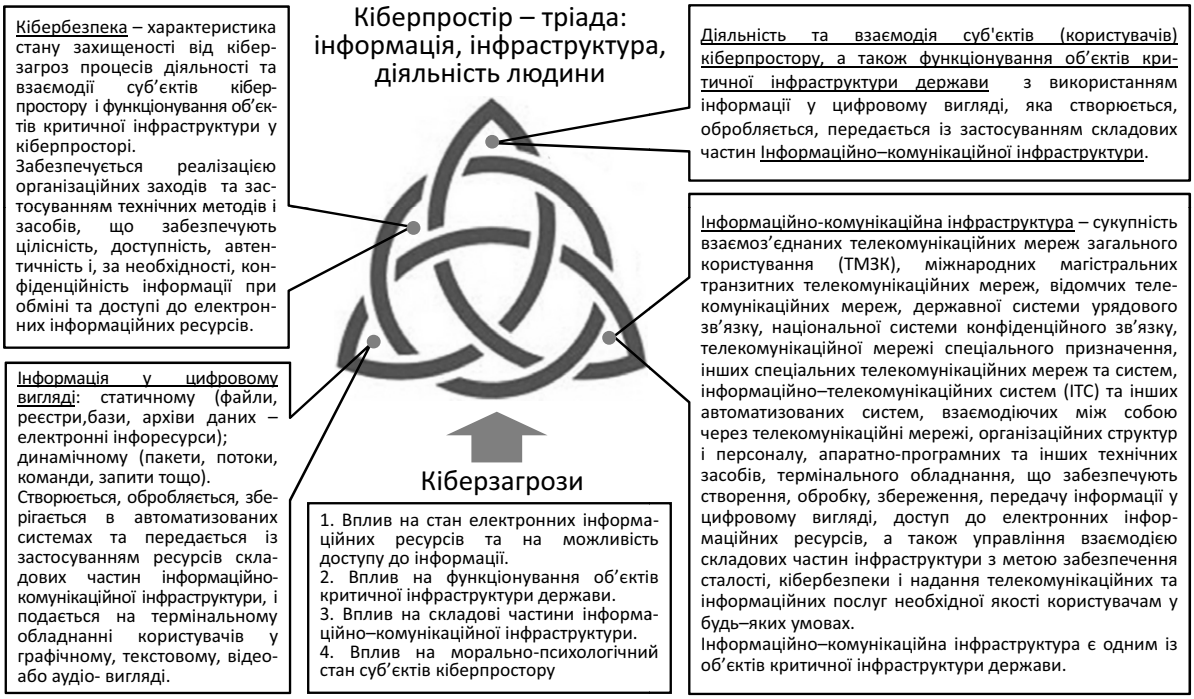

Рисунок 1. **Кіберпростір, управління інфраструктурою, кібербезпека**

Рисунок 2. **Національна інформаційно – комунікаційна інфраструктура (НІКІ)**

телекомунікаційних мереж, організованих з використанням ресурсів ТМЗК, відомчих телекомунікаційних мереж, державної системи урядового зв'язку, національної системи конфіденційного зв'язку, телекомунікаційної мережі спеціального призначення, інших спеціальних телекомунікаційних мереж, інформаційно – телекомунікаційних систем (ІТС) та інших автоматизованих систем, взаємодіючих між собою через телекомунікаційні мережі, а також правових та нормативних механізмів, організаційних структур і персоналу, апаратно-програмних та інших технічних засобів, термінального обладнання, що забезпечують створення, обробку, збереження, передачу інформації у цифровому вигляді, доступ до електронних інформаційних ресурсів, а також **управління взаємодією складових частин (об'єктів) інфраструктури з метою забезпечення її кібербезпеки** і надання телекомунікаційних та інформаційних послуг необхідної якості користувачам за будь-яких умов.

Зазначимо іще раз, що Національна **інформаційно-комунікаційна інфраструктура є одним із об'єктів критичної інфраструктури держави** разом із об'єктами енергетики та електропостачання, транспорту, хімічної промисловості тощо. Одними із основних вимог до складників «критичної інфраструктури» є:

1. Захист від фізичного руйнування та забезпечення сталості;

2. Захист від кіберзагроз та забезпечення кібербезпеки;

Нарешті, третім складником тріади є кінцеві користувачі (споживачі), діяльність та взаємодія яких як суб'єктів кіберпростору, а також функціонування об'єктів критичної інфраструктури держави здійснюється з використанням інформації у цифровому вигляді, яка створюється, обробляється, передається із застосуванням складових частин **інформаційно-комунікаційної інфраструктури.**

Кіберпростір держави і, зокрема, національна інформаційно – комунікаційна інфраструктура (надалі – НІКІ) знаходяться під реальними і потенційними кіберзагрозами, (див. рисунок 1), а саме:

– впливу на стан електронних інформаційних ресурсів та на можливість доступу до інформації;

– впливу на функціонування об'єктів критичної інфраструктури;

– впливу на складові частини інформаційно – комунікаційної інфраструктури;

– впливу на морально-психологічний стан суб'єктів кіберпростору.

Характеристика стану захищеності від **кіберзагроз** процесів діяльності та взаємодії суб'єктів **кіберпростору** і функціонування об'єктів критичної інфраструктури у **кіберпросторі** може бути визначене як кібербезпека. Кібербезпека забезпечується реалізацією організаційних заходів та застосуванням технічних методів і засобів, що забезпечують цілісність, доступність, автентичність і, за необхідності, конфіденційність інформації при обміні та доступі до електронних інформаційних ресурсів.

Кібербезпека охоплює не тільки інформацію, як об'єкт захисту, не виключно технічні засоби, які визначають можливості функціонування інформації, а захист способів функціонування нової сутності – кіберпростору.

Кібербезпека є необхідною умовою розвитку інформаційного суспільства. Захищається діяльність людей, яка здійснюється за допомогою інформації, поширюваної за допомогою інформаційно-комунікаційної інфраструктури [11].

Зважаючи на наведене вище, можливо визначити **кіберпростір** як середовище, утворене організованою сукупністю інформаційних процесів (створення інформації, передача, використання) за участю людини, у тому числі на об'єктах «критичної інфраструктури» держави, з використанням ресурсів складових частин **Національної інформаційно-комунікаційної інфраструктури**, управління **взаємодією складових частин** якої **з метою забезпечення кібербезпеки** і надання телекомунікаційних та інформаційних послуг необхідної якості користувачам у будь-яких умовах повинно здійснюватись національним центром оперативно-технічного управління (НЦУ), як головною складовою частиною системи оперативно-технічного управління телекомунікаціями.

Роль та проблеми національної інформаційно – комунікаційної інфраструктури

Національна інформаційно – комунікаційна інфраструктура є технологічним фундаментом життєдіяльності інформаційного суспільства. Вона відноситься до «**критичної інфраструктури**» держави, оскільки від сталого та надійного функціонування усіх її складових частин залежить **кібербезпека**, можливість управління державою, забезпечення потреб оборони та безпеки, функціонування промисловості, кредитно-фінансової і банківської систем, енергетичних, транспортних інфраструктур, комунального господарства, цивільного захисту, врешті – можливість безумовної реалізації конституційних прав громадян на комунікації та можливість отримання інформації у будь-яких умовах.

Склад національної інформаційно – комунікаційної інфраструктури (рис.2) наведений вище.

Необхідно зазначити, що з використанням ресурсів складових НІКІ повинні будуватись (організовуватись) компоненти мережі екстрених телекомунікацій та системи централізованого оповіщення (рис. 3).

Інфраструктура, що існує і розвивається дефакто у вельми ліберальному правовому полі, має чимало проблем. Це і правові і технічні проблеми, проблеми взаємоз'єднання та взаємодії, технологічні проблеми, проблеми кібернетичної безпеки, сталості і надійності тощо. Але ключовою проблемою НІКІ є відсутність цілісної системи управління, тобто відсутності

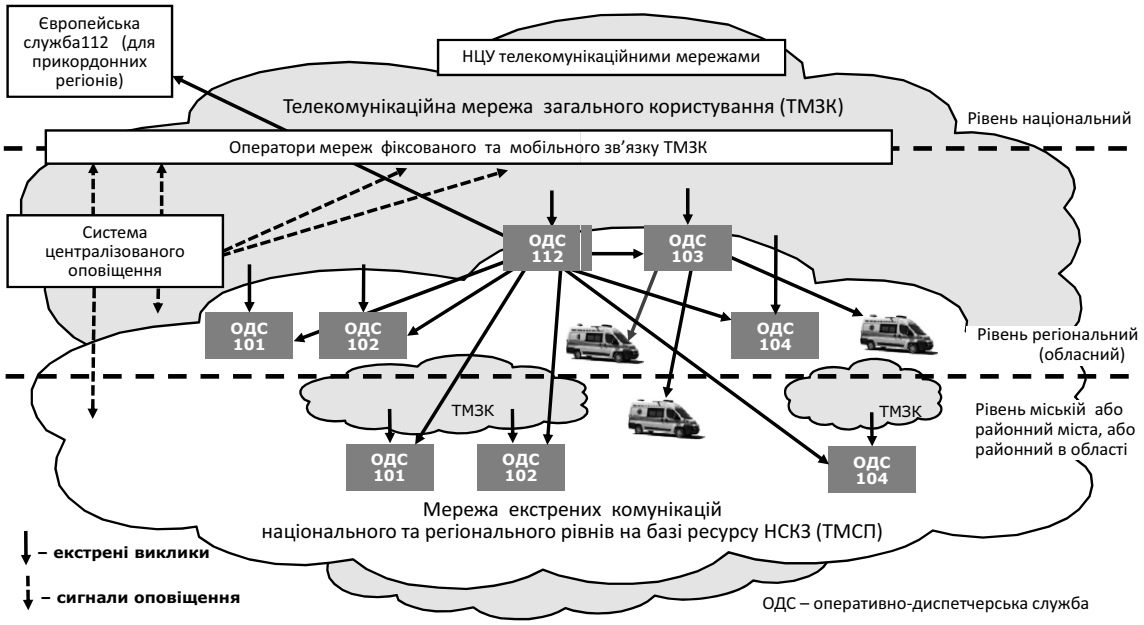

Рисунок 3. **Загальна структурна схема екстрених телекомунікацій та системи централізованого оповіщення**

у держави можливості забезпечувати моніторинг і оцінку стану складових частин інфраструктури за багатьма критеріями та в екстремальних умовах забезпечити можливість використання ресурсів усіх цих складових. Всупереч законодавству досі не створено ні системи, ні державного національного центру оперативно – технічного управління телекомунікаційними мережами.

Затверджена нещодавно Стратегія національної безпеки України [5] пріоритетами забезпечення безпеки критичної інфраструктури зокрема визначає:

комплексне вдосконалення правової основи захисту критичної інфраструктури, створення системи державного управління її безпекою;

посилення охорони об'єктів критичної інфраструктури;

налагодження співробітництва між суб'єктами захисту критичної інфраструктури, розвиток державно-приватного партнерства у сфері запобігання надзвичайним ситуаціям та реагування на них;

моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації;

забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації;

Таким чином, термінове створення НЦУ та системи оперативно – технічного управління ресурсами телекомунікаційними мереж НІКІ, як одного із об'єктів критичної інфраструктури держави, є одним із найважливіших завдань для забезпечення кібербезпеки національного сегменту кіберпростору.

Варіанти вирішення наболілої проблеми створення НЦУ, поставленої на законодавчому рівні дванадцять років тому, багаторазово обговорювалися на різних рівнях, приймалися постанови з тимчасовими рішеннями, декларувались стратегічні наміри, видавалися укази, але досі у державі не створено можливості реального управління ресурсом всіх без винятку телекомунікаційних мереж країни, значна частина яких побудована за бюджетні гроші. Такий стан призводить до неможливості прийняття оперативних та ефективних рішень управління на державному рівні щодо забезпечення кібербезпеки національної інформаційно – комунікаційної інфраструктури, використання ресурсів усіх телекомунікаційних мереж в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, зокрема в інтересах управління державою, забезпечення потреб оборони та безпеки держави.

Зауважимо іще раз, що вирішення цієї задачі – це не тільки гарантоване забезпечення зв'язком в особливих ситуаціях органів державного управління, силових структур, інших спецспоживачів, але також гарантоване забезпечення телекомунікаційним ресурсом системи централізованого оповіщення населення, системи екстреної допомоги, нарешті простих громадян, що є обов'язком держави.

Законодавчих підстав для організації і проведення робіт зі створення національного, підкреслимо державного, центру управління більш, ніж достатньо [1–3,5–9].

Науковцями і фахівцями Українського інституту із проектування і розвитку інформаційно – комунікаційної інфраструктури «Діпрозв'язок» у 2014 році проведено системне дослідження національної телекомунікаційної інфраструктури з метою визначення та обґрунтування основних принципів побудови системи оперативно – технічного управління телекомунікаційними мережами України (надалі – СОТУ), визначення основних завдань та функцій національного центру оперативно – технічного управління телекомунікаційними мережами України, як основної складової частини СОТУ, визначення та обґрунтування варіантів можливих організаційно – технічних, технологічних та будівельних проектних рішень щодо створення НЦУ, формулювання основних вимог та оцінка необхідних витрат щодо реалізації цих рішень.

Основні результати дослідження:

– проведений системний аналіз та попередня оцінка стану усіх телекомунікаційних мереж, що є складовими національної інформаційно – комунікаційної інфраструктури, визначено перелік операторів телекомунікацій (загального користування, відомчих, спеціальних), мережі яких можуть та повинні розглядатись як об'єкти управління;

– визначено та обґрунтовано основні принципи побудови СОТУ, основні завдання та функції НЦУ, як основної складової частини СОТУ, у тому числі завдання забезпечення телекомунікаційним ресурсом систем централізованого оповіщення та екстреної допомоги;

– визначено склад нормативно-правових та нормативних документів, необхідних для забезпечення функціонування НЦУ та СОТУ;

– визначено та обґрунтовано основні організаційні і технічні вимоги до НЦУ, його основних функціональних частин, інженерної інфраструктури, комплексної системи захисту інформації відповідно до [4, 10];

– запропоновано варіанти можливих організаційно – технічних, технологічних та будівельних проектних рішень НЦУ;

– надано оцінку обсягів видатків, необхідних для розробки нормативних документів, проектної документації та будівництва НЦУ.

У цій статті застосовані нові терміни або такі, визначення яких певною мірою відрізняються від застосованих у чинних нормативно – правових актах та нормативних документах. Визначення змістовної частини терміну (поняття) **національна інформаційно – телекомунікаційна інфраструктура,** запропоноване нами, наведено вище. Нижче наведено визначення термінів, які мають відношення до управління складовими частинами інфраструктури, а саме:

система оперативно – технічного управління телекомунікаційними мережами України (СОТУ) – сукупність нормативно – правових та нормативних документів, організаційних заходів, споруд центрів управління, технічних засобів телекомунікацій та інших технічних засобів, а також персоналу, що у звичайних умовах забезпечує безперебійне, стале функціонування телекомунікаційних мереж відповідно до їх призначення та надання споживачам телекомунікаційних послуг нормованої якості, а в умовах надзвичайних ситуацій (у тому числі на телекомунікаційних мережах) і в умовах надзвичайного та воєнного стану забезпечує реалізацію способів, методів і механізмів оперативного прийняття рішень та управління ресурсами усіх телекомунікаційних мереж України (незалежно від їх функціонального призначення, форми власності чи відомчої приналежності) з метою пріоритетного використання цих ресурсів для потреб управління державою, національної безпеки, оборони, охорони правопорядку;

національний центр оперативно – технічного управління телекомунікаційними мережами (НЦУ) – організаційно – технічна структура державної форми власності у складі СОТУ, яка забезпечує виконання завдань та функцій відповідно до положення про НЦУ, що затверджується Кабінетом Міністрів України.

Стан телекомунікаційних мереж України, як об'єктів управління

Формулювання основних принципів побудови системи оперативно – технічного управління телекомунікаційними мережами України, переліку завдань і функцій СОТУ та НЦУ можливе лише з позицій системного аналізу складу, кількості операторів телекомунікацій, обсягів та технічного рівня ресурсів їхніх телекомунікаційних мереж, як об'єктів управління.

Створення централізованої системи управління такою різнорідною інфраструктурою, в якій в окремих складових частинах використовуються різні технології і технічні рішення, різні організаційні принципи, яка постійно розвивається, є дуже складною задачею, що потребує введення певних обмежень, поступовості та розподілу за рівнями управління.

Значна кількість учасників ринку телекомунікацій України (понад 4200 – за даними Реєстру операторів, провайдерів телекомунікацій, який ведеться НКРЗІ, надалі – Реєстр) та не менша кількість видів діяльності, що знаходяться у сфері регулювання ринку телекомунікацій та ліцензуються або реєструються, потребує певного структурування та обмеження об'єктів управління СОТУ.

Було прийнято допущення, що на першому етапі створення системи оперативно – технічного управління найбільш важливим ресурсом телекомунікаційних мереж є волоконно – оптичні лінії зв'язку (ВОЛЗ), канали і тракти мереж міжміського та міжнародного зв'язку. Виходячи з цього допущення доцільно обмежити кількість об'єктів управління шляхом мінімізації кількості операторів телекомунікацій за такими критеріями:

розмір мереж оператора (протяжність та потужність);

присутність на національному, регіональному чи лише на місцевому рівнях та надання у користування оптичних волокон, трактів, каналів;

застосування сучасних телекомунікаційних технологій;

наявність власного центру управління мережами.

В результаті проведеного аналізу встановлено, що за таких обмежень до переліку операторів телекомунікацій, мережі яких доцільно розглядати в якості об'єктів управління на першому етапі створення НЦУ, можуть бути віднесені 16 операторів, які за даними Реєстру мають ліцензії на операторську діяльність, у тому числі: ПАТ «Укртелеком, ПрАТ «Київстар», ПАТ «МТС Україна», ТОВ «Астеліт», ТОВ «Датагруп», ТОВ «Євротранстелеком», ТОВ «Атраком», ПрАТ «Фарлеп Інвест»- Вега, ТОВ «Інтертелеком», ТОВ «Велтон Телеком», Державний концерн РРТ та інші.

До цього переліку також повинні бути віднесені власники відомчих телекомунікаційних мереж (Укртранснафта, Укртрансгаз, Укртрансенерго, Укрзалізниця, Укравтодор – усього 5) та власники спеціальних мереж зв'язку.

В дослідженні проведено аналіз стану телекомунікаційних мереж основних операторів, які володіють транспортними телекомунікаційними мережами загального користування. Ці мережі мають такі характерні особливості:

– мережі в значній частині проходять територією України за тими же або близькими, але рознесеними маршрутами;

– мережі мають численні вузли перетину і сполучення;

– мережі мають виходи за кордон і сполучення з мережами суміжних держав;

– телекомунікаційні мережі загального користування знаходяться у приватній власності;

– частина ресурсу наведених мереж використовується для організації міжнародних магістральних транзитних мереж, які:

а) мають точки обміну трафіком на території України;

б) керовані з центрів управління, розташованих поза територією України.

Топологія відомчих телекомунікаційних мереж також практично повторює маршрути телекомунікаційних мереж загального користування.

Характерні особливості відомчих мереж:

– мережі використовуються в основному для технологічних цілей;

– мережі мають незначну кількість взаємозв'єднань з телекомунікаційними мережами загального користування;

– емність (потужність) цих мереж за попередніми оцінками є надлишковою, має значний незадіяний ресурс, зокрема – «темні волокна» на волоконно-оптичних лініях;

– мережі побудовані за державні кошти і знаходяться у державній власності.

Структура і вимоги до СОТУ та НЦУ

Далі перейдемо до короткого розгляду структури СОТУ. На рис. 4 наведено інфографіку складових частин СОТУ та схему їх інформаційної взаємодії.

Тут зображені складові частини СОТУ, яка формується з урахуванням результатів аналізу телекомунікаційної складової інфраструктури та вибору операторів і власників мереж за прийнятими вище критеріями.

Головною складовою частиною СОТУ повинен стати Національний центр управління, як організаційно-технічна структура державної власності, що знаходиться у сфері управління Центрального галузевого органу влади [6] і забезпечує виконання завдань і функцій відповідно до положення про НЦУ, що затверджує Кабінет Міністрів України.

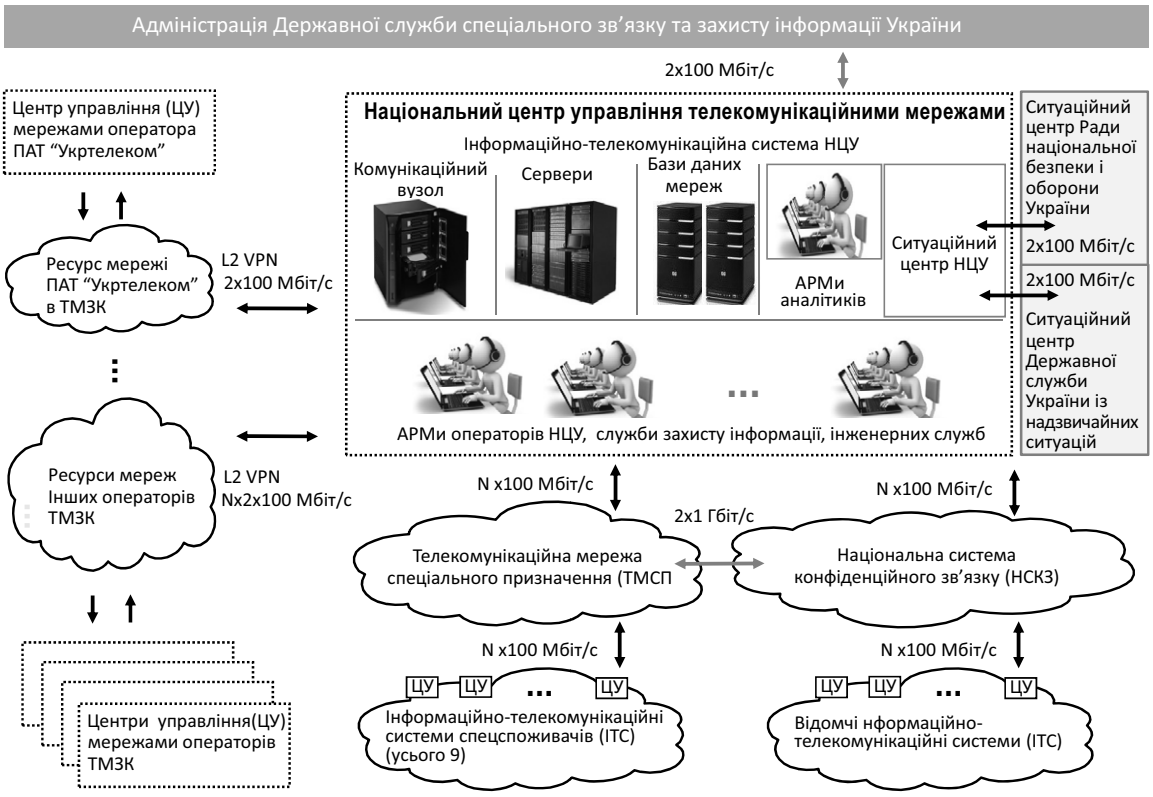

Рисунок 4. **Складові частини СОТУ та схема їх інформаційної взаємодії**

Система управління повинна будуватися за централізовано-децентралізованим принципом, що означає:

децентралізацію моніторингу стану телекомунікаційної мережі кожного оператора, надання інформації про стан мережі до НЦУ, здійснення самостійного управління мережею у звичайних умовах, виконання рекомендацій або команд управління від НЦУ у надзвичайних умовах. Ці функції виконують центри управління операторів;

централізацію постійного моніторингу і аналізу стану всіх без винятку телекомунікаційних мереж (за декількома критеріями, зокрема за критеріями сталості, захищеності від кіберзагроз) та, залежно від результатів аналізу і ситуації, прийняття рішень з координації та управління, зокрема щодо протидії кібератакам і впливу на джерела кібератак, про перерозподіл ресурсів складових частин інформаційно–комунікаційної інфраструктури у разі їх фізичного або функціонального ураження (тобто у надзвичайних умовах), вироблення відповідних рекомендацій або команд управління. Ці функції покладаються на НЦУ.

За своєю технічною та технологічною суттю НЦУ представляє досить великий центр обробки даних – автоматизовану систему, що має інформаційно – телекомунікаційну та інформаційно – аналітичну підсистеми, до складу яких повинні входити:

– серверний вузол, що забезпечує виконання функціональних завдань НЦУ;

– бази та сховища даних про телекомунікаційні мережі та їхні стан;

– телекомунікаційний вузол, що забезпечує організацію каналів управління до центрів операторів телекомунікаційних мереж;

– робочі місця операторів НЦУ з різних видів мереж.

Необхідним елементом НЦУ має стати ситуаційний центр, який забезпечить роботу загальносистемних (або інфраструктурних) аналітиків при вирішенні проблем, що виникають у надзвичайних ситуаціях та в особливий період, у тому числі при виявленні кібератак на телекомунікаційні складові НІКІ. Ситуаційний центр повинен взаємодіяти з ситуаційними центрами РНБО України та ДСНС (рис. 4).

Функціонування складових частин НЦУ повинна забезпечувати інженерна інфраструктура, склад якої характерний для центрів обробки даних (ЦОД).

До НЦУ повинні пред'являтися вимоги забезпечення високої надійності, відмовостійкості

як до ЦОД рівня Tier 4 (за стандартами ANSI TIA – 942 та Uptime Institute BICSI 0022010), і, отже, забезпечення резервування функціональної та інженерної інфраструктур за схемою 2 (N + 1).

Одним із спеціальних методів забезпечення стійкості (сталості) інформаційно-телекомунікаційної інфраструктури, як складової частини кіберпростору, при впливі загроз є аналіз топологічної структури та ресурсів телекомунікаційних мереж і вироблення рекомендацій щодо оперативної зміни топології мереж, гнучкого використання їх ресурсів, способів і конкретних алгоритмів реалізації цих рекомендацій (у звичайних умовах) або команд НЦУ (в умовах надзвичайних ситуацій та в особливий період) центрами управління операторів усіх телекомунікаційних мереж інфраструктури.

Однією із найважливіших умов забезпечення кібербезпеки національної інформаційно-комунікаційної інфраструктури, системи оперативно-технічного управління та НЦУ є застосування у всіх складових частинах інфраструктури апаратних і програмних платформ та засобів, відповідність яких встановленим вимогам в частині інформаційної безпеки, надійності і функціональної стійкості (сталості) в умовах сучасного інформаційного протиборства, а також дотримання певних умов технологічної незалежності, підтверджені сертифікатами національних органів із підтвердження відповідності.

Для забезпечення реалізації проекту створення і подальшого функціонування СОТУ та НЦУ необхідно внести зміни до Закону «Про телекомунікації» [1], до «Порядку оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану» [7] та до «Порядку використання телекомунікаційних мереж в умовах надзвичайного та воєнного стану» [8] щодо:

– визначення конкретних категорій операторів телекомунікацій, мережі яких є об'єктами управління НЦУ і покладення зобов'язань організації каналів управління від ЦУ до НЦУ та їх подальшої експлуатації на цих операторів;

– конкретизації та формалізації взаємовідносин НЦУ та ЦУ операторів в процесі взаємодії, чіткого нормативного визначення обов'язків операторів телекомунікацій та власників телекомунікаційних мереж щодо надання до НЦУ інформації (даних) про їхні мережі, у тому числі такі, що перетинають кордон України або ресурси яких використовуються для організації транзитних мереж, визначення переліку та форматів даних, конкретизації номенклатури та вартості послуг НЦУ для операторів;

– чіткого визначення зобов`язань держави щодо збереження комерційної таємниці операторів телекомунікацій;

– чіткого визначення статусу та повноважень НЦУ в умовах НС, надзвичайного та воєнного стану, покладення на НЦУ завдання ведення бази даних усіх телекомунікаційних мереж, організації забезпечення телекомунікаційним ресурсом систем централізованого оповіщення та екстреної допомоги;

Необхідно також розробити та актуалізувати:

– Технічні вимоги до системи оперативно – технічного управління телекомунікаційними мережами України.

– Положення про НЦУ.

– Технічне завдання на створення НЦУ.

– Правила взаємоз'єднання та взаємодії ЦУ операторів телекомунікаційних мереж загального користування з НЦУ.

– Правила взаємоз'єднання та взаємодії ЦУ відомчих телекомунікаційних мереж, а також інформаційно – телекомунікаційних систем центральних органів виконавчої влади, підприємств, установ та організацій з НЦУ.

– Типовий договір на взаємодію ЦУ операторів телекомунікацій ТМЗК з НЦУ;

– Типовий договір на взаємодію ЦУ відомчих телекомунікаційних мереж, а також ІТС центральних органів виконавчої влади, підприємств, установ та організацій з НЦУ;

– Вимоги до організаційно – технічного забезпечення сталого функціонування телекомунікаційних мереж НІКІ;

– Порядок приєднання спецспоживачів до телекомунікаційної мережі спеціального призначення та взаємодії ЦУ ІТС спецспоживачів з НЦУ.

Реалізація проекту створення СОТУ та НЦУ дозволить:

– забезпечити проведення єдиної технічної політики, досягти уніфікації методів та засобів оперативно – технічного управління телекомунікаційними мережами;

– оптимізувати процеси управління, координацію аварійно – відновлювальних робіт на

телекомунікаційних мережах у зонах дій надзвичайних ситуацій;

– підвищити рівень безпеки інформації в телекомунікаційних мережах, у тому числі за рахунок скоординованих дій центрів управління телекомунікаційними мережами, що входять до складу СОТУ;

– забезпечити ефективне використання наявних ресурсів усіх без винятку телекомунікаційних мереж України як у звичайних умовах, так і в умовах надзвичайних ситуацій, надзвичайного та воєнного стану в інтересах потреб державного управління, забезпечення національної безпеки та обороноздатності держави, функціонування системи централізованого оповіщення про надзвичайні ситуації, системи екстреної допомоги та реалізації конституційних прав громадян на комунікації та можливість отримання інформації.

Сьогодні створення державного НЦУ (до речі, це реальна усталена практика таких країн, як США, Німеччина, Франція) та забезпечення можливості оперативного управління ресурсами усіх без винятку телекомунікаційних мереж – це не тільки забезпечення виконання функцій згідно Закону «Про телекомунікації», відповідних постанов уряду та указів Президента України [1,3,5,7,8], але також і вирішення завдань гарантованого забезпечення телекомунікаційним ресурсом у надзвичайних умовах **системи централізованого оповіщення**, **систем екстреної допомоги**, можливості **моніторингу стану мереж та виявлення кіберзагроз** для одного із об'єктів **«критичної інфраструктури»** держави, якою є **національна інформаційно-комунікаційна інфраструктура**, врешті – **вирішення задач кібербезпеки** та захисту телекомунікаційної транспортної складової **кіберпростору,** у тому числі за рахунок можливості оперативного управління телекомунікаційним ресурсом мереж операторів телекомунікацій (взаємне резервування, тимчасове використання ресурсу тощо).

Перелік посилань:

1. Закон України «Про телекомунікації» від 18.11.2003 №1280 – IV.
2. Концепція розвитку телекомунікацій в Україні (Редакція згідно розпорядження Кабінету Міністрів України від 27.12.2008 № 1612 – р).
3. Указ Президента України від 24.09.2014 № 744/2014 «Про рішення Ради національної безпеки і оборони України від 28 серпня 2014 року «Про невідкладні заходи щодо захисту України та зміцнення її обороноздатності».
4. Закон України «Про захист інформації в інформаційно – телекомунікаційних системах» від 05.07.1994 №81/94 – ВР.
5. Стратегія національної безпеки України. Затверджена указом Президента України від 26.05.2015 №287/2015/
6. Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затверджене постановою Кабінету Міністрів України від 03.09.2014 №411.
7. Порядок оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, затверджений постановою Кабінету Міністрів України від 29.06.2004 №812.
8. Порядок використання телекомунікаційних мереж в умовах надзвичайного та воєнного стану, затверджений постановою Кабінету Міністрів України від 13.07.2004 №920–13.
9. Порядок використання технічних засобів телекомунікацій і ресурсів телекомунікаційних мереж в інтересах Державної системи урядового зв'язку, затверджений постановою Кабінету Міністрів України від 23.08.2005 №805.
10. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно – телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.2006 №373.
11. Про проблеми вдосконалення системи захисту критичної інфраструктури в Україні. Аналітична записка./ Національний інститут стратегічних досліджень, Київ, квітень 2014.
12. Безкоровайный М. М., Татузов А. Л. Кибербезопасность – подходы к определению понятия/ Вопросы кибербезопасности №1 (2) – 2014.
13. ISO/IEC 27032 :2012 Information technology – Security techniques – Guidelines for cybersecurity.
14. Словник української мови: в 11 тт. / АН УРСР. Інститут мовознавства; за ред. І. К. Білодіда. – К.: Наукова думка, 1970—1980.– Том 10, 1979. – Стор. 269.