УДК 004.738 (045)

DOI: 10.18372/2073-4751.72.17458

Дрововозов В.І., к.т.н.,
orcid.org/0000-0002-6303-9741,
Водоп'янов С.В., к.т.н.,
orcid.org/0009-0006-0424-6173,
Журавель С.В.,
orcid.org/0000-0001-6536-6298

ЗАХИСТ МЕРЕЖ ТРАНСПОРТНИХ ЗАСОБІВ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ШЛЯХОМ ІЗОЛЯЦІЇ ПРОТОКОЛІВ ОБМІНУ

Національний авіаційний університет

drovvlad47@gmail.com

Вступ

Інтенсивний прогрес інформаційних та телекомунікаційних технологій, їх впровадження в усі галузі людської діяльності пов’язані з розробкою та побудовою складних та розвинених інформаційно-обчислювальних систем. Вони стали невід’ємною частиною інформаційно-управляючих систем будь-якого призначення. Це стосується, у першу чергу, розподілених систем обробки інформації та управління складними об’єктами. Водночас з розширенням меж застосування технологій взаємодії відкритих систем і міжнародних стандартів функціонування інформаційно-обчислювальних структур зростають і вимоги до їх швидкодії та надійності, особливо за умовами використання в системах критичного застосування (СКЗ). До таких систем належать, наприклад, авіаційні, ракетно-космічні, залізничні, транспортні, енергетичні та інші системи спеціального призначення [1]. Вони, як правило, працюють в умовах безперервного цілодобового застосування у реальному часі.

За результатами 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. Тому задачі підвищення продуктивності обчислювальних структур, комп’ютерних та телекомунікаційних мереж як для систем критичного застосування, безумовно, є актуальними. Це у повній мірі відноситься і до інформаційно-телекомунікаційних систем залізничного транспорту.

Інформаційно-телекомунікаційні системи залізничного транспорту є гетерогенними за визначенням. В окремих сегментах комп'ютерних та телекомунікаційних систем залізниці обмін даними здійснюється через кабельні мережі (оптоволокно або мідний кабель). Наприклад, від вагонної точки доступу мультимедійна інформація розподіляється до кожного пасажирського місця. Однак отримання будь-якої інформації у точці доступу вже здійснюється через безпроводові канали – від мереж *Wi-Fi, WiMAX* або супутникових мереж.

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.

Зв'язок потягу з будь-яким стаціонарним чи мобільним абонентом об'єктивно може бути лише безпроводовим. Таким чином, безпроводовий сегмент посідає

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

Специфікою безпроводових мереж є розповсюдження сигналів через вільне середовище, тобто принципово відкритий доступ до сигналів як до носіїв інформації, яка передається від одного абонента іншому. Тому, окрім загальних проблем управління інформаційно-телекомунікаційними мережами, у безпроводових мережах досить гостро стоять проблеми захисту від несанкціонованих втручань та зовнішніх завад самого різного походження. Такі твердження є справедливими й для авіаційних систем доступу та розподілу даних через комунікаційні та комп'ютерні мережі.

Дана робота присвячена розробці комбінованого методу захисту сегментів просторово-обмеженої мережі від несанкціонованих вторгнень та спроб перехоплення управління транспортними засобами різних видів.

Короткий опис архітектур та топологій просторово-обмежених мереж

На рис. 1 зображена сукупність повітряних суден (ПС) у зоні аеровузла. Дамо коротку характеристику мережі. Об'єм мережі не фіксований:

$$L_{netw} \leq L_{netwmax}|_{q \geq q_{min}}|,$$

де $L_{netwmax}$ – максимальна відстань між вузлами мережі, обумовлена мінімальним співвідношенням $SINR$ – сигнал / (завади + шуми). Об'єм мережі неперервно змінюється випадковим чином. Зміни залежать від різних (внутрішніх та зовнішніх) чинників. При перевищенні припустимого об'єму мережі система управління мережею намагається негайно повернути мережу до початкового стану.

Механізм управління – триплет якості сервісу *QoS*. Для забезпечення норм на *QoS* у відповідності до рекомендацій *Y*.1564-201602-III – паспортизація потоку трафіку – зазвичай використовують наступні параметри (ключовий триплет *QoS*): пропускна спроможність C_{th}; затримка передачі τ_{lt} та її імовірнісний розподіл $w(\tau_{lt})$; середня кількість бітових помилок у потоці f_{err}.

Доступність мережних вузлів до отримання інформації з гарантованою якістю сервісу залежить від їх географічного положення, зокрема, від дальності бортів одне від іншого.

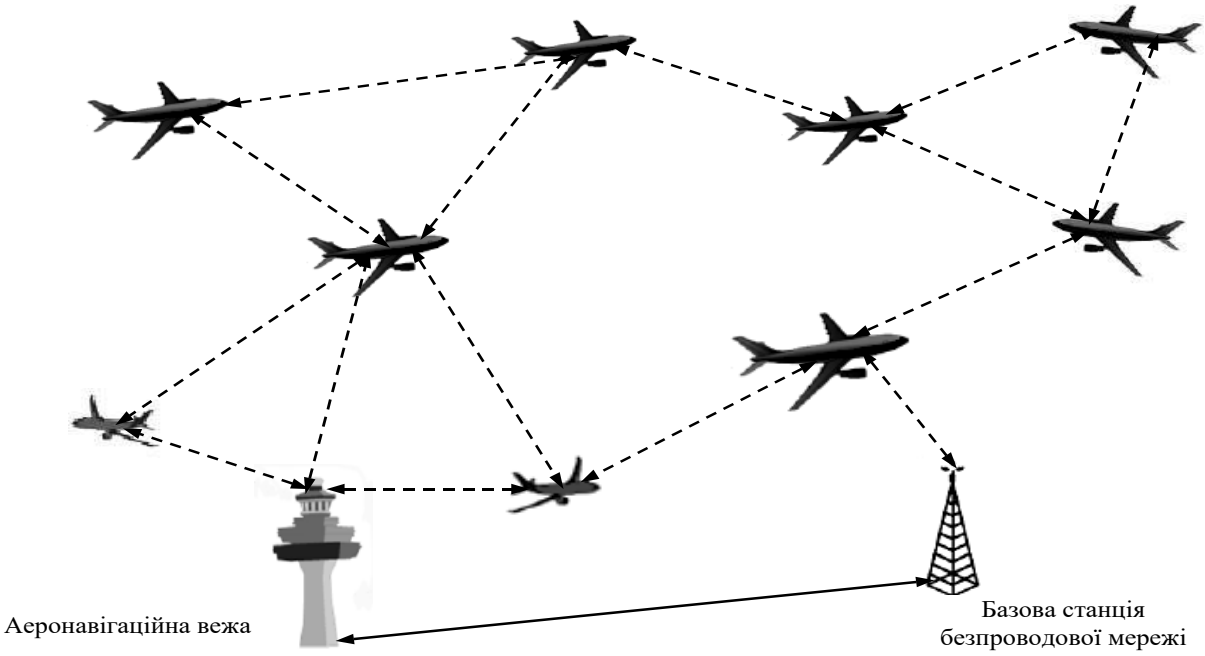

Рис. 1. Схема розміщення ПС у зоні аеровузла

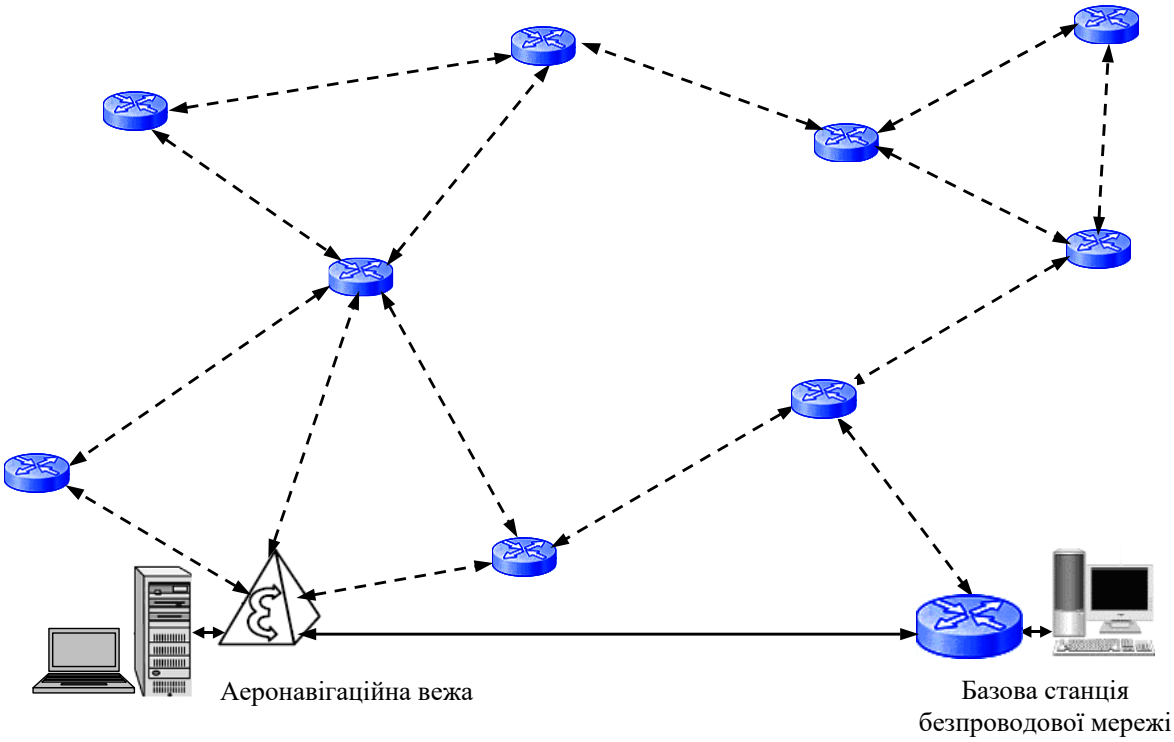

Рис. 2. Еквівалентна схема поточної топології авіаційної бортової мережі; елементи термінальних вузлів – кореневий маршрутизатор та програмний комутатор Softswitch

Безпроводова інформаційно-телекомунікаційна система (БП ІТС) залізничного транспорту, по суті, як і інформаційно-телекомунікаційна система 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. Недотримання хоча б однієї з таких вимог веде до катастрофічних наслідків – людських жертв, повного руйнування системи без можливості її відновлення тощо. Різницю між звичайною системою та системою критичного застосування можна умовно позначити так, як це зображено на рис. 3..

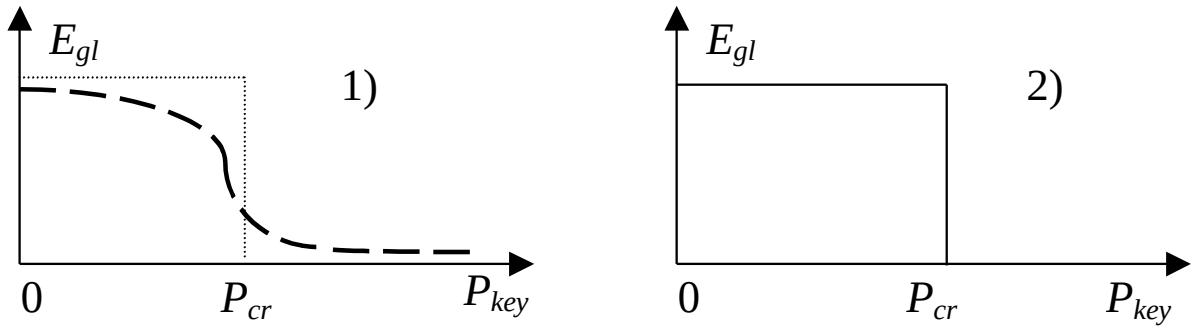

Рис. 3. Залежність глобальної ефективності E_{gl} системи від величини P_{key} ключового параметру: 1) звичайна система; 2) система критичного застосування. P_{cr} – критичне значення ключового параметру

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 інших деталей та відмінностей авіаційного, залізничного та автомобільного транспорту, обговоримо

загальні проблеми забезпечення їх глобальної ефективності. Це тривалий багатоетапний процес, який у певній мірі носить циклічний характер. Після вибору структури системи, який обґрунтовується результатами математичного моделювання та коригується на проміжних етапах, висуваються вимоги до обладнання (у тому числі, до мережного обладнання), що входить до складу системи.

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.

Апаратні засоби СКЗ складаються з різних комплектуючих елементів. По своєму призначенню апаратура підрозділяється на засоби обчислювальної техніки (інформаційно-обчислювальна підсистема), передачі, опрацювання і зберігання інформації (інформаційно-телекомунікаційна підсистема), відображення інформації, джерела живлення тощо.

На ефективність СКЗ впливають різноманітні фактори. Для виявлення їх впливу у штатних режимах використання системи потрібно проведення натурних випробувань. Вплив на ефективність СКЗ у нештатних (екстремальних, критичних) режимах, як правило, доводить до втрати системи, тому його, як правило, досліджують шляхом імітаційного моделювання.

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.

Не допускається механічно переносити принципи організації контролю окремих виробів на організацію контролю великих систем типа СКЗ. Якщо для простих об'єктів масовий контроль ефективності орієнтований на статистичні випробування та на ухвалення рішення або про працездатність, або на вибраковку, то контроль великої системи орієнтується на управління ефективністю в ході її створення та реального функціонування. Це означає, що 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. Якщо об'єкт не підготовлений до виконання заданих функцій у критичних режимах (не налаштований, не відрегульований), то немає сенсу піддавати його контролю ефективності, захищеності, сталості тощо.

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 з використовуванням інформації про ефективність, тобто точність, оперативність та надійність;

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 потребує розробки своєї методики випробувань, що відображає її особливості, масштаб, область застосування. Контроль ефективності пристроїв, що входять до складу великої системи, слід розглядати як попередній етап контролю ефективності всієї системи.

Не менш важливою проблемою є забезпечення захищеності ключових елементів, зокрема, автономних сегментів інформаційно-комунікаційних та комп'ютерних мереж від несанкціонованого доступу. Вважаючи абстрактну транспортну систему об'єктом з обмеженим об'ємом та призначенням, розглянемо типові сегменти мереж обміну даними.

Для вирішення обчислювальних задач, пов'язаних з обробкою конфліктних або екстремальних ситуацій, сплесками інтенсивності руху, заторами та ін., до складу ЛОМ включаються спеціалізовані обчислювачі реального часу. Обробка статистики навантаження на магістральну і локальні обчислювальні мережі може здійснюватися в універсальному обчислювачі. Там же реалізуються алгоритми адаптивної логічної структуризації мереж.

Кількість термінальних вузлів кожного автоматизованого робочого місця (АРМ) оператора залежить від об'єму і напруженості вирішуваних задач і визначається індивідуально для кожної конкретної диспетчерської системи. 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 змінних 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.

Звичайно, сучасні мережні технології доволі складні. Тим не менш, Інтернет представляє собою сукупність програм, які взаємодіють одне з одним за певними правилами. У свою чергу, правила визначаються відповідними мережними протоколами.

Розглянемо автономні мережні сегменти локальної інформаційно-комунікаційної та обчислювальної мережі ПС. На рис. 4 зображена схема мережної інфраструктури, яка вміщує мережі з контрольованим (закритим та обмеженим) доступом та мережу із загальним (відкритим) доступом. Для гарантованого захисту мереж з контрольованим доступом від несанкціонованого втручання необхідно впровадити такі апаратно-програмні засоби:

– ізоляції мережних протоколів закритих сегментів від протоколів сегментів з відкритим доступом;

– системи виявлення та запобігання вторгнень (*IDS-IPS*).

Позначимо сукупність статистичних показників мережного трафіку I_{stat}, як $I_{stat} = \{I_1, I_2, \dots, I_M\}$, де M – кількість статистичних показників. До таких показників відносяться:

– середня кількість вхідних IP-пакетів в одиницю часу $\overline{n}_{inIP}$;

– середня кількість вихідних IP-пакетів за одиницю часу $\overline{n}_{outIP}$;

– середня кількість вхідних TCP-пакетів за одиницю часу $\overline{n}_{inTCP}$;

– середня кількість вихідних TCP-пакетів за одиницю часу $\overline{n}_{outTCP}$;

– середня кількість вхідних UDP-пакетів за одиницю часу $\overline{n}_{inUDP}$;

– середня кількість вихідних UDP-пакетів за одиницю часу n_{outUDP};

– середній час отримання пакетів $\overline{\tau}_{rec}$;

– середній час відправлення пакетів $\overline{\tau}_{send}$;

– середня тривалість сеансу зв'язку в мережі $\overline{T}_{sess}$;

– імовірності прийому повідомлення P;

– імовірності станів Q системи.

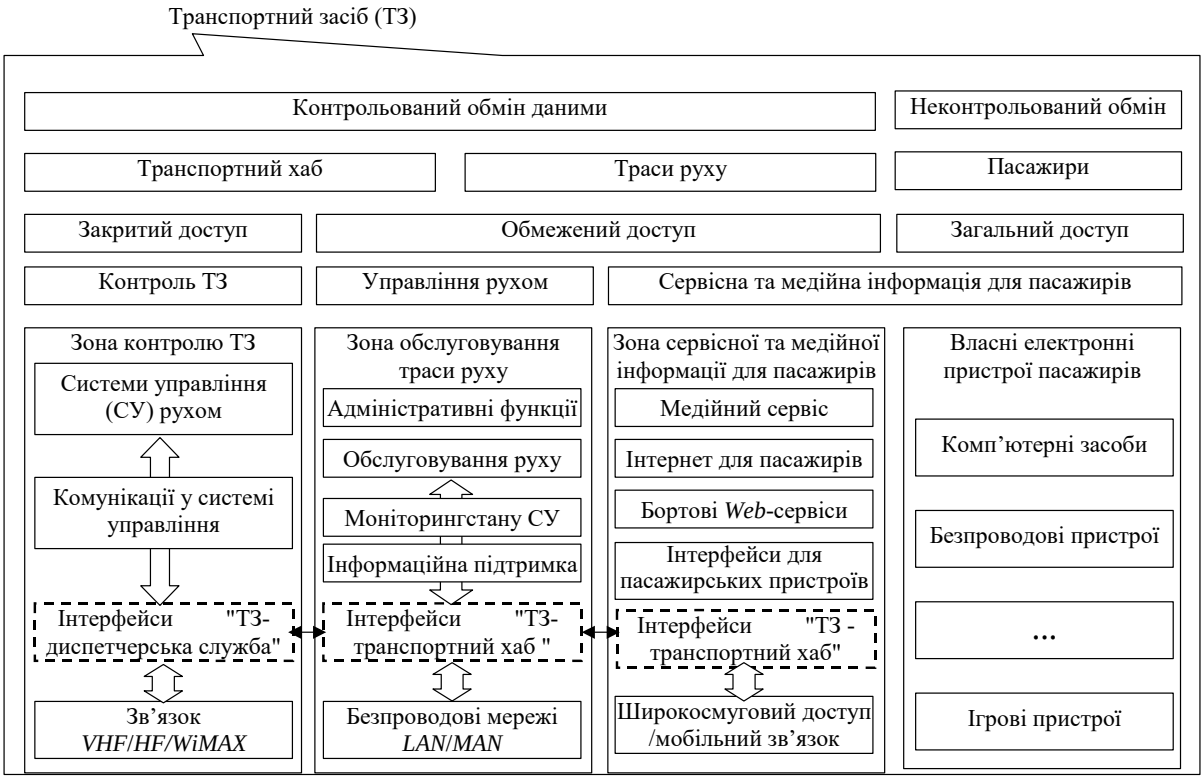

Рис. 4. Структурна схема мережних сегментів, що входять до складу мережі транспортного засобу

Сигнатури складають сукупність

$$K = \{K_1, K_2, \dots, K_N\}$$

де N – кількість сигнатур атак. Наприклад, $K_i, i = \overline{1,N}$ має такі характеристики:

– поле «адреса відправника» F_{SA};

– поле «адреса отримувача» F_{RA};

– поле "тип" F_{type};

– поле «дані» F_{data};

– поле CRC F_{CRC};

– власне дані пакетів $data$, байт;

– час отримання пакетів t_{rec};

– час відправлення пакетів t_{send};

– тривалість сеансу зв'язку в мережі.

Позначимо вектори сигнатур наступним чином:

– вектор сигнатур трафіку закритого доступу $\boldsymbol{K}_{cch}$;

– вектор сигнатур трафіку обмеженого доступу $\boldsymbol{K}_{ltd}$;

– вектор сигнатур трафіку відкритого доступу K_{open}.

Теоретично нормований скалярний добуток векторів K_{cch} та K_{ltd} з кутом θ між ними, має дорівнювати одиниці:

$$R_{norm12} = \frac{|\mathbf{K}_{cch}| \times |\mathbf{K}_{ltd}|}{\sqrt{|\mathbf{K}_{cch} \times \mathbf{K}_{cch}|}\sqrt{|\mathbf{K}_{ltd} \times \mathbf{K}_{ltd}|}} \cos\theta_{12} \to 1. \quad (1)$$

У той же час нормовані скалярні добутки вектору K_{cch} та K_{open} з кутом θ_{13} між ними та $\mathbf{K}_{ltd}$ й $\mathbf{K}_{open}$ з кутом θ_{23} між ними, мають прагнути до нуля:

$$R_{norm13} = \frac{|\mathbf{K}_{cch}| \times |\mathbf{K}_{open}|}{\sqrt{|\mathbf{K}_{cch} \times \mathbf{K}_{cch}|}\sqrt{|\mathbf{K}_{open} \times \mathbf{K}_{open}|}} \cos\theta_{13} \to 0 \quad (2)$$

$$R_{norm23} = \frac{|\mathbf{K}_{ltd}| \times |\mathbf{K}_{open}|}{\sqrt{|\mathbf{K}_{ltd} \times \mathbf{K}_{ltd}|}\sqrt{|\mathbf{K}_{open} \times \mathbf{K}_{open}|}} \cos\theta_{23} \to 0 \quad (3)$$

Аналогічно позначимо вибірки полів протоколів наступним чином:

– вибірка полів протоколів трафіку закритого доступу I_{cch};

– вибірка полів протоколів трафіку обмеженого доступу I_{ltd};

– вибірка полів протоколів трафіку відкритого доступу I_{open}.

Без будь-яких втрат узагальненості можна припустити, що об'єми вибірок I_{cch}, I_{ltd} та I_{open} однакові і складають M відліків кожна. Якщо на практиці вони будуть різними, треба обирати максимальний об'єм, а для решти вибірок доповнювати відсутні відліки нульовими відліками.

Вважаючи, що поля протоколів представляють собою вибірки випадкових величин, наведемо формули для нормованих взаємно кореляційних функцій. Для функції взаємної кореляції вибірок I_{cch} та I_{ltd}

$$\Re_{12}(i)=\frac{1}{M-i+1}\sum_{k=1}^{M-i}I_1(i)I_2(i-k); \quad (4)$$

відповідно, для вибірок I_{cch} та I_{open}

$$\Re_{13}(i)=\frac{1}{M-i+1}\sum_{k=1}^{M-i}I_1(i)I_3(i-k), \quad (5)$$

для вибірок I_{ltd} та I_{open}

$$\Re_{23}(i)=\frac{1}{M-i+1}\sum_{k=1}^{M-i}I_2(i)I_3(i-k). \quad (6)$$

При цьому треба так формувати протоколи закритого, обмеженого та відкритого доступу, щоб при $k=0$ функції $\Re_{12}(0)$ прагнула до одиниці: $\Re_{12}(i) \underset{i=0}{\rightarrow} 1$, а функції $\Re_{13}(0)$ та $\Re_{23}(0)$ прагнули до нуля: $\Re_{13}(i) \underset{i=0}{\rightarrow} 0, \Re_{23}(i) \underset{i=0}{\rightarrow} 0$.

Методи ізоляції протоколів закритого доступу від протоколів обмеженого та відкритого (загального) доступу розробляються з урахуванням формату заголовків пакетів [2]. Це завдання вельми просте. Наприклад, змінюється довжина заголовка, довжина та зміщення фрагменту. Широкі можливості для варіацій дають додаткові дані заголовка й особливо – дані вирівнювання, які не мають практичного значення і уводяться в заголовок тільки для вирівнювання його довжини до границі чотирьохбайтного слова.

Висновки

Для захисту мережних сегментів із закритим доступом від несанкціонованого проникнення (хакерської атаки на мережу, перехоплення управління транспортним засобом) статистичні показники повідомлень, зокрема, кількість вхідних та вихідних *IP, TCP, UDP* пакетів на інтервалі спостереження, час отримання та відправлення пакетів та ін., робляться параметрично несумісними, а відповідні коефіцієнти взаємної кореляції стають 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 скалярні добутки – величинами 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.

Таким чином, запропонована формальна модель комбінованого (статистично-сигнатурного) аналізу повідомлень, що поступають на вхід мережних сегментів з закритим доступом, дозволяє перейти на якісно новий метод виявлення та фільтрації мережних атак. Статистичний підхід є запорукою захисту від нових, раніше невідомих атак та шкідливого програмного забезпечення – так званих "експлоїтів нульового дня".

Література

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.

Дрововозов В.І., Водоп'янов С.В., Журавель С.В.

ЗАХИСТ МЕРЕЖ ТРАНСПОРТНИХ ЗАСОБІВ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ШЛЯХОМ ІЗОЛЯЦІЇ ПРОТОКОЛІВ ОБМІНУ

Статтю присвячено дослідженню методів захисту безпроводових інформаційно-телекомунікаційних систем транспорту. За результатами 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. Специфікою безпроводових мереж є розповсюдження сигналів через вільне середовище, тобто принципово відкритий доступ до сигналів як до носіїв інформації, яка передається від одного абонента іншому. Тому, окрім загальних проблем управління інформаційно-телекомунікаційними мережами, у безпроводових мережах досить гостро стоять проблеми захисту від несанкціонованих втручань та зовнішніх завад самого різного походження. 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. Статистичних показників повідомлень, зокрема, кількість вхідних та вихідних IP, TCP, UDP пакетів на інтервалі спостереження, час отримання та відправлення пакетів та ін., 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 скалярні 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.

***Ключові слова**: безпроводова інформаційно-телекомунікаційна система, протоколи закритого, обмеженого та відкритого доступу, комбінований аналіз сигнатур та протоколів, несанкціоноване втручання.*

Drovovozov V.I., Vodopianov S.V., Zhuravel S.V.

PROTECTION OF VEHICLE NETWORKS AGAINST UNAUTHORIZED ACCESS THROUGH ISOLATION OF EXCHANGE PROTOCOLS

The article is devoted to the study of methods of protection of wireless information and telecommunication systems of transport. According to the results of the analysis of the methods of organization and ensuring the quality of service in promising information and communication and computer networks of critical application, it was found that the main problems for networks are the heterogeneity of network traffic and overloading, which worsen QoS indicators. Congestion prevention is implemented by building a multi-level hierarchical structure, but the methods of coordinating the interaction protocols of autonomous network segments need

improvement. The specificity of wireless networks is the propagation of signals through a free environment, that is, fundamentally open access to signals as carriers of information that is transmitted from one subscriber to another. Therefore, in addition to the general problems of managing information and telecommunication networks, the problems of protection against unauthorized interference and external interference of various origins are quite acute in wireless networks. To protect network segments with closed access from unauthorized intrusion (hacker attack on the network, interception of vehicle control), methods of isolating closed access protocols from restricted and open (general) access protocols have been developed. Statistical indicators of messages, in particular, the number of incoming and outgoing IP, TCP, UDP packets during the observation interval, the time of receiving and sending packets, etc., are parametrically incompatible, and the corresponding coefficients of mutual correlation are values of the second order of smallness; sets of signature indicators of closed access, restricted access, and open access messages and signatures of attacks are components of vectors that are almost orthogonal to each other, and their scalar products are values of the second order of smallness; according to the results of statistical and signature analysis, attempts of both accidental and intentional unauthorized interference to segments with closed and limited access are filtered.

Keywords*: wireless information and telecommunication system, protocols of closed, limited and open access, combined analysis of signatures and protocols, unauthorized intrusion.*