УДК 004.056:621.391
DOI: 10.31673/2412-9070.2022.040308

Л. Н. БЕРКМАН[1], доктор техн. наук, професор;
О. Г. ВАРФОЛОМЕЄВА[1], канд. техн. наук, доцент;
Г. Ф. КОЛЧЕНКО[2], канд. техн. наук, доцент;
А. Г. ЗАХАРЖЕВСЬКИЙ[1], канд. техн. наук;
Н. Л. ПЕРЕПЕЛИЦЯ[1], ст. викладач,
[1] Державний університет телекомунікацій, Київ
[2] ТОВ Випробувальний центр «ОМЕГА», Київ

ІНТЕГРАЦІЯ ПОСЛУГ БЕЗПЕКИ В АРХІТЕКТУРУ СИСТЕМИ КЕРУВАННЯ ТЕЛЕКОМУНІКАЦІЯМИ

Розглянуто основні завдання щодо забезпечення безпеки системи керування телекомунікаційними мережами України. Проаналізовано стандарти та іншу нормативну документацію з питань інформаційної безпеки телекомунікацій і систем керування ними. Особливу увагу приділено питанням керування безпекою як складової функціональної архітектури системи керування телекомунікаціями згідно з концепцією побудови мережі керування телекомунікаціями TMN. Визначено особливості впровадження послуг безпеки для кінцевих або проміжних вузлів телекомунікаційних мереж. Проведено порівняння ієрархічної моделі надання послуг безпеки з моделлю взаємодії відкритих систем OSI. Запропоновано практичну модель організації безпеки системи керування телекомунікаційними мережами. Досліджено основні переваги та недоліки інтеграції послуг безпеки на нижніх та верхніх протокольних рівнях. Інтеграція послуг та механізмів безпеки в архітектуру телекомунікаційного зв'язку визначається двома основними міркуваннями: в яких вузлах мають бути реалізовані послуги безпеки та на якому рівні має бути здійснено кожну послугу. Оскільки існує низка аргументів на користь та проти кожного з цих рівнів, єдиного правильного розв'язку цієї проблеми не існує. Доцільно знайти оптимальне вирішення, залежно від конкретної задачі безпеки.

Ключові слова: мережа; система керування; безпека; послуга; кінцева система; проміжна система.

Вступ

Постановка проблеми та аналіз останніх досліджень і публікацій. Основою політики забезпечення безпеки системи керування телекомунікаційними мережами України є законодавчі акти і нормативно-технічні документи галузі, рекомендації як вітчизняних, так і міжнародних органів стандартизації тощо [1; 2].

Серед важливих завдань є такі:

- забезпечення технологічної незалежності України стосовно систем керування та обладнання телекомунікацій;
- створення систем і засобів запобігання несанкціонованому доступу до інформації, а також тих, що заважають чи руйнують вплив втручання;
- виявлення програм, які спричинюють порушення передавання інформації;
- застосування криптографії, контроль виконання спеціальних вимог щодо захисту інформації;
- сертифікація систем керування.

Нині на питаннях стандартизації керування телекомунікаційними мережами зосереджені як офіційні організації в міжнародній системі стандартизації: ISO (*International Standard Organization*), IEC (*International Electrotechnical Commission*), ITU (*International Telecommunication Union*), так і промислові консорціуми та професійні організації, до яких належать IETF (*Internet Engineering Task Force* — робоча група інженерів Internet), IEEE (*Institute of Electrical and Electronic Engineers* — Інститут інженерів з електротехніки та електроніки, OMG (*Object Management Group* — Група об'єктно-орієнтованого керування), *TeleManagement Forum* — глобальний консорціум операторів та постачальників послуг та багато інших, включно з усіма достатньо великими постачальниками телекомунікаційного обладнання.

Загальновизнаним принципом керування є концепція TMN (*Telecommunications Management Network* — мережа керування телекомунікаціями), логічна багаторівнева модель якої передбачає рівні керування елементами мережі, мережею, послугами, бізнесом. TMN — це по суті міжнародний стандарт, що визначає технологію побудови систем керування телекомунікаційними мережами та визначає всі аспекти їх функціонування [1; 2].

Традиційно опис TMN починається з розгляду трьох її архітектур: функціональної, інформаційної та фізичної.

Системи керування є автоматизованими системами, що реалізують завдання керування в п'яти функціональних сферах, визначених моделлю OSI та концепцією TMN, а саме:

- керування продуктивністю мережі;
- керування аварійними ситуаціями на мережі;
- керування (ре-)конфігурацією мережі;
- керування розрахунками (білінг);
- керування безпекою мережі.

Однією з цих функціональних напрямів є сфера керування безпекою. Вирішення завдання безпеки автоматизованих систем керування не є можливим у відриві і без взаємодії з безпекою керованих нею мереж та обладнання телекомунікацій.

Аналіз науково-технічної літератури показує, що проблемам дослідження побудови ефективних систем керування мережами та питанням безпеки мереж присвячено велику кількість наукових праць вітчизняних та зарубіжних вчених, таких як Афанасьєв В. В., Лазарєв В. Г., Нейман В. І., Нетес В. А., Зайцев Г. Ф., Беркман Л. Н., Поповський В. В., Daniel A. Menascé та ін. [2-7].

Основна частина

Питання, що постають через інтеграцію послуг безпеки в телекомунікаційні системи, можна розподілити на дві категорії. Розглядаючи орієнтацію за горизонталлю (рис. 1, *а*), потрібно визначити, які послуги безпеки мають бути реалізовані в окремих частинах мережі телекомунікацій. Поодинокі послуги безпеки можуть забезпечуватися в кінцевих або проміжних вузлах (системах). Щодо інтеграції в проміжні системи, то може бути проведено подальшу диференціацію стосовно того, які послуги безпеки мають бути вбудовані в проміжні системи, наприклад, чи повинні ці послуги інтегруватися тільки в «граничні вузли» мережі або по всій мережі загалом [7; 8].

Перший підхід передбачає, що послуги безпеки здебільшого мають забезпечуватися в кінцевих системах, оскільки лише тут користувачі можуть повністю контролювати їх і бути впевненими, що їх дані матимуть необхідний захист. Проте потрібно брати до уваги, що контроль із боку користувачів за послугами безпеки фактично може стати джерелом відсутності безпеки [9].

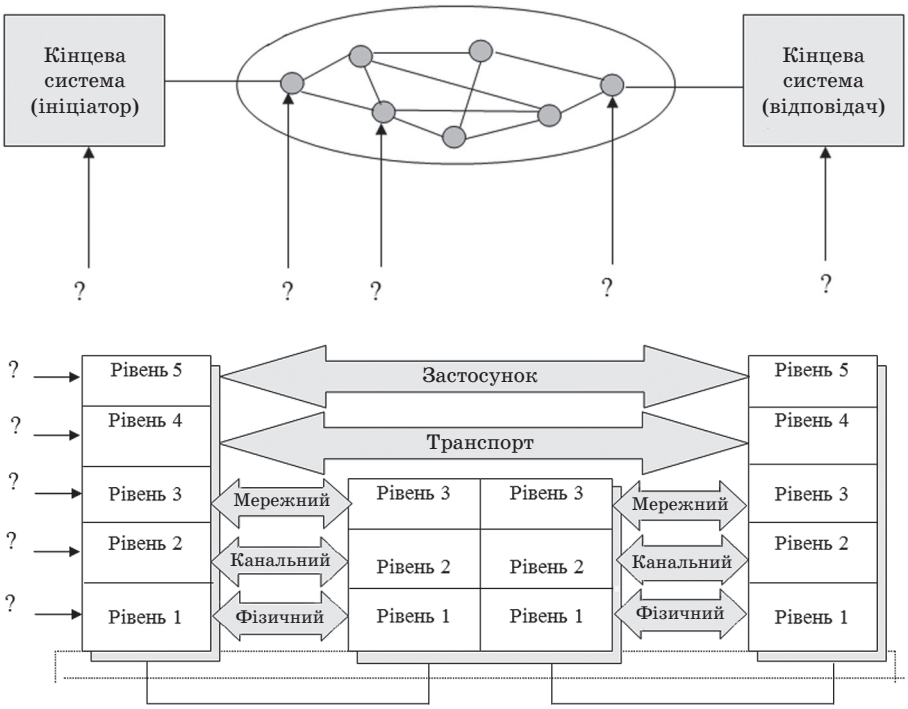

Рис. 1. Базові вирішення щодо побудови безпеки мережі телекомунікацій: *а* — орієнтація за горизонталлю; *б* — орієнтація за вертикаллю

Водночас, розглядаючи орієнтацію за вертикаллю, необхідно визначити рівні, в які мають інтегруватися певні безпекові послуги (рис. 1, *б*). Тут також можна прийняти одну чи іншу екстремальну позицію, стверджуючи, що послуги безпеки переважно мають забезпечуватися на прикладному рівні, оскільки лише програми мають повні знання щодо семантики, а отже, сприйнятливості потенційно захищених даних. Так само легко довести, що загалом усі дані, включно з протокольною інформацією

інших рівнів, потребують однакового захисту, аби досягти найкращої безпеки. Це означало б, що послуги безпеки мають бути поширені максимально на всі протокольні рівні. Навіть якщо обидва аргументи є обґрунтованими, аспекти реальних мереж торкаються настільки багатьох рівнів, що питання безпеки не може бути розв'язане задовільно, використовуючи «заготовлені вирішення».

Очевидно, що основною метою організації мереж зв'язку та розподілених систем є надання деяких застосунків користувачам цих систем. Ґрунтуючись на цих міркуваннях, наведемо можливий варіант практичної моделі системи керування мережами, організованими в безпечну структуру, зображений на рис. 2.

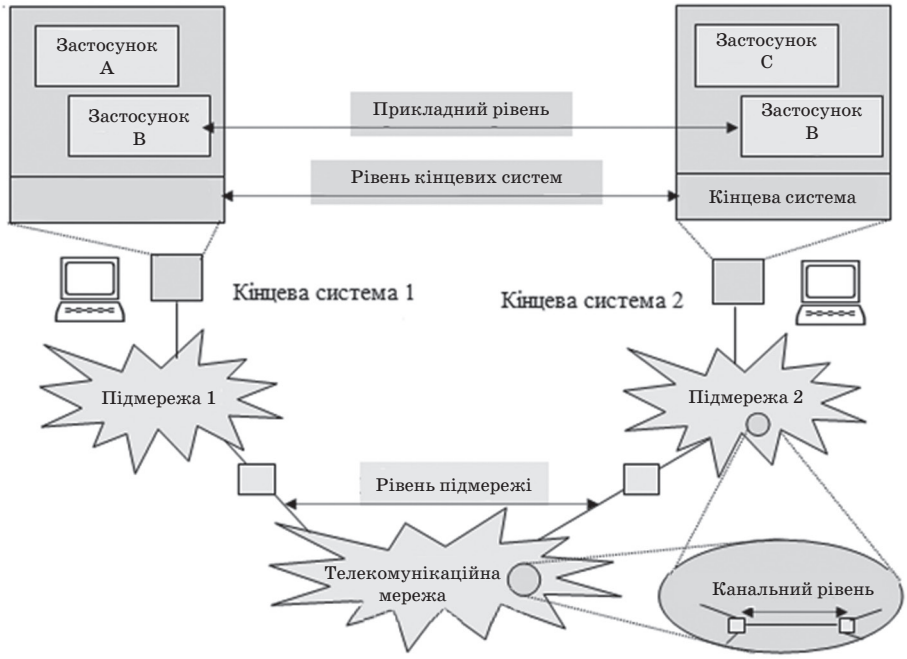

Рис. 2. Практична модель організації безпеки системи керування мережами

У моделі зроблено розмежування між чотирма основними рівнями, в яких діють певні вимоги до безпеки:

1. Вимоги, які мають бути визначені на прикладному рівні, стосуються певних застосунків та їх виконання має забезпечуватись безпосередньо самими застосунками. Програмами є програмні об'єкти, які розв'язують певні завдання, такі як електронна пошта, послуги WWW, оброблення слів, запам'ятовування даних тощо.

2. Рівень кінцевої системи виробляє вимоги та визначає засоби реалізації для кінцевих систем. Як кінцеві системи можуть розглядатися пристрої, починаючи з персональних комп'ютерів до серверів і мейнфреймів. Політика безпеки кінцевої системи так чи інакше визначається об'єктом, який відповідає за вироблення політики для всієї системи загалом.

3. На рівні підмережі політика безпеки для підмереж зазвичай визначається однаково для всіх систем у підмережі. Основна ідея полягає в гарантуванні того, що зв'язок між конкретними підмережами в потенційно ненадійних мережах (наприклад, інтернет) є безпечним.

4. Канальний рівень стосується безпеки між окремими вузлами мережі зв'язку, які пов'язані безпосередньо з фізичним середовищем.

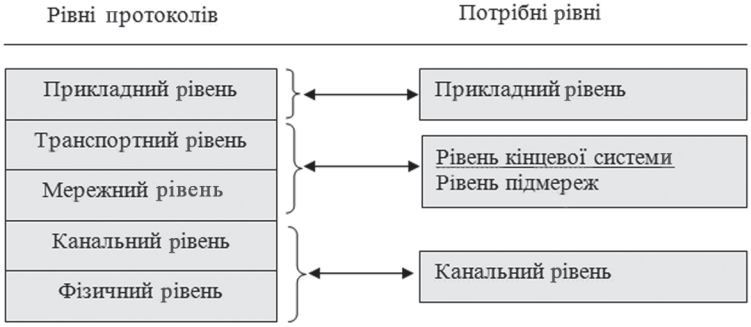

Рис. 3. Зіставлення протокольних рівнів із рівнями безпеки

Порівнюючи рівневу модель для систем зв'язку, які широко застосовуються сьогодні, бачимо, що рівні, зображені на рис. 2, не є ідентичними з протокольними рівнями. Як випливає з рис. 3, наведеному на с. 5, єдина безпосередня асоціація існує між прикладними рівнями, оскільки послуги безпеки, що забезпечуються на цьому рівні, реалізуються в прикладному шарі або безпосередньо в самому застосунку.

Заходи безпеки для задоволення вимог рівнів кінцевої системи та підмережі можуть бути реалізовані транспортним або мережним рівнем. Так само вимоги на канальному рівні можуть реалізуватися як на рівні каналу даних, так і на фізичному рівні.

Далі розглянемо загальні міркування, на які потрібно зважати в процесі ухвалення рішень щодо розміщення послуг безпеки.

• ***Змішування різних потоків даних***. У результаті мультиплексування в системах зв'язку існує тенденція в нижніх рівнях або шарах, коли потоки даних із різних джерел і приймачів із різних застосунків існують як змішані потоки даних. Переважно послуги безпеки для певних рівнів обробляють трафік даних цього рівня. Однак це може призвести до неадекватного контролю механізмів безпеки, які використовуються для деяких даних. Наприклад, якщо політика безпеки вимагає, щоб трафік оброблявся у спеціальний спосіб для певних програм або користувачів, це було б краще реалізувати на вищому рівні.

• ***Знання маршрутизації***. Зазвичай нижні рівні мають більше знань про характеристики безпеки різних трактів зв'язку (наприклад, маршрутів чи каналів). У тих середовищах, в яких ці характеристики значно відрізняються одна від одної, розміщення координованих механізмів захисту в нижніх рівнях може давати значні переваги щодо ефективності та продуктивності. Тракти зв'язку, які наражаються на більший ризик (наприклад, безпроводові канали або тракти, що перетинають мережі загального користування між двома взаємно пов'язаними локальними мережами), можуть бути захищені особливим чином, без тих частин мережі, які підпадають під менший ризик, а це потребує додаткових засобів захисту.

• ***Кількість захищених точок***. Якщо послуги безпеки реалізовано на прикладному рівні, вони мають виконуватись у кожній програмі та в кожній кінцевій системі. Аналогічна ситуація виникає з реалізацією на канальному рівні, оскільки всі кінцеві точки мають бути захищені від менш довірчих маршрутів зв'язку.

• ***Захист протокольної інформації***. Взагалі заходи безпеки високих протокольних рівнів не можуть захистити протокольні поля рівнів, розміщених нижче за них. Цей момент не слід ігнорувати ще й тому, що не тільки дані користувача мають бути захищені, а і вся мережна інфраструктура загалом.

• ***Зв'язок між джерелом та приймачем***. Деякі послуги безпеки, такі як автентифікація джерела даних та безвідмовність, ґрунтуються на взаємовідносинах між даними та їх відправником та, частково, одержувачем. Це ставлення може бути більш ефективним на високих рівнях, зокрема на прикладному рівні.

На додаток до наведених загальних міркувань питання щодо рівнів також допомагають отримати виграшні аргументи на користь визначення найбільш доцільного розміщення окремих послуг безпеки для конкретної конфігурації мережі.

Іноді прикладний рівень є єдиним зручним рівнем, який може забезпечити послуги безпеки. Послуги безпеки, характерні для прикладного рівня, зокрема контроль доступу до розподіленої файлової служби, можуть бути реалізовані лише на прикладному рівні. Також можливо буде потрібно, аби послуги безпеки були ефективними після деяких прикладних шлюзів. За приклад можна взяти конфіденційність та автентифікацію джерела даних для електронної пошти, яка зазвичай транспортується кількома шлюзами електронної пошти, перш ніж буде доставлена до місця призначення. Крім того, семантика деяких елементів даних може потребувати особливу безпеку. Так, для послуг безпеки в разі неможливості відмовитися від факту отримання або відправлення повідомлення достатні знання семантики деяких елементів даних існують лише на прикладному рівні. І, нарешті, програмісти застосунків іноді не мають іншого вибору, окрім як інтегрувати деякі послуги безпеки в прикладний рівень, оскільки вони не можуть впливати на механізми безпеки на нижніх рівнях [4-6].

Рівень кінцевої системи для впровадження послуг безпеки використовується за таких умов:

• якщо кінцеві системи характеризуються як довірчі, а мережа між ними не є довірчою;

• коли послуги можуть реалізовуватися прозоро щодо програми;

• у разі, що конфігурація та керування послугами безпеки може передаватися спеціально призначеному адміністратору системи.

Рівень підмережі не слід плутати з рівнем кінцевої системи, навіть якщо послуги безпеки реалізовані в тому самому протокольному шарі. Коли заходи безпеки здійснюються лише на рівні підмережі, усім кінцевим системам цієї підмережі забезпечується однаковий захист. Передбачається, що підмережа,

безпосередньо з'єднана з кінцевою системою, є такою ж довірчою, як і сама кінцева система. Підставою для цього твердження слугує те, що кінцева система і підмережа розташовані в одному місці та конфігуруються і керуються одним і тим самим персоналом. Перевагою реалізації заходів безпеки на рівні підмережі є те, що зазвичай кількість шлюзів підмереж набагато менша, ніж кінцевих систем, і тому заходи безпеки потрібні для меншої кількості систем.

Канальний рівень для реалізації заходів безпеки має сенс використовувати, коли існує мало ненадійних каналів зв'язку. А отже, з економічного погляду легше й ефективніше захищати ті канали, які характеризуються як небезпечні. Залежно від використовуваної технології рівень каналу дає змогу також застосовувати такі механізми захисту, як передавання широкого спектра або комутацію, котра залежить від ключа (стрибкоподібної перебудови частоти). Крім того, канальний рівень є єдиним рівнем, в якому може бути ефективно реалізовано захист несанкціонованого доступу до потоку навантаження [6-8].

Ще одним аспектом щодо заходів безпеки є потенційна взаємодія з користувачем, яка не може бути інтегрована в поточну модель, оскільки користувачі перебувають поза системою зв'язку. Наприклад, автентифікація потребує взаємодії з користувачем. Існують такі альтернативні методи.

• ***Локальна автентифікація***. Користувачі автентифікують себе в кінцевій системі, яка, зі свого боку, автентифікує себе у віддаленій системі, одночасно зазначаючи ім'я користувача. Згідно з цим варіантом система має бути впевнена, що локальна кінцева система правильно виконує верифікацію автентифікації.

• ***Використання певних протокольних елементів на прикладному рівні***. Користувач надсилає до локальної системи деяку автентифікаційну інформацію, котру локальна система направляє у віддалену систему, застосовуючи певні правила. Тобто віддалена система сама верифікує автентифікацію.

• ***Комбінація цих методів***. У цьому разі об'єднується локальна та віддалена автентифікації, оскільки вони використовують ці обидва види автентифікації.

Розглянемо основні переваги інтеграції послуг безпеки на нижніх протокольних рівнях.

1. Інфраструктура мережі сама собою має бути захищена в такий спосіб, щоб бути здатною гарантувати свою доступність і коректне функціонування, зокрема й точне використання послуг, що підлягають контролю.

2. Засоби безпеки, реалізовані в мережних елементах, зазвичай важче піддаються атакам користувачів, ніж ті, що розміщені в кінцевих системах. Зокрема тоді, коли їх реалізації потрібне апаратне підтримання.

3. Основні заходи безпеки можуть бути здійснені на нижніх рівнях для всіх застосунків і не повинні інтегруватися в кожний окремий застосунок.

4. Потоки даних, до яких висуваються особливі вимоги стосовно якості послуг передавання (мінімальна затримка, флуктуація затримки тощо), можуть дістати додаткові можливості під час інтеграції в нижні протокольні рівні, де легше поєднувати планування якості послуг системи з плануванням криптографічних операцій. Візьмемо приклад, в якому множинні потоки даних із різними вимогами та характеристиками трафіку (скажімо, передавання мови та перенесення файлу) закодовані апаратним криптографічним модулем, а потім передані. І тут планування якості послуги обох операцій може інтегруватися ефективніше, якщо шифрування виконано до передавання в адаптері зв'язку.

5. Завдяки поліпшеним можливостям інтеграції апаратного підтримання безпосередньо до адаптера зв'язку, криптографічні операції можуть виконуватися більш ефективно, коли інтеграція відбувається на нижніх протокольних рівнях. Отже, хоча застосунок загалом може використовувати спеціальне апаратне розширення для проведення ефективних обчислень криптографічних операцій, зумовлюючи відповідні функції, слід зважати на те, що це призводить до додаткового транспортування даних системною шиною, неминуче впливаючи на якість роботи.

Крім визначення рівня, в якому мають реалізовуватися послуги безпеки, важливо також встановити, чи повинні деякі послуги безпеки інтегруватися в кінцеві або в проміжні системи.

Стосовно інтеграції в кінцеві системи, слід зазначити, що це може відбуватися лише на рівні застосунків і навіть лише на рівні кінцевої системи. За деяких обставин є сенс упроваджувати безпеку і в канальний рівень — наприклад, якщо використовується модем для з'єднання кінцевої системи з виділеною системою. Це може бути випадок, коли для комутаційної системи є віддалений доступ.

Інтеграція в проміжні системи може здійснюватися на всіх чотирьох рівнях. Однак, залежно від рівня, простежуються різні цілі. Якщо безпека інтегрується в застосунках або на рівні кінцевої системи, вона прагне захисту інтерфейсів керування проміжних систем, а не даних користувача.

Залежно від передбачуваних цілей безпеки може мати сенс інтеграція або в кінцеві системи, або в проміжні. Насправді часто зустрічаються обидва види інтеграції.

Висновки

Отже, проста прагматична модель для захищених систем, які різняться чотирма різними рівнями з різними вимогами до безпеки та в яких можуть бути вжиті заходи щодо безпеки, може бути використана для проєктування.

Інтеграція послуг та механізмів безпеки в архітектуру телекомунікаційного зв'язку визначається такими основними міркуваннями:

- в яких вузлах мають бути реалізовані послуги безпеки;
- на якому рівні має бути реалізовано кожну послугу.

Оскільки існує низка аргументів на користь та проти кожного з цих рівнів, єдиного правильного вирішення цієї проблеми не існує. Доцільно знайти оптимальний розв'язок, залежно від конкретної задачі стосовно безпеки.

Заходи щодо безпеки, які можуть бути вжиті, часто є компромісом із погляду досягнення безпеки, якісних показників, гнучкості тощо.

Список використаної літератури

1. ***ITU-T*** *Recommendation M.3060/Y.2401. Principles for the Management of Next Generation Networks.*

2. ***Principles*** *for a Telecommunications Management Network (Принципи керування телекомунікаційними мережами) // ITU-TRecommendation M.3010. 2010.*

3. ***Daniel A. Menascé, Virgilio A. F. Almeida.*** *Capacity Planning for Web Services: Metrics, Models, and Methods. 2001. Prentice Hall, Sep 11, 2001. 608 p.*

4. ***Чаадаев В. К., Шеметова И. В., Шибаева И. В.*** *Информационные системы компаний связи. Москва: Эко-Трендз, 2004. 256 с.*

5. ***Стеклов В. К., Беркман Л. Н.*** *Проектування телекомунікаційних мереж. Київ: Техніка, 2002. 792 с.*

6. ***Методи*** *підвищення показників якості системи керування телекомунікаційними мережами: монографія / В. В. Хиленко, Л. Н. Беркман, Г. Ф. Колченко, О. Г. Варфоломеєва. Київ: Норіта-плюс, 2007. 236 с.*

7. ***Стеклов В. К., Костік Б. Я., Беркман Л. Н.*** *Сучасні системи керування в телекомунікаціях / за заг. ред. В. К. Стеклова. Київ: Техніка, 2005. 400 с.*

8. ***Телекомунікаційні*** *системи та мережі наступного покоління / В. Ф. Заїка, О. Г. Варфоломеєва, К. О. Домрачева, Г. О. Гринкевич: навч. посіб. Київ: ДУТ, 2019. 352 с.*

9. ***Оптимізація*** *параметрів інфокомунікаційних мереж / В. Б. Толубко, Л. Н. Беркман, В. О. Власенко, Ю. М. Зіненко // Сучасний захист інформації. 2016. №4. С. 58–64.*

L. Berkman, O. Varfolomeeva, G. Kolchenko, A. Zakharzhevsky, N. Perepelytsya

INTEGRATION OF SECURITY SERVICES IN THE ARCHITECTURE OF TELECOMMUNICATIONS MANAGEMENT SYSTEMS

The main tasks of providing the security of the management system of telecommunication networks in Ukraine are considered. Standards and other regulatory documentation on information security of telecommunications and their management systems were analyzed. Special attention is paid to issues of security management as a component of the functional architecture of the telecommunications management system according to the concept of building a TMN telecommunications management network. The peculiarities of the implementation of security services for terminal or intermediate nodes of telecommunication networks are determined. The hierarchical model of providing security services is compared with the model of open systems interaction. A practical model of the security organization of the telecommunications network management system is proposed. The main advantages and disadvantages of the integration of security services at the lower and upper protocol levels are studied. The integration of security services and security mechanisms into the telecommunications architecture is determined by two main considerations: in which nodes should the security services be implemented; at what level each service should be implemented. Because there are a number of arguments for and against each of these levels, there is no single correct solution to this problem. It is advisable to find the optimal solution, depending on the specific security problem.

Keywords: network; management system; security; service; termination system; mediation system.