УДК 004.056.5

Ю.В. Костюк
Ю.О. Самойленко

ПРОБЛЕМИ ЗАХИСТУ КОРПОРАТИВНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Київський національний торговельно-економічний університет

Анотація: *В статті розглянуто проблеми захисту корпоративних інформаційно-телекомунікаційних мереж, захист яких здійснюється в умовах неповної та нечіткої інформації про мережеві процеси. Тому необхідно повністю забезпечити безпечне функціонування КІТМ в умовах атак зловмисниками на інформаційні ресурси та процеси.*
Ключові слова: корпоративна інформаційно-телекомунікаційна мережа; системи захисту; інформація; контроль; несанкціонований доступ; система підтримки прийняття рішень.

PROBLEMS OF PROTECTION OF CORPORATE INFORMATION AND TELECOMMUNICATIONS NETWORKS

Abstract: *The article considers the problems of protection of corporate information and telecommunication networks, the protection of which is carried out in conditions of incomplete and unclear information about network processes. Therefore, it is necessary to fully ensure the safe operation of KITM in the event of attacks by attackers on information resources and processes.*
Keywords: corporate information and telecommunication network; protection systems; information; control; unauthorized access; decision support system.

Корпоративна інформаційно-телекомунікаційна мережа (КІТМ) є результатом еволюції двох науково-технічних галузей сучасної цивілізації − комп'ютерних і комунікаційних технологій. Інформаційно-телекомунікаційна мережа є цілісною багатофункціональною системою каналів зв'язку, які забезпечують якісну передачу даних на різні відстані. До складу інформаційно-телекомунікаційних мереж входить таке різне комутаційне обладнання. Інформаційно-телекомунікаційні мережі, як високотехнологічні структури, діляться на різні види: безпровідні, провідні, оптичні та інші. В залежності від виду сигналу, фахівці, як правило, виділяють цифрові й аналогові системи, останні сьогодні відживають останні дні свого існування, так як в самому найближчому майбутньому всі інформаційно-телекомунікаційні системи та мережі перейдуть у цифровий формат. Мета існування таких мереж – це передача даних, які в самому процесі передачі піддаються у найменшій кількості помилок та перекручень. До розряду таких інформаційно-комунікаційних мереж можна віднести всім відому мережу Інтернет, телефонні, мобільні мережі, кабельне телебачення.

КІТМ є складною розподіленою системою, що характеризується наявністю великої кількості взаємодіючих ресурсів і водночас протікаючих системних та прикладних інформаційних та телекомунікаційних процесів. Враховуючи тенденцію до створення єдиного інформаційного простору та, як наслідок, підключення корпоративних мереж до глобальної мережі Інтернет, слід очікувати в майбутньому безліч атак на такі системи з метою їхнього руйнування або отримання конфіденційної інформації [1].

Для досягнення ефективного захисту КІТМ засоби та методи захисту повинні адекватно захищати інформацію на підприємстві відповідно до її цінності. Недостатнє вивчення питань кількісної оцінки цінності інформації в сучасній науці не дає можливості об’єктивно оцінити та обґрунтувати необхідні витрати на побудову систем захисту інформаційних та телекомунікаційних систем і мереж.

Телекомунікаційні та мережеві технології нині є тією рушійною силою, яка забезпечує поступальний рух уперед усієї світової цивілізації. Все це особливо важливо для України, де багато чого з названого знаходиться в стадії становлення.

Реалізація методів для забезпечення ефективного функціонування системи захисту в конкретних корпоративних мережах вимагає розробки жорстких заходів захисту для запобігання випадковим та умисним порушенням їх функціонування. Для протидії комп'ютерним злочинам або хоча б зменшення шкоди від них, необхідно правильно вибирати методи та засоби забезпечення захисту інформації (ЗІ) від умисного знищення, крадіжки, псування та несанкціонованого доступу. У простих корпоративних мережах контроль базується на мережевому моніторингу та збору інформації (мережевий моніторинг).

Проблема забезпечення інформаційної безпеки є головною для таких корпоративних мереж. Функціонування складної системи захисту КІТМ забезпечує система управління мережею, яка виконує повний та безперервний контроль за всіма елементами мережі, своєчасне виявлення помилок, несправностей, збоїв та відмов обладнання, програмного забезпечення, управління конфігураціями мережевих вузлів, резервне копіювання та відновлення всіх елементів мережі, управління мережним трафіком та політикою безпеки [2].

Зазначені проблеми унеможливлюють застосування традиційних математичних методів, у тому числі методів математичної статистики та теорії ймовірностей, а також класичних методів оптимізації для вирішення прикладних завдань захист інформації в КІТМ.

Відомі математичні моделі, що використовуються для опису структури, поведінки та управління системою захисту інформації (СЗІ), в умовах некоректної постановки задач не дають бажаного результату. Тому необхідна розробка нових СЗІ, орієнтованих на специфіку процесів захисту методів та засобів моделювання.

Таким чином, складне обладнання КІТМ, великий обсяг інформації, складність вирішення погано формалізованих та слабо структурованих завдань за відсутності повної та достовірної інформації про стан мережевих елементів, а також короткий час для аналізу проблемних ситуацій та прийняття рішень, призводить до невідповідності персоналу до вимог до ефективного управління мережею.

Складність процесу прийняття рішень, відсутність математичного апарату призводить до того, що при оцінці та виборі методів захисту необхідно використовувати та обробляти лише якісну експертну інформацію. Перспективним напрямком розвитку методів прийняття рішень у експертній первинній інформації та впровадження інтелектуальної системи підтримки прийняття рішень використовують лінгвістичний підхід, заснований на теорії нечітких множин та лінгвістичної змінної для управління та діагностикою стану сучасних КІТМ. Крім того, високий рівень автоматизації та інтелектуалізації системи підвищить ефективність надійності функціонування мережі та зменшення економічних ризиків для підприємств.

Забезпечення комплексу засобів захисту інформації з ідентифікацією користувачів при запиту доступу до КІКМ повинна бути реалізована за допомогою сучасних СЗІ від несанкціонованого доступу (НСД). У цьому випадку завдання захисту при виконанні цієї вимоги зменшується до контролю правильності користувацького НДС під час запиту доступу до ресурсів, оскільки використання сервісу НСД користувача може призвести до неконтрольованої зміни ідентифікатора джерела. Контроль доступу включає в себе ідентифікацію користувачів, персоналу та системних ресурсів [3].

Тому важливо розробити інтелектуальну систему підтримки прийняття (СППР) рішень на базі комплексного підходу до проблеми управління інформаційною безпекою та захисту інформації КІКМ від несанкціонованого втручання у процес функціонування КІКМ, в якій розроблений комплекс програм дозволить реалізувати інтелектуальну СППР у задачах захисту інформації в КІТМ з використанням нечітких моделей.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Захист систем електронних комунікацій: навч. посіб. / В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. Київ: Київ. нац. торг.-екон. ун-т, 2019. 164 с.

2. Аналіз стану захищеності інформаційно-телекомунікаційних систем / О. В. Криворучко, О. М. Сунічук, Д. В. Швець та ін. // Управління розвитком складних систем. 2020. № 42, с. 56–62.

3. Developments in the field of information and telecommunications in the context of international security. Resolution adopted by the General Assembly. 2000. № 55/28.

Костюк Юлія Володимирівна, здобувач Phd, асистент кафедри інженерії програмного забезпечення та кібербезпеки, Київський національний торговельно-економічний університет, м. Київ, e-mail: kostyuk.yu@ukr.net.

Самойленко Юлія Олександрівна, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки, Київський національний торговельно-економічний університет, м. Київ, e-mail: y.samoilenko@knute.edu.ua

Kostiuk Yuliia V. - Phd, assistant Department of Software Engineering and Cyber Security, Kyiv National University Of Trade And Economics, Kyiv, e-mail: kostyuk.yu@ukr.net.

Samoilenko Yuliia O. - candidate of technical sciences, Associate Professor, Department of Software Engineering and Cyber Security, Kyiv National University Of Trade And Economics, Kyiv, e-mail: y.samoilenko@knute.edu.ua