УДК 004.738 (043.2)

**В.І. Дрововозов,** к.т.н.,
**С.В. Водоп'янов,** к.т.н.,
**О.В. Толстікова,** к.т.н.
*Національний авіаційний університет, Київ*

## ЗАХИЩЕНІСТЬ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ У МЕРЕЖАХ ТРАНСПОРТНИХ ЗАСОБІВ

У результаті аналізу методів організації та забезпечення якості обслуговування в перспективних інформаційно-комунікаційних та комп'ютерних мережах критичного застосування виявлено, що основним проблемами для мереж є різнорідність мережного трафіку та перевантаження, які погіршують показники QoS. Запобігання перевантаженню реалізується шляхом побудови багаторівневої ієрархічної структури, але методи узгодження протоколів взаємодії автономних мережних сегментів потребують вдосконалення. Це у повній мірі відноситься і до інформаційно-телекомунікаційних систем залізничного транспорту [1].

Інформаційно-телекомунікаційні системи залізничного транспорту є гетерогенними за визначенням. В окремих сегментах комп'ютерних та телекомунікаційних систем залізниці обмін даними здійснюється через кабельні мережі.

Мережі залізничних станцій також мають змішану структуру з поєднанням проводового та безпроводового доступу. Вибір того чи іншого типу доступу обумовлюється міркуваннями пропускної спроможності, надійності та зручності встановлення з'єднань.

Безпроводовий сегмент посідає важливе місце в загальній структурі інформаційно-телекомунікаційних систем транспорту, зокрема, залізничного транспорту.

Окрім загальних проблем управління інформаційно-телекомунікаційними мережами, у безпроводових мережах досить гостро стоять проблеми захисту від несанкціонованих втручань та зовнішніх завад самого різного походження.

Безпроводова інформаційно-телекомунікаційну система (БП ІТС) залізничного транспорту. По суті, вона, як і інформаційно-телекомунікаційні системи повітряного транспорту, представляє собою систему критичного застосування, тобто систему, до якої пред'являються жорсткі вимоги стосовно швидкості опрацювання штатних та екстремальних ситуацій, захищеності від

несанкціонованих втручань та інших ключових параметрів ефективності.

Система критичного застосування (СКЗ) також лежать в основі організаційного управління авіаційним транспортом. Відмітимо тільки, що принциповою відмінністю авіаційного транспорту є те, що зовнішній обмін з іншими абонентами, що знаходяться як на землі, так і у повітрі, здійснюється виключно по безпроводовим каналам зв'язку. Не вдаючись до відмінностей авіаційного, залізничного та автомобільного транспорту, є загальні проблеми забезпечення їх глобальної ефективності.

Слід відмітити, що відбувається поступове нарощування апаратно-програмних засобів аж до створення апаратно-програмних комплексів, що виконують задані функції. Ця особливість СКЗ вимагає, щоб контроль ефективності також був безперервним.

Відмічені особливості інформаційних систем дозволяють сформулювати наступні рекомендації по проектуванню систем контролю та управління СКЗ.

1. Контроль представляє собою комплекс взаємозв'язаних заходів, які супроводжують процес створення системи від етапу проектування до здачі в експлуатацію.

На різних етапах створення СКЗ відкидаються або приймаються зразки комплектуючих елементів, варіанти структури системи, способи резервування, контролю і інші технічні рішення для досягнення головної мети – забезпечити на завершальному етапі створення системи необхідну ефективність.

2. Випробуванням на ефективність слід піддавати об'єкти, заздалегідь перевірені на функціонування. Ефективність авіаційних, залізничних та автотранспортних СКЗ – це властивість найкращої застосовності у критичних режимах.

3. До складу системи контролю включають різноманітні види і способи випробувань, що відповідають особливостям виробництва випробовуваних об'єктів.

4. Система контролю СКЗ за часом його проведення включає наступні основні етапи:

а) контроль апаратури і її елементів з метою отримання інформації про ефективність ключових елементів системи: власне

транспортних засобів, залізничних, повітряних та наземних автомобільних трас, диспетчерських систем тощо;

б) контроль апаратно-програмних комплексів та інформаційних систем в цілому;

в) уточнення оцінки ефективності системи за наслідками підконтрольної експлуатації системи і її частин у нештатних режимах.

5. Найдоцільнішим рішенням проблеми оцінки ефективності СКЗ в цілому є розрахунково-експериментальні методи, тобто поєднання натурних випробувань, розрахунків та імітаційного моделювання. У подальшому отримані оцінки підтверджуються, уточнюються або скасовуються на основі результатів випробувань достатньо репрезентативного об'єму.

6. Кожна СКЗ вимагає розробки своєї методики випробувань, що відображає її особливості, масштаб, область застосування.

Важливою проблемою є забезпечення захищеності ключових елементів, зокрема, інформаційно-комунікаційних та комп'ютерних мереж від несанкціонованого доступу.

Відповідно, і при загальному виборі конкретного мережного комутаційного, термінального і лінійно-кабельного обладнання необхідно враховувати безліч організаційних, технічних і економічних факторів.

У першу чергу, треба локалізувати та ізолювати протоколи обміну даними у сегментах мереж закритого, обмеженого та загального доступу. По суті, сучасні мережі, включаючи Інтернет, базуються на досить обмеженому списку ідей [2]:

– пакетний принцип передання даних та управління;

– адаптація довжини пакету до умов передачі (фрагментація/дефрагментація);

– інкапсуляція пакетів при переході від нижніх рівнів моделі *OSI* на верхні рівні та декапсуляція пакетів при переході від верхніх рівнів на нижні рівні;

– динамічна маршрутизація.

Із-за обмеженості об'єму даної роботи (детальне викладення методу наведене у роботі [2]) наведемо основні результати досліджень:

– для захисту мережних сегментів із закритим доступом від несанкціонованого проникнення (хакерської атаки на мережу,

перехоплення управління транспортним засобом) розроблено методи ізоляції протоколів закритого доступу від протоколів обмеженого та відкритого (загального) доступу;

– $n$ статистичних показників повідомлень, зокрема, кількість вхідних та вихідних *IP, TCP, UDP* пакетів на інтервалі спостереження, час отримання та відправлення пакетів та ін., описуються $n$ -мірною щільністю імовірності;

– щільності імовірності статистичних показників повідомлень у мережах закритого, обмеженого та відкритого доступу є параметрично несумісними, а відповідні коефіцієнти взаємної кореляції є величинами другого порядку малості;

– сукупності сигнатурних показників повідомлень у закритому доступі, у обмеженому доступі, у відкритому доступі та сигнатури атак представляють собою компоненти векторів, майже ортогональних одне одному, а їх векторні добутки – величини другого порядку малості;

– за результатами статистичного та сигнатурного аналізу фільтруються спроби як випадкового, так і навмисного несанкціонованого втручання до сегментів з закритим та обмеженим доступом [3].

## ВИКОРИСТАНІ ДЖЕРЕЛА

*1. Горбенко А.В. Методи та інструментальні засоби розробки комп'ютерних мереж інформаційно-управляючих систем критичного застосування. Автореферат. Канд. техн. наук. – Харків: Національний аерокосмічний університет ім. М.Є. Жуковського "Харківський авіаційний інститут", 2004. – 20 с.*

*2. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. - Pearson Education, Inc., Old Tappan, New Jersey, 2016. – 538 p.*

*3. Водоп'янов С.В. Методи побудови автономних комп'ютерних сегментів аеровузлової мережі. – Дис. канд. техн. наук. - К.: НАУ, 2018. – 164 с.*