УДК 355.40

СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МУЛЬТИСЕРВІСНИХ МЕРЕЖ

КОНОНОВИЧ В.Г.

ОРЦ ТЗІ ВАТ "Укртелеком"

SYSTEM OF INFORMATION SEQURITY OF MULTI SERVICE NETWORKS

KONONOVICH V.

ORC TPI OC "Ukrtelecom"

ВСТУП

Задачі системи інформаційної безпеки мультисервісних мереж (МСМ) витікають з цільових функцій інформаційно-телекомунікаційних мереж і є частиною системи інформаційної безпеки останніх [1]. Телекомунікаційні мережі створюються для задоволення певних потреб людини, суспільства та держави, зокрема для: забезпечення управління державою, виробництвом та суспільством в умовах постіндустріального суспільства; забезпечення інформаційних потреб економічного та суспільного розвитку, національної безпеки та оборони держави; задоволення інформаційних потреб та інформаційного обміну громадян, суспільства, ринку та виробництва; своєчасного інформування та забезпечення інформаційного впливу на соціальні, економічні й політичні групи населення в інтересах національної безпеки.

Відповідно до виконуваних задач телекомунікаційні системи стають невід'ємними частинами інформаційних систем і надають телекомунікаційний ресурс для низки інформаційних систем, зокрема для: державної системи урядового зв'язку, мереж воєнної організації держави, системи «Електронний уряд», інформаційно-аналітичних систем міністерств та відомств; Національної системи конфіденційного зв'язку та систем електронного документообігу; систем «електронної торгівлі»; систем масової інформації, зокрема цифрового мовлення та цифрового телебачення; систем надання власне телекомунікаційних послуг. Порядок створення та функціонування системи інформаційної безпеки у телекомунікаційних мережа визначаються міжнародними та вітчизняними рекомендаціями та нормативними документами, зокрема [2, 5]. Вимоги з інформаційної безпеки включені до документів ITU-T серії Е: «Загальна експлуатація мережі, функціонування служб та людські фактори, управління мережею». Тим самим визначається місце і актуальність системи інформаційної безпеки.

Метою даної роботи є визначення засобів і заходів забезпечення ін формаційної безпеки мультисервісної мережі.

МУЛЬТИСЕРВІСНІ МЕРЕЖІ ЯК РЕСУРС ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Задачі забезпечення інформаційної безпеки повинні розподілятись за всіма елементами ІМСМ. Система інформаційної безпеки телекомунікаційних систем має бути складовою частиною системи безпеки інформаційних ресурсів державних систем. Способи розподілу розрізняють у залежності від степені критичності інформаційних систем. Зона *розмежування відповідальності захисту* може проникати на різну глибину та на різні рівні телекомунікаційної мережі (рис. 1). Інформаційні системи можуть об'єднуватись з телекомунікаційною мережею

на рівні мережі первинних каналів, рівні транспортної мережі, рівні комутації та керування процесами, на рівні надання послуг.

Найбільш критичні інформаційні системи можуть використовувати власні мережі телекомунікацій з обмеженим використанням елементів мереж загального користування та впровадженням спеціальних захищених телекомунікаційних систем. Недолік такого рішення у його високій вартості.

Рисунок 1 – Розподіл відповідальності за інформаційну безпеку між телекомунікаційними та інформаційними системами (ІС).

Сучасні економічні рішення досягаються інтеграцією інформаційних та телекомунікаційних технологій, створенням пакетних мультисервісних мереж, конвергенцією ресурсів та функцій мереж, а в майбутньому створенням полі-функціональної конвергентної мережі (*BCN – Broadband Convergence Network*). Але перевагою стає простота й надійність забезпечення задач інформаційної безпеки. Менш критичні інформаційні системи можуть використовувати транспортні телекомунікаційні мережі або на рівні стандартних мереж з комутацією пакетів та каналів. Масові інформаційні мережі використовують телекомунікаційні мережі на рівні послуг.

Розподіл задач захисту регулювався наказом ДСТСЗІ СБ України № 76 від 24 грудня 2001 р., яким було затверджено "Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах", де викладено основи організації та порядок захисту державних інформаційних ресурсів в мережі передавання даних (МПД). Згідно з чинним законодавством, створення переліку вимог, сертифікацію й атестацію систем шифрування покладено на відповідно уповноважений орган виконавчої влади. Ця діяльність регламентується "Положенням про порядок здійснення криптографічного захисту інформації в Україні". В МПД захисту підлягають державні інформаційні ресурси, інформація користувачів, яка передається мережею незалежно від способу її фізичного та логічного представлення, технологічна інформація та інформація бази даних захисту (*Security Management Information Base − SMIB*) самої комплексної системи захисту інформації (КСЗІ). При цьому, здійснення заходів щодо забезпечення *конфіденційності* державних інформаційних ресурсів та захист

від несанкціонованого доступу до них в автоматизованих системах *покладається* не на оператора, а на користувачів МПД, тобто на власників інформаційної системи.

У телекомунікаційній системі має забезпечуватись її власником цілісність, доступність інформації та інформаційних ресурсів мережі, а також живучість, сталість, надійність мереж. Такий розподіл задач обґрунтовується особливостями телекомунікаційних мереж, як найбільш критичного державного ресурсу [3]. Критичні технології – це технології, визначені у встановленому законодавством порядку як такі, що забезпечують визначальний вклад у досягнення конкретних цілей у сфері забезпечення національної безпеки, економічного та соціального розвитку держави, у вирішення найважливіших проблем реалізації пріоритетних напрямків розвитку науки і техніки [4].

Розвиток сфери телекомунікацій повинен здійснюватись з урахуванням телекомунікаційних потреб національної безпеки та оборони держави. З цією метою передбачається: телекомунікаційна підтримка функціонування спеціальних телекомунікаційних мереж; створення стійких систем телекомунікацій та систем їх управління; проведення організаційно-технічних заходів, спрямованих на забезпечення безпеки функціонування елементів телекомунікаційної інфраструктури; незалежно від форми власності, в телекомунікаційних мережах передбачається захист технічних засобів телекомунікаційних мереж та інформації, що ними передається.

ЗАВДАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МСМ

Забезпечення захисту інформації в телекомунікаційних мережах вимагає виконання таких *завдань*: формування і поступове впровадження законодавчої та нормативно-правової бази технічного та криптографічного захисту інформації, гармонізованої з європейськими та міжнародними стандартами; розроблення сучасних методів захисту інформації для забезпечення комплексного захисту інформації в телекомунікаційних мережах; створення системи легального перехоплення інформації з телекомунікаційних мереж у випадках, передбачених законодавством України; створення державного координаційного центру з питань безпеки в інформаційно-телекомунікаційних мережах загального користування, сприяння створенню державних та недержавних центрів компетенції та реагування на інциденти в телекомунікаційних мережах.

Захист інформації передбачається у стратегічно важливих системах оперативно-технічного управління телекомунікаційними мережами та системі управління транспортними магістральними телекомунікаційними мережами. Крім того, має забезпечуватись захист від несанкціонованого втручання в режим функціонування обладнання мереж, а також вирішення проблеми «непрозорості» впроваджуваних в телекомунікаційних мережах іноземних технічних засобів, програмних продуктів і технологій.

Нові проблеми інформаційної безпеки є порівняно складними і мають охоплювати декілька рівнів та сфер діяльності: мережне адміністрування, фізичну безпеку, моніторинг, програмне забезпечення телекомунікацій, інструменти забезпечення безпеки, аудит безпеки. Міжнародні рекомендації визначають перелік функціональних вимог, послуги, які ці вимоги забезпечують та особливості реалізації послуг безпеки за рівнями моделі взаємодії відкритих систем. Рекомендацією ITU-T E.408 визначені функціональні класи (*Functional Classes*, *FC*), за якими можна класифікувати заходи безпеки.

Розглянемо реалізацію інформаційної безпеки в різних елементах МСМ.

ІЄРАРХІЯ ПІДСИСТЕМ У ЗАГАЛЬНІЙ СИСТЕМІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МСМ

Загальна проблема безпеки ресурсів МСМ повинна вирішуватись комплексно на всіх етапах і стадіях життєвого циклу: технічного завдання, проектування, створення системи захисту інформації (СЗІ) та системи фізичного захисту (СФЗ), їх експлуатації та утилізації. Згідно з Концепцією розвитку телекомунікацій в Україні до 2010 р. [6] розвиток МСМ повинен здійснюватись з урахуванням потреб національної безпеки та оборони держави. З цією метою передбачається телекомунікаційна підтримка функціонування спеціальних телекомунікаційних мереж, проведення організаційно-технічних заходів, спрямованих на забезпечення безпеки функціонування всіх елементів телекомунікаційної інфраструктури України, особливий порядок вирішення питань оперативно-технічного управління телекомунікаційними мережами у частині національної безпеки та оборони держави, забезпечення порядку використання засобів, споруд і мереж в умовах надзвичайних ситуацій та воєнного стану.

Одними з найбільш вразливих та незахищених елементів телекомунікаційних мереж є фізичні елементи – лінії, канали, засоби комутації тощо. Без їх фізичної безпеки неможливо реалізувати інформаційну та інші види безпеки. Тому проектування відповідних заходів та засобів щодо захисту інформації та фізичної безпеки МСМ є важливою задачею створення комплексної системи безпеки.

Вітчизняні нормативні документи визначають вимоги до проектування, проектної документації та порядку проведення робіт щодо технічного захисту інформації (ТЗІ) [7, 8], а також комплекс документів щодо проектування, технічної експлуатації та охорони споруд, лінійно-кабельних систем (МСМ), зокрема [9...11]. Задачі безпеки повинні розподілятись за всіма елементами МСМ.

Фізична безпека – це фізична захищеність ресурсів від навмисних та випадкових загроз. *Система фізичного захисту* (СФЗ) – сукупність правових норм, організаційних заходів та інженерно-технічних засобів, спрямованих на фізичний захист життєво-важливих інтересів та ресурсів об’єкта від загроз фізичній безпеці. *Безпека інформації* [12] – стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації. *Комплексна система захисту інформації* (КСЗІ) – сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в системі.

Категорія *комплексна безпека* має дещо ширший зміст ніж *фізична безпека* та *інформаційна безпека*. Тому термін *комплексна система безпеки (КСБ) МСМ* означає організаційно-технічну систему, що складається з алгоритмічно об’єднаних та взаємопов’язаних підсистем (фізичної, інформаційної безпеки тощо), які забезпечують захист МСМ від загроз різного походження (рис. 2).

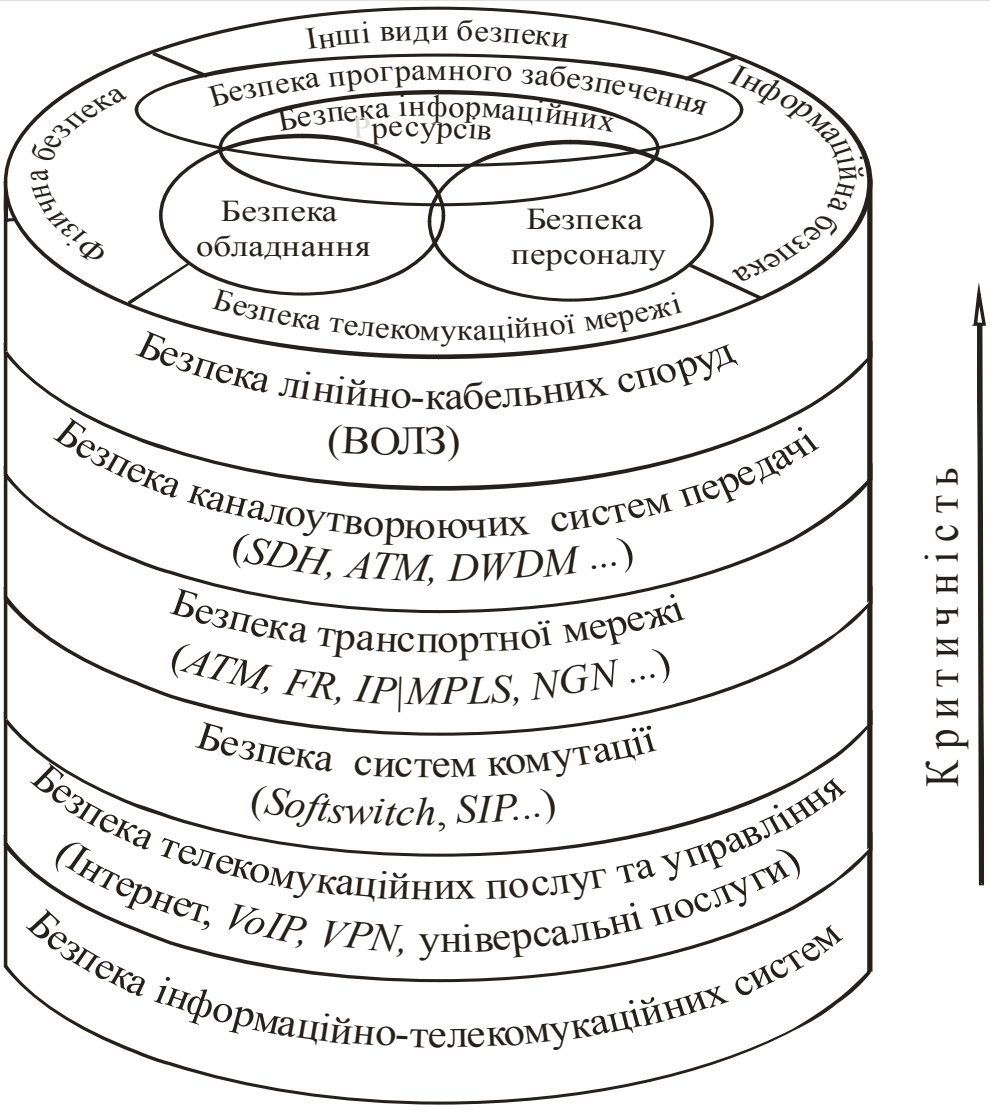

Рисунок. 2 – Ієрархія підсистем в комплексній системі безпеки МСМ

При проектуванні МСМ, відповідні СЗІ та СФЗ є підсистемами по відношенню до комплексної системи безпеки ТМ в цілому як багаторівневого ієрархічного об'єкта захисту. Розподіл завдань СЗІ та СФЗ розрізняється у залежності від ступеня критичності. Зона розмежування відповідальності може проникати на різну глибину та на різні рівні МСМ. Підсистеми безпеки повинні взаємодіяти і функціонувати у МСМ на усіх рівнях, починаючи з рівня МСМ, каналоутворюючих систем передачі, транспортної мережі, комутації, керування процесами та надання послуг. Відповідно мають створюватись *підсистеми:* безпеки лінійно-кабельних споруд; безпеки каналоутворюючих систем передачі; безпеки транспортної мережі; безпеки систем комутації; безпеки послуг; безпеки інформаційних систем. Згідно [13] захисту в МСМ підлягають усі її складові елементи: лінії, канали, системи передавання, обладнання, програмне забезпечення, інформація та персонал. Кожна з підсистем безпеки, у свою чергу, повинна органічно включати у себе: безпеку інформаційних ресурсів; безпеку програмного забезпечення; безпеку обладнання; безпеку персоналу.

При реалізації проектних процедур щодо створення заходів безпеки МСМ необхідно враховувати їхні особливості: структурну складність, глобально-розподілений характер мереж, велику довжину ліній зв'язку, які знаходяться на неконтрольованій території, тощо. В процесі проектування, створення та експлуатації необхідно узгоджувати методи забезпечення ІБ різних компонентів.

Перед тим, як проектувати СЗІ та СФЗ, потрібно визначити взаємозв'язок та взаємозалежність задач, які будуть реалізовані за допомогою цих систем. Задачі забезпечення ІБ пе-

ресікаються з: задачами технологічного управління МСМ; задачами керування якістю функціонування МСМ, де захищеність МСМ є складовою частиною оцінки якості функціонування МСМ; задачами технічної експлуатації та фізичної безпеки МСМ в частині забезпечення вимог до збереження мінімального набору критично важливих функцій, до живучості МСМ, до запасу стійкості при дії дестабілізуючих факторів зовнішнього середовища (рис. 3). Гомеостаз МСМ підтримується забезпеченням цілісності МСМ, їх живучості та пропускної здатності.

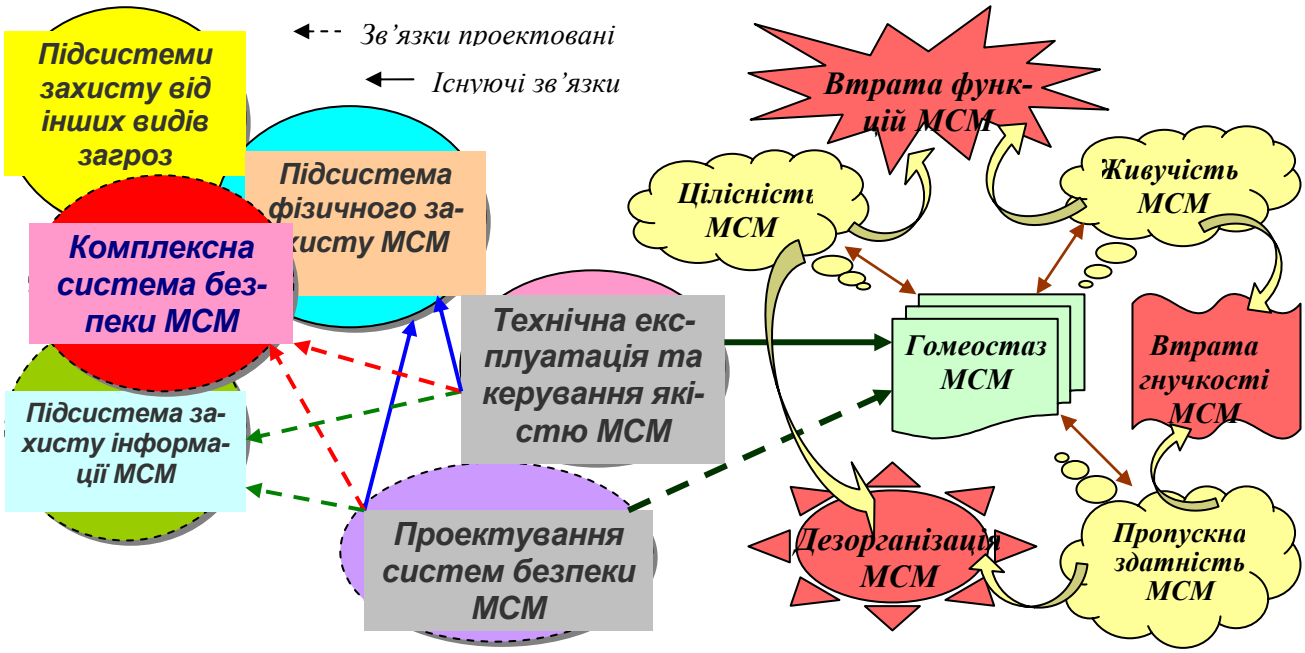

Рисунок 3 – Взаємозв'язки завдань щодо СЗІ та СФЗ МСМ
(рисунок розробив та виконав аспірант Гладиш С.В.)

На різних стадіях життєвого циклу МСМ, в різних етапах проектування, створення та експлуатації формуються показники захищеності, гарантій, якості та взаємопов'язані з ними техніко-економічні показники.

Мережецентрична модель постановки та вирішення проблеми ІБ МСМ витікає з підвищених вимог до живучості МСМ, які характеризуються високим ступенем розподілу ресурсів (обслуговуванням, логікою, алгоритмами, програмним та апаратним забезпеченням). Для повноцінної роботи та збереження мінімального набору критично важливих функцій МСМ повинні мати певний запас стійкості до дестабілізуючих факторів зовнішнього середовища.

Порушення цілісності МСМ на фоні зниження активності їх елементів тягне за собою дезорганізацію управління, одночасне зниження активності елементів та їх живучості – втрату гнучкості, а зниження живучості і порушення цілісності МСМ – втрату найважливіших функцій.

Поняття *живучості МСМ* передбачає їх спроможність своєчасно виконувати свої функції в умовах дії дестабілізуючих факторів (фізичне руйнування, часткова втрата ресурсів, відмови та збої елементів, несанкціоноване втручання в контур управління). При цьому *технічна надійність*, яка проявляється як здатність МСМ працювати на протязі заданого проміжку часу в штатній системі без відмов, визначає мінімальний поріг стійкості МСМ, за яким без наявності відновлення втрачених елементів та функції може настати повна зупинка функціонування. Живучість МСМ має визначальну роль для ІБ МСМ в цілому.

В системі технічної експлуатації та СФЗ МСМ вироблено розвинуті засоби підтримки заданого рівня достовірності передавання даних і надійності функціонування МСМ та інших показників якості передавання інформації і такі показники споріднені показникам ІБ МСМ.

ПОРЯДОК ВИКОНАННЯ РОБІТ ІЗ ЗАХИСТУ ІНФОРМАЦІЇ У МСМ

Сучасні телекомунікаційні мережі класифікуються як надскладна ієрархічна система. Телекомунікаційну мережу складає велика кількість об'єктів типу вузлів комутації, з'єднаних між собою каналами або сегментами магістралі, які також треба вважати об'єктами, де обробляється, тимчасово зберігається та передається інформація. У такій системі важко точно застосувати всі етапи існуючого порядку виконання робіт з технічного захисту інформації (ТЗІ) та процедури створення КСЗІ, які розраховані на захист об'єкта інформаційної діяльності за типом «кругової оборони». До існуючого порядку розробки доцільно додати етапи й процедури, які б враховували ієрархічний та розподілений характер телекомунікаційної мережі, а також інтеграцію інформаційних та телекомунікаційних мереж.

Формально можна розбити порядок виконання робіт на три загальних цикли, кожен з яких розділявся б на етапи у відповідності з вимогами ДСТУ 3396.0-96, а етапи виконувались би за стадіями, в порядку, що передбачається ДСТУ 3396.1-96. Цикли виконання робіт можуть бути такими:

1) загальний цикл створення технічного завдання (ТЗ) та плану захисту телекомунікаційної мережі в цілому як складової інформаційно-телекомунікаційної системи. У цьому циклі проводиться обстеження телекомунікаційної мережі та інформаційної системи, в інтересах якої функціонує телекомунікаційна мережа, аналізуються загрози інформаційним ресурсам, визначаються вимоги до системи захисту інформації саме в телекомунікаційній мережі, обирається мережний функціональний профіль захисту, розробляються засоби реалізації комплексної системи захисту державних інформаційних ресурсів (КСЗІР) в телекомунікаційній мережі;

2) загальний цикл декомпозиції телекомунікаційної мережі на взаємопов'язані об'єкти інформаційної діяльності (ОІД), раціональної інтерпретації загальних вимог до захищеності інформації за вимогами до системи захисту інформації в ОІД, розробка оптимального розподілу засобів захисту за об'єктами ОІД;

3) загальний цикл виконання робіт з ТЗІ на кожному з телекомунікаційних ОІД відповідно до вимог ДСТУ 3396.0-96 та ДСТУ 3396.1-96.

Але недоліком такого розподілу робіт є те, що не враховується ієрархічний характер телекомунікаційних мереж та нерівномірний розподіл механізмів захисту за рівнями ієрархії. Це стосується, перш за все, штатних засобів захисту, які вбудовуються в кожні пристрої, системи, технології, які у сукупності утворюють телекомунікаційну мережу.

Модель взаємодії відкритих систем передбачала сім рівнів ієрархії: фізичний, канальний, мережний, транспортний, сеансовий, представницький та прикладний. Розвиток мікроелектроніки, мініатюризація пристроїв, програмна й мікропрограмна реалізація функцій та, навпаки, апаратна реалізація типових програмно виконуваних функцій привели до інкапсуляції деяких рівнів.

На сьогодні в телекомунікаційних мережах виділяють чотири-п'ять ієрархічних рівнів: - абонентського доступу (інкапсулює фізичний та канальний рівні); комутації (мережний рівень); програмного управління (рівень транспорту); управління мережею та створення й надання послуг (інкапсулює сеансовий, представницький та прикладний рівні).

Тому у другому та третьому загальних циклах виконання робіт з ТЗІ мають додаватись наступні етапи:

- аналіз та ініціалізація штатних засобів захисту, вбудованих в елементи телекомунікаційної мережі на її ієрархічних рівнях;

- реалізація організаційних, організаційно-технічних та програмно-технічних заходів, які доповнюють штатні засоби захисту до повної КСЗІР згідно обраного мережного функціонального профілю захисту;

- розробка порядку й засобів взаємодії механізмів захисту на кожному з ієрархічних рівнів із засобами управління та контролю функціонування КСЗІР;

- прив'язка ієрархії засобів захисту інформації до конкретних фізично-географічних ОІД.

Діючі нормативно-правові документи сфери захисту інформації рекомендують аналізувати рівень захищеності інформації, виявляти нові загрози й ризики інформаційної безпеки, розробляти ТЗ на вдосконалення й модернізацію КСЗІР повторюючи увесь цикл виконання робіт.

На цьому періоді має значення розвиток штатних засобів захисту, що має призводити до більш ефективного розподілу задач захисту між штатними та додатковими механізмами захисту.

ВИСНОВКИ

Обґрунтовано основні положення системи інформаційної безпека системи цифрового мовлення, яка невід'ємно інтегрована в систему інформаційної безпеки мультисервісних мереж. Але в цілому проблема захисту інформації в цих мережах потребує свого вдосконалення.

Література

1. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено постановою Кабінету Міністрів України від 29 березня 2006 р. № 373. – 9 с.

2. НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. НД ТЗІ 1.1-001-99.

3. Леваков А. Анатомия информационной безопасности США. Jet Info online #6(109), 2002. Електронний ресурс http://daily.sec.ru/dailypblshow.cfm?rid=9&pid=5503&pos=13&stp=10. – 74 с.

4. Питання технічного захисту інформації в Україні. Указ президента України (проект). – 8 с.

5. Рекомендация МСЭ-Т Е.408 Требования к безопасности сетей электросвязи. – 30 с.

6. Концепція розвитку телекомунікацій в Україні до 2010 року.

7. ДБН А.2.2-2-96. Державні будівельні норми України. Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва. - Держкоммістобудування України. – Київ. – 1996.

8. ДСТУ 3396.1-96. Технічний захист інформації. Порядок проведення робіт.

9. ВСН-116-87. Инструкция по проектированию линейно-кабельных сооружений связи.

10. КНД 45-112-1999. Правила технічної експлуатації первинної мережі ЄНСЗ. Частина 3. Правила технічної експлуатації лінійних споруд первинної мережі ЄНСЗ.

11. Правила охорони ліній зв'язку. Затверджені постановою Кабінету Міністрів України від 29.01.1996 р. №135.

12. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

13. ITU-T Recommendation X.805. Security architecture for system providing end-to-end communications. – Geneva: 2003. – 28 с.

14. Закон України «Про телекомунікації» // Відомості Верховної Ради (ВВР), в редакції Закону 2007, N 13, ст.132.

15. ДСТУ 3396.0-96. Технічний захист інформації. Основні положення. – 13 с.

16. ДСТУ 3396.1-96. Технічний захист інформації. Порядок проведення робіт. – 17 с.