

УДК 621. 618:519

А.О. Аносов<sup>1</sup>, С.П. Василенко<sup>2</sup>, О.В. Сторожук<sup>2</sup><sup>1</sup> Військова частина А1906<sup>2</sup> Центральний науково-дослідницький інститут Збройних Сил України, Київ

## МОДЕЛЬ КОМП'ЮТЕРНОЇ РАДІОМЕРЕЖІ ВІЙСЬКОВО-МОРСЬКОГО ОБ'ЄДНАННЯ ЯК ОБ'ЄКТА ПРОГРАМНО-КОМП'ЮТЕРНОГО ПОДАВЛЕННЯ ПІД ЧАС ОБОРОНИ ДЕРЖАВИ З МОРСЬКОГО НАПРЯМКУ

У статті, на основі аналізу світового досвіду моделювання програмно-комп'ютерного подавлення комп'ютерних мереж сучасних телекомунікаційних систем, створена математична модель комп'ютерної радіомережі військово-морського об'єднання як об'єкта програмно-комп'ютерного подавлення під час оборони держави з морського напрямку.

**Ключові слова:** моделювання, програмно-комп'ютерне подавлення, модель, комп'ютерна радіомережа.

### Вступ

#### Постановка проблеми у загальному вигляді.

Основною складовою сучасних систем розвідки та управління військами є мобільні комп'ютерні засоби, що об'єднані за допомогою захищених радіоліній у комп'ютерні радіомережі (КРМ) [1; 2], які інтегруються у глобальні (регіональні) КРМ. КРМ практично є основою для передавання розвідувальної інформації та команд управління у реальному масштабі часу. У таких умовах для порушення інформаційного обміну у комп'ютерних мережах противник може застосовувати нову складову сучасного протидіювання в інформаційному просторі – програмно-комп'ютерне подавлення (ПКП) [3 – 5]. Тому захист інформаційного обміну в КРМ стає одним з пріоритетних завдань [3 – 5].

Під час розроблення способів захисту від ПКП, оцінювання якості функціонування КРМ в умовах ПКП виникає необхідність формалізувати їх роботу та вплив на їх елементи деструктивних програмних засобів (ДПЗ), що порушують оперативність інформаційного обміну. Однак, підходи до формалізованого опису впливу ДПЗ на роботу серверів, робочих станцій, елементів комутації та маршрутизації даних КРМ не наведені у повному обсязі у відомій авторам літературі, а також не визначені показники для оцінювання впливу ДПЗ на оперативність інформаційного обміну у локальній КРМ (ЛКРМ).

**Аналіз останніх досліджень і публікацій.** Загальні питання ведення програмно-комп'ютерного подавлення комп'ютерних мереж противника розглянуті в [3 – 5]. Математичні ймовірнісні моделі структур електронних обчислювальних машин (ЕОМ) вивчені в [6, 7]. Моделі локальних обчислювальних мереж (ЛОМ) Ethernet та КРМ X.25 на основі системи масового обслуговування (СМО) з очікуванням розроблені в [6, 7]. Але в роботах [6, 7] не визначені показники порушення інформаційного

обміну у КРМ, не врахований процес оброблення даних на робочих станціях (РС) та серверах (СрВ). Результати [6, 7] не адаптовані для вирішення завдань захисту КРМ від ПКП. Тому постає актуальне наукове завдання, що полягає у розробленні моделі, що описує вплив деструктивних програмних засобів на комп'ютерні радіомережі військово-морських об'єднань для врахування при визначенні способів захисту КМ від ПКП.

**Формулювання цілей статті (постановка завдання).** Тому метою і основним змістом статті є розроблення моделі комп'ютерної радіомережі військово-морського об'єднання як об'єкта програмно-комп'ютерного подавлення.

### Виклад основного матеріалу досліджень

Аналіз КРМ військово-морських об'єднань провідних країн світу показав, що основними об'єктами деструктивного програмного впливу у складі сучасних військових комп'ютерних радіомереж є (рис. 1):

робочі станції командирів бойових частин (БЧ), кораблів, груп кораблів, об'єднаних за протоколом типу X.25 засобами системи бойового радіозв'язку (типу SINCGARS SIP та інші.);

робочі станції та сервери автоматизованих інформаційних центрів управління бойовими діями (ЦУБД) та ГКЦ, об'єднаних радіомережами за протоколом Ethernet;

обладнання ГKM, що утворюються на базі КРМ різних ланок управління, об'єднаних засобами тактичної пакетної мережі (ТПМ) за протоколом X.25.

Типова структура КРМ військово-морського об'єднання показана на рис. 1.

Моделювання КРМ – об'єкта ПКП можливо здійснити на основі представлення КРМ сукупністю ієрархічно об'єднаних систем масового обслуговування (СМО), рис. 2.

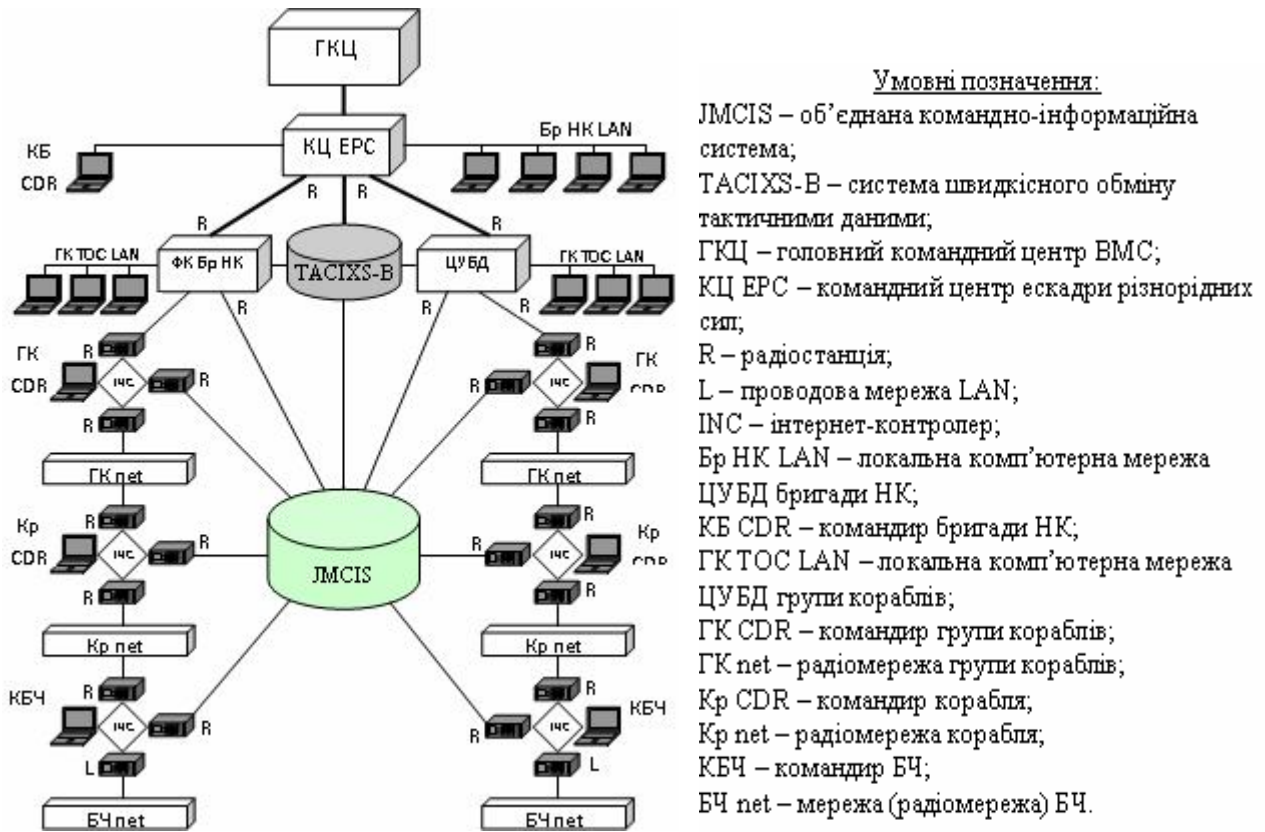


Рис. 1. Типова структура комп'ютерної радіомережі у ланці „бригада надводних кораблів – група кораблів – корабель”

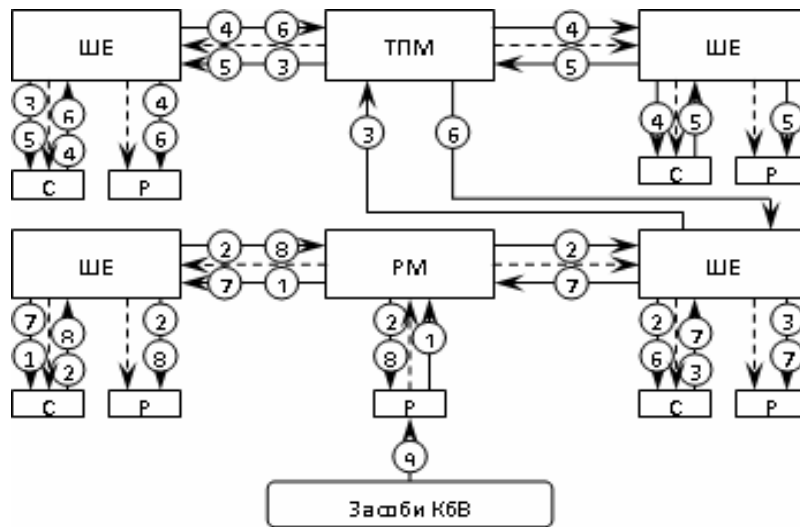


Рис. 2. Представлення КРМ сукупністю ієрархічно об'єднаних СМО

Запроваджені ДПЗ впливають на КРМ, що моделюються, завдяки перевантаженню їх каналів передавання інформації.

Кружками позначене передавання даних про оперативно-тактичну обстановку (ОТО):

1 – від РС засобів розвідки, командирів кораблів, групи кораблів на сервер ЦУБД Бр НК;

2 – від серверу групи кораблів на сервер ЦУБД Бр НК;

3 – від серверу ЦУБД бригади Бр НК на сервер ЦУБД ГКЦ;

4 – від серверу ЦУБД ГКЦ на сервер командного пункту Бр НК;

5 – від серверу командного пункту Бр НК на сервер ЦУБД ГКЦ;

6 – від серверу ГКЦ на сервер ЦУБД Бр НК;

7 – від серверу ЦУБД Бр НК на сервер ЦУБД групи кораблів;

8 – від серверу ЦУБД групи кораблів на сервер кораблів;

9 – запровадження ДПЗ у комп'ютерну мережу підсистемою програмно-комп'ютерного подавлення.

Запроваджені у РС або сервери ДПЗ здійснюють атаку типу “відмова в обслуговуванні”. При цьому, показником ефективності дій противника з програмно-комп’ютерного подавлення може бути обрана  $P^{noi}$  імовірність несвоєчасного отримання командирами (штабами) інформації про ОТО

$$P^{noi} = P(\bar{T}^{noi} > T^{ct}) = 1 - e^{-\beta \bar{T}^{noi}}; \beta = \frac{1}{T^{ct}}, \quad (1)$$

де  $\bar{T}^{noi}$  – середній час отримання інформації про ОТО;  $\beta$  – інтенсивність старіння інформації про ОТО;  $T^{ct}$  – час старіння інформації про ОТО.

$$\begin{aligned} \bar{T}_{Кр}^{oi} &= (\bar{T}_{pc} + \bar{T}_{pm} + \bar{T}_{ше} + \bar{T}_c + \bar{T}_{ше} + \bar{T}_{pm} + \bar{T}_{pc})N_{pc} = (2\bar{T}_{pc} + 2\bar{T}_{pm} + 2\bar{T}_{ше} + \bar{T}_c)N_{pc}; \\ \bar{T}_{БрНК}^{oi} &= \bar{T}_{ГКр}^{oi} + (\bar{T}_c + \bar{T}_{ше} + \bar{T}_{pm} + \bar{T}_{ше} + \bar{T}_c + \bar{T}_{ше} + \bar{T}_{pm} + \bar{T}_{ше} + \bar{T}_c)N_{ГКр} = \\ &= \bar{T}_{ГКр}^{oi} + (4\bar{T}_{ше} + 2\bar{T}_{pm} + 3\bar{T}_c)N_{ГКр}; \\ \bar{T}_{ЕРС}^{oi} &= \bar{T}_{БрНК}^{oi} + (\bar{T}_c + \bar{T}_{ше} + \bar{T}_{тпм} + \bar{T}_{ше} + \bar{T}_c + \bar{T}_{ше} + \bar{T}_{тпм} + \bar{T}_{ше} + \bar{T}_c)N_{БрНК}; \end{aligned} \quad (3)$$

де  $\bar{T}_{ГКр}^{oi}$ ,  $\bar{T}_{БрНК}^{oi}$ ,  $\bar{T}_{ЕРС}^{oi}$  – середній час отримання інформації про ОТО у ланках «група кораблів», «бригада НК», «ескадра різнорідних сил» відповідно;  $\bar{T}_{pc}$ ,  $\bar{T}_c$  – середній час оброблення даних транзакції у РС та сервері відповідно;  $\bar{T}_{pm}$ ,  $\bar{T}_{ше}$ ,  $\bar{T}_{тпм}$  – середній час очікування і передавання даних транзакції через радіомережу по шині Ethernet локальної обчислювальної мережі (ЛОМ), через ТПМ відповідно;  $N_{pc}$  – кількість РС у ЛОМ;  $N_{ГКр}$  – кількість груп кораблів у бригаді надводних кораблів;  $N_{БрНК}$  – кількість бригад НК у ЕРС.

Для оцінювання показників

$$\bar{T}_{pc}, \bar{T}_c, \bar{T}_{pm}, \bar{T}_{ше}, \bar{T}_{тпм}$$

необхідно розробити математичні моделі сервера, робочої станції, радіомережі, шини Ethernet, та тактичної пакетної мережі як об’єктів здійснення програмно-комп’ютерного подавлення. Середній час оброблення даних транзакцій сервером дорівнює

$$\bar{T}_c = \bar{T}_c^{op} q, \quad (4)$$

де  $\bar{T}_c^{op}$  – середній час обслуговування пакету сервером;  $q$  – математичне сподівання кількості пакетів транзакції.

Розглянемо варіант  $E_r - n - M$ , коли функція розподілу часу обслуговування вузлами  $B_1$  та  $B_2$  – ерлангівська  $f_1(t) = \frac{\lambda_1(\lambda_1 t)^{r-1} e^{-\lambda_1 t}}{(r-1)!}$  та експоненцій-

на  $f_2(t) = \lambda_2 e^{-\lambda_2 t}$  відповідно, де  $\lambda_1, \lambda_2$  – інтенсивності обслуговування вузлами  $B_1$  та  $B_2$  відповідно;  $r$  – показник Ерланга (кількість етапів обслуговування).

Тоді, враховуючи (1), можна основним показником ефективності захисту КРМ від атаки типу “відмова в обслуговуванні” обрати ймовірність  $P_{пкп}^{coi}$  своєчасного отримання інформації про ОТО відповідним командиром в умовах проведення противником заходів з ПКП

$$P_{пкп}^{coi} = P(\bar{T}^{oi} \leq T^{ct}) = 1 - (1 - e^{-\beta \bar{T}^{oi}}), \quad (2)$$

а частковим критерієм ефективності захисту КРМ від ПКП є виконання умови  $1 > P_{пкп}^{coi} \geq 0,85$  [3].

Середній час отримання інформації про ОТО представлений на рис. 1:

Середній час обслуговування заявки такою системою [6] визначимо у вигляді

$$\begin{aligned} \bar{T}_c^{op} &= \frac{r}{\lambda_1} + \frac{1}{\lambda_2} \times \\ &\times \left[ \sum_{s=0}^n (-1)^{n-s} \frac{(r(s+1))!}{(n-s)!(r(s+1)-n+s)!} a_1^{n-s} a_2^{s+1} \right]^{-1}, \quad (5) \\ a_1 &= \frac{\lambda_2}{\lambda_1 + \lambda_2}, \quad a_2 = \left( \frac{\lambda_1 + \lambda_2}{\lambda_1} \right)^r. \end{aligned}$$

У [6] показано, що вираз (5) справедливий і для варіанта  $M - n - E_r$ , тобто для випадку, коли сервер передає дані транзакції на РС.

Математичне сподівання кількості заявок (пакетів) дорівнює:

$$q = \sum_{k=1}^K \sum_{j=1}^J p_j g_{jk} \left[ \sum_z (p_{w_{kz}} + p_{v_{kz}}) \left( \left[ \frac{z}{b} \right] + 1 \right) \right], \quad (6)$$

де  $p_j$  – імовірність звернення робочої станції до  $j$ -ої транзакції;  $g_{jk}$  – середня кількість операторів, які виконуються при зверненні до  $j$ -ої транзакції;  $K$  – кількість усіх транзакцій;  $J$  – кількість операторів;  $p_{w_{kz}}$  – імовірність того, що для передавання  $k$ -го оператора на сервер потрібно  $z$  байтів;  $b$  – максимальний обсяг даних в пакеті;  $p_{v_{kz}}$  – імовірність того, що після передавання результатів виконання  $k$ -го оператора на робочу станцію потрібно  $z$  байтів.

Цей процес охарактеризуємо показником с зниження інтенсивності обслуговування пакетів даних транзакцій. Він залежить від співвідношення інтенсивностей пакетів даних транзакцій та пакетів, які цьому заважають:

$$c = \frac{\lambda^{TP}}{w_c \lambda_c^{3п} + \lambda^{TP}}, \quad (7)$$

де  $\lambda^{TP}$  – інтенсивність пакетів даних транзакцій;  $\lambda_c^{3п}$  – інтенсивність пакетів, які цьому заважають при подавленні серверу;  $w_c$  – кількість РС, у які запроваджені ДПКЗ для подавлення серверу;

$$\lambda^{TP} = \frac{N_{pc} Q}{A}; \quad (8)$$

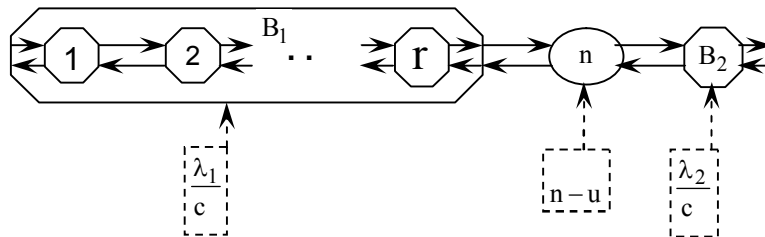


Рис. 3. Модель сервера (робочої станції) при здійсненні програмно-комп'ютерного подавлення КРМ

$$\bar{T}_c = \left[ \frac{r}{c\lambda_1} + \frac{1}{c\lambda_2} \left( \sum_{s=0}^{n-u} (-1)^{n-u-s} \frac{(r(s+1))!}{(n-u-s)!(r(s+1)-n+u+s)!} a_1^{n-u-s} a_2^{s+1} \right)^{-1} \right] \times \sum_{k=1}^K \sum_{j=1}^J p_j g_{jk} \left[ \sum_z (p_{w_{kz}} + p_{v_{kz}}) \left( \left[ \frac{z}{b} \right] + 1 \right) \right]. \quad (9)$$

Функціонування РС КРМ під час оброблення даних транзакції принципово не відрізняється від роботи серверу.

$$\bar{T}_{pc} = \left[ \frac{r}{\lambda_1} + \frac{1}{\lambda_2} \left( \sum_{s=0}^n (-1)^{n-s} \frac{(r(s+1))!}{(n-s)!(r(s+1)-n+s)!} a_1^{n-s} a_2^{s+1} \right)^{-1} \right] \times \sum_{k=1}^K \sum_{j=1}^J p_j g_{jk} \left[ \sum_z (p_{w_{kz}} + p_{v_{kz}}) \left( \left[ \frac{z}{b} \right] + 1 \right) \right]. \quad (10)$$

Шину Ethernet КРМ можна моделювати як СМО з випадковим вибором заявки (пакета) на обслуговування та дисципліною обслуговування, що не допускає переривання обробки.

Модель програмно-комп'ютерного подавлення шини Ethernet представлена на рис. 4.

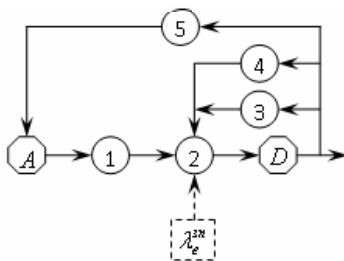


Рис. 4. Модель шини Ethernet як об'єкта програмно-комп'ютерного подавлення

Восьмикутниками позначені апарати обслуговування: А – обдумування користувачем будь-якої РС ЛОМ результатів виконання транзакції і заповнення вихідних форм перед запуском нової транзакції; D – передавання кадру по шині Ethernet при оброблення будь-якої транзакції. Кругами позначені події: 1 – запуск нової транзакції; 2 – постановка кадру, який

де  $\lambda^{TP}$  – інтенсивність пакетів даних транзакцій;  $\bar{A}$  – середній час обмірковування користувачем РС результатів виконання транзакції і заповнення вихідних форм перед запуском нової транзакції.

Тоді модель серверу (РС) КРМ в умовах ведення противником ПКП може бути представлена у вигляді, як на рис. 3, де восьмикутники – вузли СМО; овали – накопичувач заявок; пунктирними прямокутниками показаний процес генерування пакетів даних, які цьому заважають.

З урахуванням (5) – (7) середній час оброблення даних транзакції робочою станцією може бути оцінений за виразом

передається, в чергу до шини Ethernet; 3 – перехід до наступного кадру, який передається; 4 – перехід до наступного оператора транзакції; 5 – відображення результатів виконання транзакції. Середній час очікування і передавання пакетів транзакції по шині Ethernet ЛОМ можливо оцінити за виразом [6]:

$$\bar{T}_{ше} = \frac{\rho v q}{2m_b(1-\rho)} + q m_b; \quad m_b = \frac{b+S}{C_e}; \quad (11)$$

$$\rho = \left( \frac{N_{pc} Q}{A} + w_e \lambda_e^{3п} \right) m_b; \quad v = m_b^2,$$

де  $\rho$  – завантаження СМО;  $q$  – математичне сподівання кількості пакетів, які обслуговуються системою під час передавання даних транзакції, розраховується за виразом (5);  $w_e$  – кількість РС, у які запроваджені ДПКЗ для подавлення шини Ethernet;  $\lambda_e^{3п}$  – інтенсивність пакетів даних, які заважають при подавленні шини Ethernet;  $v$  – другий початковий момент часу передавання пакета по шині мережі;  $S$  – сума довжин заголовку та кінцевика пакету;  $b$  – максимальний обсяг даних у пакеті;  $C_e$  – швидкість передавання даних у мережі Ethernet.

Однак, при розрахунках середнього часу очікування і передачі пакетів транзакції по шині Ethernet ЛОМ необхідно враховувати, що вираз (11) справедливий для значень завантаження шини Ethernet  $\rho \leq \rho_{кр}$ , де  $\rho_{кр} = 0,3 \dots 0,35$  [3]. За  $\rho > \rho_{кр}$  виникає лавиноподібне збільшення кількості колізій, падіння продуктивності шини, при цьому, середній час очікування і передавання пакетів транзакції по шині Ethernet ЛОМ прагне до нескінченності.

Розглянемо моделювання процесу передавання даних через ТПМ. Нехай  $\Lambda = \|\lambda_{lt}\|$  – матриця інтенсивностей пакетів, які передаються між парою маршрутизаторів  $l$  та  $t$  [6]:

$$\begin{aligned} \lambda_{lt} &= \lambda_{l(t)} (Y_{l(t)} + Z_{l(t)}); \\ Y_{l(t)} &= \sum_{k=1}^K \sum_{j=1}^J p_{l(t)j} g_{jk} \sum_z p_{w_{kz}} \left( \left\lfloor \frac{z}{b} \right\rfloor + 1 \right); \\ Z_{l(t)} &= \sum_{k=1}^K \sum_{j=1}^J p_{l(t)j} g_{jk} \sum_z p_{v_{kz}} \left( \left\lfloor \frac{z}{b} \right\rfloor + 1 \right), \end{aligned} \quad (12)$$

де  $\lambda_{l(t)}$  – інтенсивність запитів до транзакцій серверів ЛОМ, які передаються через маршрутизатори  $l(t)$ ;  $p_{l(t)j}$  – імовірність звертання серверу ЛОМ до  $j$ -ої транзакції, яка передається через маршрутизатор  $l(t)$ ;  $Y_{l(t)}$  – середня кількість пакетів, що передаються з одного маршрутизатора на інший під час оброблення всіх операторів будь-якої транзакції;  $Z_{l(t)}$  – середня кількість пакетів, що передаються з одного маршрутизатора на інший після оброблення операторів будь-якої транзакції. Визначимо матрицю  $U = \|x_{df}\|$  інтенсивностей пакетів, які передаються по фізичному каналу, що пов'язують комутатори  $d$  та  $f$ :

$$x_{df} = \sum_{l,t \in (d,f)} \lambda_{lt}, \quad (13)$$

тобто сума береться за тими віртуальними каналами, які проходять через фізичний канал  $(d, f)$ . Нехай буфер комутатора має велику місткість (втрат немає), розміри пакетів, які передаються по мережі X.25, мають неоднакову довжину, а час передавання пакета по фізичному каналу  $(d, f)$  розподілений за експоненційним законом з інтенсивністю  $1/m_{df}$ , де  $m_{df}$  – математичне сподівання часу передавання пакета по фізичному каналу  $(d, f)$ , розраховується як [7]:

$$\begin{aligned} m_{df} &= (C_x)^{-1} \times \\ &\frac{\sum_{k=1}^K \sum_{j=1}^J p_{l(t)j} g_{jk} \left( \sum_z (p_{w_{kz}} + p_{v_{kz}}) \left( z + \left\lfloor \frac{z}{b} \right\rfloor + 1 \right) S \right)}{\sum_{k=1}^K \sum_{j=1}^J p_{l(t)j} g_{jk} \left( \sum_z (p_{w_{kz}} + p_{v_{kz}}) \left( z + \left\lfloor \frac{z}{b} \right\rfloor + 1 \right) \right)}, \end{aligned} \quad (14)$$

де  $C_x$  – швидкість передавання даних у мережі X.25.

Нехай потік пакетів, які передаються між парою маршрутизаторів, є пуассонівським. У цьому випадку середній час передавання пакета по віртуальному каналу, який поєднує два маршрутизатору, можливо оцінити за виразом [7]:

$$\bar{T}_{lt} = \sum_{l,t \in (d,f)} \frac{m_{df}}{1 - x_{df} \cdot m_{df}}, \quad (15)$$

ДПЗ запускає процес завантаження, який генерує пакети даних для передавання через ТПМ та її перевантаження. Враховуючи (12) – (15), середній час очікування і передачі даних транзакції через ТПМ можна оцінити за формулою:

$$\begin{aligned} \bar{T}_{ТПМ} &= \sum_{k=1}^K \sum_{j=1}^J p_{l(t)j} g_{jk} \left( \sum_z (p_{w_{kz}} + p_{v_{kz}}) \left( \left\lfloor \frac{z}{b} \right\rfloor + 1 \right) \right) \times \\ &\times \sum_{l,t \in (d,f)} \frac{m_{df}}{1 - x_{df} \cdot m_{df}} \cdot x_{df} = \sum_{l,t \in (d,f)} \lambda_{lt} + \sum_{l^* \in (d,f)} \lambda_x^{3п}, \end{aligned} \quad (16)$$

де  $l^*$  – маршрутизатори, через які передаються пакети, що заважають від серверів із запровадженими ДПЗ;  $\lambda_x^{3п}$  – інтенсивність пакетів, що заважають даних при подавленні ТПМ.

При оцінюванні середнього часу оброблення даних транзакції сервером або робочою станцією, передавання даних транзакції по шині Ethernet та через ТПМ необхідно враховувати, що інтенсивності пакетів, які заважають при подавленні сервера  $\lambda_c^{3п}$ , при подавленні шини Ethernet  $\lambda_e^{3п}$ , при подавленні ТПМ  $\lambda_x^{3п}$ , мають обмеження зверху  $\lambda_{max}^{3п}$ , зумовлені продуктивністю РС та серверів, у які запроваджені ДПЗ:

$$\begin{aligned} \lambda_{max}^{3п} &= \\ &= \left[ \frac{r}{\lambda_1} + 1 / \left( \lambda_2 \left( \sum_{s=0}^n \frac{(-1)^{n-s} \cdot (r(s+1))! \cdot a^{n-s} b^{s+1}}{(n-s)!(n-s-r(s+1))!} \right) \right) \right]^{-1}, \end{aligned} \quad (17)$$

де величина показника  $r$  залежить від реалізації ДПЗ, може відрізнитись від значення, що отримане при оцінюванні середнього часу оброблення даних транзакції сервером або робочою станцією. Модель радіомережі представлена на рис. 5, де восьмикутником  $K$  позначений апарат обслуговування – квант часу, протягом якого відбувається обслуговування заявки; прямокутником  $H$  позначена черга заявок; кружками позначені заявки: 1 – нові, 2 – зациклені (для обслуговування яких потрібні декілька квантів), 3 – обслужені.

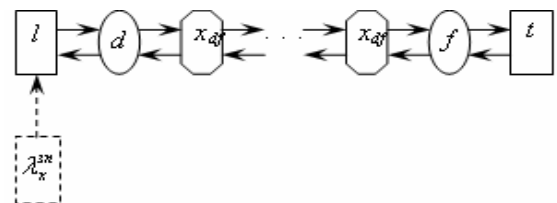


Рис. 5. Модель ТПМ як об'єкта програмно-комп'ютерного подавлення

Для такої СМО (рис. 6) середній час очікування і передавання даних транзакції визначається як

$$\bar{T}_{PM} = q(b+S)/C_{ep}, \quad (18)$$

де  $q$  – математичне сподівання кількості пакетів під час передавання даних транзакції, розраховується за виразом (5);  $b$  – максимальний обсяг даних у пакеті;  $S$  – сума довжин заголовку пакета, заголовку кадру, кінцевика кадру;  $C_{ep}$  – швидкість передавання даних у радіомережі типу TACIXS-B.

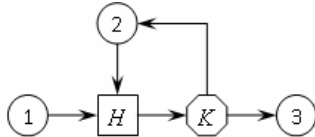


Рис. 6. Модель радіомережі TACIXS-B – об'єкта

Оскільки кількість тайм-слотів, які виділяються кожному абоненту радіомережі TACIXS-B для передавання пакетів даних протягом кадру, залежить від пріоритету абонента і є фіксованою, інтенсивність звертань до транзакцій однієї РС не вплине на час очікування і передавання даних іншими РС.

### Висновки та перспективи подальших досліджень

Розроблена математична модель програмно-комп'ютерного подавлення КРМ, де остання моделюється як багаторівнева система масового обслуговування, дозволяє формалізувати процеси передавання інформації в умовах проведення комп'ютерної атаки "відмова в обслуговуванні". Розроблені математичні моделі елементів КРМ як об'єктів впливу деструктивних програмних засобів створюють можливість визначення ймовірності своєчасного отримання командирами (штабами) інформації, яка є показником ефективності захисту комп'ютерної радіомережі при проведенні комп'ютерної атаки типу "відмова в обслуговуванні". Показниками, що впливають на ефективність захисту комп'ютерної мережі, є кількості РС та серверів, у які запроваджені ДПКЗ в умовах застосування апаратно-програмних засобів захисту мережі, а також інтенсивності пакетів даних, що заважають при подавленні серверу, шини Ethernet ЛОМ, ТПМ.

### МОДЕЛЬ КОМП'ЮТЕРНОЇ РАДИОСЕТІ ВОЕННО-МОРСКОГО ОБ'ЄДИНЕННЯ ЯК ОБ'ЄКТА ПРОГРАМНО-КОМП'ЮТЕРНОГО ПОДАВЛЕННЯ ПРИ ОБОРОНЕ ГОСУДАРСТВА С МОРСКОГО НАПРАВЛЕННЯ

А.А. Аносов, С.П. Василенко, А.В. Сторожук

В статті на основі аналізу мирового опыта моделирования программно-компьютерного подавления компьютерных сетей современных телекоммуникационных систем создана математическая модель компьютерной радиосети военно-морского объединения как объекта программно-компьютерного подавления при обороне государства с морского направления.

**Ключевые слова:** моделирование, программно-компьютерное подавление, модель, компьютерная радиосеть.

### RADIO NETWORK COMPUTER MODEL NAVY ASSOCIATION AS AN OBJECT COMPUTER SOFTWARE AND SUPPRESSION IN DEFENSE OF THE STATE WITH OFFSHORE DESTINATIONS

A.A. Anosov, S.P. Vasilenko, A.V. Storozhuk

On the basis of analysis of world experience modelling computer software and computer networks suppression of modern telecommunication systems a mathematical model of computer radio naval association as an object of computer software and suppression in the defence of the state and direction of the sea.

**Keywords:** modelling, computer software, suppression, model, computer radio.

Розроблена модель може бути використана для створення універсальних апаратно-програмних "полігонів" для дослідження процесів впливу ДПКЗ на ефективність застосування систем захисту інформації комп'ютерних мереж. Окремим напрямом застосування моделі є оцінювання ефективності застосування ДПКЗ в умовах дії різних типів систем захисту інформації при їх розробленні.

Напрямок подальшого застосування математичної моделі є визначення підходів та обґрунтування раціональних способів захисту інформації у КМ за умови комплексного застосування ДПКЗ різного призначення.

### Список літератури

1. Массной, В. Автоматизированные системы управления войсками США [Текст] / В. Массной, Ю. Судачков // Зарубежное военное обозрение. – 2003. – № 9. – С. 25–32; № 10. – С. 28–36.
2. Чайка, Ю. Д. Архитектура системы военного зв'язку армій країн НАТО XXI ст. [Текст] / Ю. Д. Чайка // Проблеми розвитку інформаційних мереж військового призначення: матеріали II наук.-практ. семін. – К.: НА ОУ. – 2004. – С. 71–90.
3. Шолохов, С. М. Наукові підходи до оцінки ефективності дезорганізації управління військами (силами) противника у збройній боротьбі сучасності та майбутнього [Текст] / С. М. Шолохов, Г. М. Тіхонов, Е. В. Лучук // Труды академії. – 2007. – № 76. – С. 78–91.
4. Шолохов, С. М. Програмно-комп'ютерне подавлення комп'ютерної транспортної мережі передачі даних тактичної ланки в операціях (бойових діях) [Текст] / С. М. Шолохов // Труды академії. – 2005. – № 59 – С. 144–152.
5. Шолохов, С. Н. Информационное оружие – новый класс вооружения для дезорганизации АСУ войсками и оружием при проведении информационных наступательных операций [Текст] / С. М. Шолохов, Г. М. Сидченко // Сб. научн. трудов ХВУ. – Х.: ХВУ, 2002. – № 1(39). – С. 48–53.
6. Артамонов, Г. Т. Аналитические вероятностные модели функционирования ЭВМ [Текст] / Г. Т. Артамонов, О. М. Брехов. – М.: Энергия, 1978. – 368 с.
7. Григорьев, Ю. А. Модели анализа процессов передачи данных в компьютерных сетях [Текст] / Ю. А. Григорьев, А. А. Остапенко, А. Д. Плутненко. – М.: МГТУ им. Баумана, 2000. – 99 с.

Надійшла до редколегії 19.11.2013

**Рецензент:** д-р техн. наук доц. Д. П. Пашков, Національний університет оборони України ім. І. Черняховського, Київ.