Підвищення ефективності захисту інформації в мережах спеціального призначення

УДК 004:722.4; 004.056.53

Марина Костяк[1], Любомир Пархуць[2]

Національний університет "Львівська політехніка",
[1]Maryna.Y.Kostiak@lpnu.ua, [2]Liubomyr.T.Parkhuts@lpnu.ua

В умовах тотальної інформатизації та комп'ютеризації усіх галузей діяльності суспільства, всебічного розповсюдження засобів комп'ютерної техніки, значно розширюються і можливості несанкціонованого втручання в інформаційні мережі із реалізацією певних загроз інформаційної безпеки. Розподіленість на великих територіях програмно-апаратних засобів інформаційних мереж, необмежений доступ користувачів до інформаційних ресурсів ускладнює проблему інформаційної безпеки. Фактор розподіленості інформаційних мереж у просторі унеможливлює застосування відомих методів та заходів прямого адміністративного контролю доступу користувачів до ресурсів мережі.

Події останніх років свідчать, що мережі загального користування не можуть забезпечити гарантований захист інформації з обмеженим доступом. Численні проникнення в банківські рахунки, доступ до мережі оборонних відомств, поява в мережі даних державних служб та багато інших випадків підтверджують те, що ідеального захисту від несанкціонованого доступу в мережах не існує. Рано чи пізно навіть найкращий захист може бути зламано.

Тому концепція забезпечення інформаційної безпеки в інформаційному середовищі, якими є сучасні інформаційні мережі, передбачає застосування криптографічних засобів захисту інформації у аспектах конфіденційності, цілісності та доступності. У практичному аспекті ця концепція виражається перш за все у використанні мережевих екранів, віртуальних приватних мереж (VPN), систем виявлення та запобігання вторгненням і т.д.

Криптографічний захист забезпечує достатньо високий рівень інформаційної безпеки абонентів відкритих мереж, якщо йде мова про захист інформації приватного характеру і комерційної таємниці. Проте коли питання ставиться про гарантований захист інформації, що становить державну таємницю чи військову таємницю, необхідно застосовувати інші підходи, які базуються на побудові відокремлених захищених інформаційних мереж, що фізично не під'єднані до мереж загального користування. Саме фізична відокремленість спеціальних інформаційних мереж кардинально знижує рівень зовнішніх загроз, створює передумови гарантованого захисту інформації [1].

Побудова нових мереж висуває на перший план проблему оптимального розміщення апаратних засобів мережі (зокрема, вузлів комутації, пристроїв концентрації та передачі даних), що зведе до мінімуму затрати на побудову такої мережі. Другою проблемою є оптимізація технології функціонування мережі, яка включає організацію ефективного обміну повідомленнями абонентів та мінімізацію службового трафіку, який використовується для управління мережею.

В роботах авторів Євсеєва С.П., Казакової Н.Ф., Капустян М.В., Конаховича Г.Ф., Корченка О.Г., Кудінова В.А., Кузнєцова О.О., Нейвот Я.В., Толюпи С.В., Хорошка В.О., Шелеста М.Є. та інших авторів розглядаються результати наукових

досліджень, які спрямовані на підвищення ефективності функціонування захищених інформаційних мереж [2].

Ефективність функціонування досягається оптимізацією структури мережі для мінімізації затрат на її побудову, оптимізацію загального трафіку в мережі, забезпечення максимально можливих швидкодії і пропускної здатності, а найважливіше забезпечення максимального захисту таємної інформації, що передається такою мережею, від можливого перехоплення та несанкціонованого доступу [3].

Розвиток захищених інформаційних мереж спеціального призначення, розробка ефективних засобів захисту інформаційних ресурсів, оптимізація архітектури, технології функціонування, забезпечення безпеки інформаційних технологій є надзвичайно важливим науково-технічним завданням.

Крім того, існує реальна загроза, що застосування квантових комп'ютерів, які матимуть надвисоку швидкодію при виконанні обчислень, для криптографічного аналізу в найближчій перспективі призведе до компрометації ключів та існуючих методів шифрування. Тому слід шукати новий підхід [4].

Доповідь присвячена вирішенню об'єктивного протиріччя між різко зростаючими обсягами оброблюваних і переданих даних, підвищенням ймовірнісно-часових вимог до безпеки і достовірності команд бойового управління та можливостями апаратури засобів засекреченого зв'язку і шифрувального зв'язку, що стоять на озброєнні Збройних сил України, в умовах гібридності та сінергетичності загроз, коли математичний апарат криптографічного перетворення даних, що застосовується, не дозволяє забезпечити ефективний захист інформації в системах управління і зв'язку спеціального призначення.

1. Костяк М.Ю. Методологія підвищення рівня захисту таємної інформації при її передачі в мережах спеціального призначення / М.Ю.Костяк, Л.Т.Пархуць // Військово-технічний збірник. Академія сухопутних військ. – 2019. – С.31-34.
2. Костяк М.Ю. Розробка профілів захисту в інформаційно-комунікаційних системах / С.О.Іванченко, М.Ю.Костяк, О.В.Мілов, Є.В.Прокопенко // Спеціальні телекомунікаційні системи та захист інформації. ІСЗЗІ КПІ ім. Ігоря Сікорського. – 2019. – Вип. № 2 (6). – С. 96-105.
3. Kostiak M. Information security investment model: resource representation and organizational training /Milov O., Kostiak M., Milevskyi S., Rzaev H. // Advanced Information Systems. – 2019. Vol. 3, No. 4. – С. 96–104.
4. Костяк М.Ю. Програмна реалізація системи потокового шифрування інформації на основі дискретних відображень / О.В.Гресь, Г.М.Розорінов, Ю.Г.Пількевич, М.Ю.Костяк, Л.Т.Пархуць // Міжнародний науковий журнал "Вимірювальна та обчислювальна техніка в технологічних процесах". – 2020. – № 1 (65). – С. 60-66.