КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (2), 2018
ISSN 2663 - 4023

УДК 004.056.5:004.75

Смірнов Олексій Анатолійович
доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
OrcID: 0000-0001-9543-874X
dr.smirnovoa@gmail.com

Смірнов Сергій Анатолійович
кандидат технічних наук, старший викладач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
OrcID: 0000-0002-7649-7442
smirnov.ser.81@gmail.com

Поліщук Людмила Іванівна
старший викладач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
OrcID: 0000-0001-5093-1581
pli_80@ukr.net

Конопліцька-Слободенюк Оксана Костянтинівна
викладач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
OrcID: 0000-0001-9981-5194
ksuha80@gmail.com

Смірнова Тетяна Віталіївна
кандидат технічних наук
Центрально український національний технічний університет, Кропивницький, Україна
OrcID:0000-0001-6896-0612
sm.tetyana@gmail.com

GERT-МОДЕЛІ ТЕХНОЛОГІЇ ХМАРНОГО АНТИВІРУСНОГО ЗАХИСТУ

Анотація. У даній статті розроблено комплекс математичних GERT-моделей технології хмарного антивірусного захисту телекомунікаційної системи (ТКС), що дозволило отримати аналітичні вирази для розрахунку часу передачі файлів метаданих і формування та доставки команд передачі керування. Розроблено математичну модель і проведено дослідження ймовірнісно-часових характеристик алгоритмів і програм формування й обробки метаданих у хмарних антивірусних системах. Її відмінною рисою є врахування необхідності формування команд передачі керування програмному клієнтові ТКС. На другому етапі моделювання розроблені GERT-моделі технології формування і обробки метаданих у хмарних антивірусних системах. Особливістю даних моделей є врахування таких технологічних факторів ТКС, як гетерогенність, багатозв'язковість, можливість розбивання файлу метаданих і команд передачі керування на кадри й ін. Використання розробленої GERT-моделі технології передачі файлів метаданих, а також обробки й доставки команд передачі керування та врахування в ній можливості розбивання файлу метаданих і команд передачі керування на кадри дозволило в 1,2 рази підвищити точність при оцінці часової характеристики, і в 1,4 рази при оцінці джиттера часу передачі й обробки файлів метаданих і команд передачі керування. Оцінка точності результатів моделювання підтвердила факт доцільності використання розробленої GERT-моделі технології передачі геш-файлу метаданих і команд передачі керування при проектуванні систем антивірусного захисту сучасних ТКС.

Ключові слова: телекомунікаційні системи; антивірусний захист; обробка метаданих; хмарні антивірусні системи.

ISSN 2663 - 4023

1. ВСТУП

1.1 ПОСТАНОВКА ЗАВДАННЯ ДОСЛІДЖЕННЯ

Технології хмарного антивірусного захисту містять у собі складні математичні методи й програмно-апаратні комплекси зберігання, обробки й передачі даних, комп'ютеризовані засоби управління, телекомунікацій і ін. Постійний розвиток засобів обчислювальної техніки й комплексів автоматизації, а також попит, що підвищується, на послуги хмарних антивірусних систем призводить до збільшення обсягів переданих метаданих у дані системи.

У цей час прогрес в області хмарних технологій, розвиток обчислювальних і телекомунікаційних технологій, а також нове науково-методичне забезпечення проектування хмарних антивірусних систем [1], [2], створили реальну базу для підвищення якості проектних робіт, уніфікації засобів антивірусного захисту даних і створення умов оптимізації процесу обробки метаданих у хмарних антивірусних системах. Однак ріст вимог до точності моделювання і якості технічних розробок вимагає враховувати безліч об'єктивних і суб'єктивних факторів, що виникають у процесі функціонування ТКС. Такими факторами є:

– гетерогенність ТКС, що містять різні компоненти багато з яких самі є складними, багатофункціональними системами;

– багатозв’язковість і великомасштабність ТКС;

– децентралізація інформаційних і обчислювальних ресурсів у глобальній мережі;

– схильність різного роду зовнішнім і внутрішнім вторгненням (особливо вірусним атакам);

– наукоємність і безперервність розвитку, базування на перспективних технічних і програмних розробках і ін.

Метою роботи є розробка математичних моделей, які найбільш точно формалізують технологію функціонування ТКС. Найбільш важливим при цьому є завдання математичного опису технології хмарного антивірусного захисту ТКС із урахуванням ряду основних факторів (гетерогенність, багатозв’язковість і ін.).

Для рішення поставленого завдання розглянемо загальну структуру технології хмарного антивірусного захисту ТКС.

1.2 СТРУКТУРА ТЕХНОЛОГІЇ ХМАРНОГО АНТИВІРУСНОГО ЗАХИСТУ

Проведені дослідження процесу збирання, зберігання і обробки метаданих у хмарних антивірусних системах показали, що загальну структуру технології хмарного антивірусного захисту можна представити у вигляді схеми рис. 1.

Розглянемо більш детально призначення кожного із блоків.

Потік даних з каналів зв'язку надходить до телекомунікаційного адаптеру (мережний додаток), основне завдання якого – це виділення з потоку даних окремих додатків і формування файлів (команд передачі управління) для обробки в програмному клієнті, а також безперешкодна передача метаданих у канал зв'язку телекомунікаційної мережі.

Програмний клієнт – модуль, розміщений на комп'ютері-клієнті, призначений для організації взаємодії апаратної і програмної (додатки) складових системи, подання підозрілих файлів у формувач метаданих, а також подання в зручному

ISSN 2663 - 4023

форматі (побудова таблиць, графіків, діаграм і ін.) результатів роботи хмарної антивірусної системи. Програмний клієнт функціонально пов'язаний з аналізатором файлів – пакетом програм, який призначено для здійснення попереднього сигнатурного і евристичного аналізу (порівняння із установленими еталонами, перевірка допустимості значень і ін.) на клієнтській частині системи.

Формувач метаданих призначений для виділення спеціальних сигнатур підозрілих файлів за допомогою сучасних засобів хешування файлів. Спеціальні сигнатури через описаний вище адаптер передаються в канал зв'язку телекомунікаційної мережі. Передача в телекомунікаційній мережі через проміжні вузли комутації (блок передачі метаданих) проходить в відповідності з відомими протоколами і вдосконаленими методами управління інформаційним трафіком.

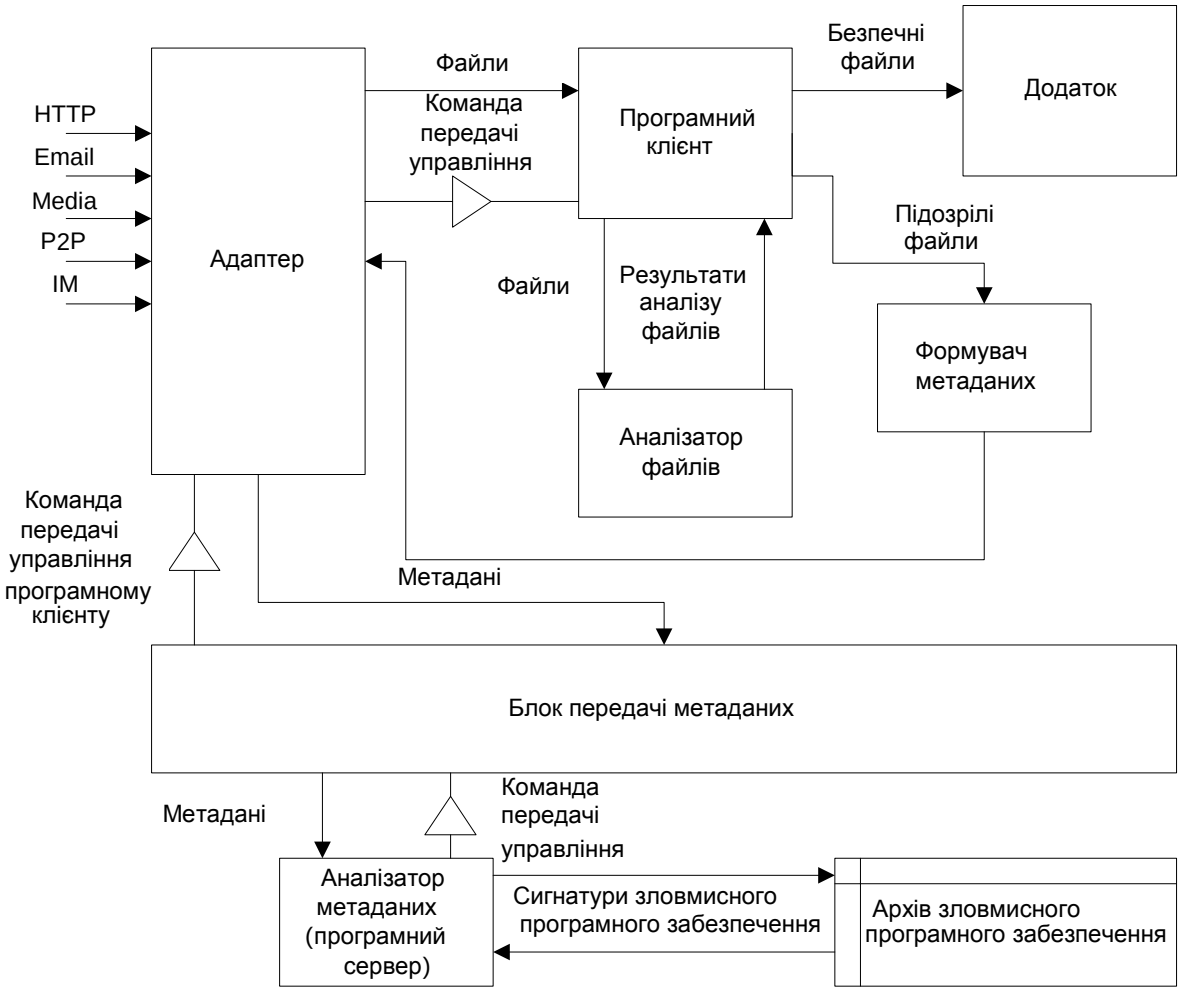


Рис. 1. Структурна схема технології хмарного антивірусного захисту

Аналізатор метаданих у хмарному антивірусі виявляє загрози і перевіряє якість ухвалених рішень на помилки, після чого шукає джерела поширення загроз. Знайдені джерела також проходять автоматичну контрольну перевірку – щоб виключити помилкові спрацьовування. Отримана за допомогою аналізатора інформація про загрози що щойно з'явилися і джерела їхнього поширення оперативно заноситься в

архів злочинного програмного забезпечення та стає доступною всім іншим користувачам продукту.

Інформація про зараження використовується для самонавчання аналізатора метаданих, внаслідок чого вона швидко реагує на новітні розробки зловмисників і в автоматичному режимі виявляє активні загрози на комп'ютерах користувачів. Інформація про зараження, що використовується для самонавчання включає, у тому числі, вердикти, отримані за допомогою сигнатурного і евристичного детектування.

Збираючи й обробляючи дані про підозрілу активність від кожного учасника мережі, хмарний захист являє собою потужну експертну систему, спрямовану на аналіз кіберкримінальної активності. Дані, необхідні для блокування атаки, якою був атакований комп'ютер будь-якого користувача, передаються всім учасникам хмарної мережі, що дозволяє запобігати наступним зараженням.

Проведені дослідження показали, що для реалізації багатокористувацьких розподілених додатків (якою і є хмарна антивірусна система) необхідно передбачити інтерфейс сокетів.

Сокети (*sockets* – "гнізда") – це один із способів передачі даних і обміну інформацією між комп'ютерами. Сокети є програмними кінцевими точками мережного з'єднання. Для роботи із сокетами необхідно використовувати деякий протокол на основі *TCP/IP* і програмний порт транспортного рівня *Windows*. Сокети діляться на три основних типи [3].

Клієнтські сокети ініціюють з'єднання з боку клієнта з серверним сокетом на віддаленій машині. Для того щоб відкрити з'єднання, клієнтський сокет повинен "знати" *IP*-адресу віддаленої машини та номер порту, що використовується серверним сокетом. Клієнт надсилає серверу запит на з'єднання. Серверні сокети самі не займаються встановленням зв'язку із клієнтськими сокетами. Це завдання виконують слухаючі сокети, які вбудовано в серверні сокети. Запит на підключення нового клієнта одержує слухаючий сокет, який ставить його в чергу. Після того, як серверний сокет звільниться від поточної роботи, він обробляє запит із черги та створює слухаючий сокет для нового з'єднання. Серверні сокети встановлюють з'єднання із клієнтським сокетом у відповідь на його запит. Клієнтський сокет отримує опис серверного сокету, після чого з'єднання вважається встановленим [3], [4].

Проведемо математичну формалізацію технології передачі і обробки метаданих у хмарних антивірусних системах і визначимо основні часові характеристики цих процесів.

1.3 ОЦІНКА ЧАСУ ОБРОБКИ МЕТАДАНИХ В АНАЛІЗАТОРІ ХМАРНИХ АНТИВІРУСНИХ СИСТЕМ

Час обробки метаданих в аналізаторі хмарних антивірусних систем (програмним сервером) визначимо шляхом знаходження суми випадкового числа незалежних випадкових величин $\xi_1, \xi_2 \ldots$ з тим самим розподілом F і виробляючою функцією моментів $M(s)$. Нехай N – цілочисельна випадкова величина з виробляючою функцією $\grave{A}(s) = \sum \mathrm{P}_i s^i$ і не залежна від усіх ξ_j. Тоді випадкова сума $\xi_1 + \ldots + \xi_N$ має розподіл, описуваний виробляючою функцією моментів

$$\chi(s) = W(M(s)), \qquad (1)$$

де $W(s)$ – виробляюча функція, що описує випадкове число елементів метаданих, які запитує програмний клієнт,

$M(s)$ – виробляюча функція моментів, що характеризує випадковий час обробки одного елементу метаданих.

Розглянемо метод розрахунку часу обробки при описі числа елементів метаданих, які зажадав програмний клієнт, рівномірним розподілом із цілочисельними значеннями. Число параметрів у завданні може змінюватися від h до ℓ. Виробляюча функція моментів цього розподілу з урахуванням того, що всі події вважаються рівноімовірними зі значенням $\overline{p}$, дорівнює

$$M(s)=\overline{p}\left(e^{hs}+e^{(h+1)s}+...+e^{(\ell-1)s}+e^{\ell s}\right)=\left(\overline{p}\left(e^{hs}-e^{(\ell+1)s}\right)\right)\Big/\left(1-e^{s}\right).$$

Виробляюча функція цього розподілу $W(s)=\left(\overline{p}(s^{h}-s^{(l+1)})\right)\Big/(1-s)$. Для оцінки випадкового часу обробки одного елемента метаданих використовуємо рівномірний безперервний розподіл з параметрами a й b. Тоді відповідно до (1) $\chi(s)$ можна обчислити як

$$\chi(s)=\overline{p}\left(\frac{\left(\frac{e^{as}-e^{bs}}{(a-b)s}\right)^{h}-\left(\frac{e^{as}-e^{bs}}{(a-b)s}\right)^{\ell+1}}{1-\frac{e^{as}-e^{bs}}{(a-b)s}}\right). \tag{2}$$

Диференціюючи $\chi(s)$ за змінною s і прирівнюючи в отриманих виразах величину s нулю, отримуємо перший μ_1 і другий μ_2 моменти відносно початку координат і, відповідно, середнє значення t_s і дисперсію D часу обробки одного елемента метаданих, що передано за запитом програмного клієнта.

$$\mu_1=t_{\tilde{n}\delta}^{(\hat{\imath})}=\left.\frac{\partial(\chi(s))}{\partial s}\right|_{s=0}=\frac{(h+\ell)(a+b)}{4}, \tag{3}$$

$$J^{(\hat{\imath})}=\mu_2-\mu_1^2=\left.\frac{\partial^2(\chi(s))}{\partial s^2}\right|_{s=0}-\left(\left.\frac{\partial(\chi(s))}{\partial s}\right|_{s=0}\right)^2=\frac{(h+\ell)(b-a)^2}{24}, \tag{4}$$

У випадку, коли аналізатор метаданих виконує обробку файлів різних, незалежних інформаційних потоків, кількість вимог програмного клієнта на формування, аналіз і обробку керуючих команд може бути описано розподілом Пуассона [5].

У цьому випадку виробляюча функція розподілу Пуассона дорівнює

$$W(s)=e^{\lambda s-\lambda}.$$

Звідси виробляюча функція моментів часу формування керуючих команд і виконання завдання програми-клієнта дорівнює

$$\chi(s)=e^{\left(-\lambda+\lambda\frac{e^{as}-e^{bs}}{(a-b)s}\right)}. \tag{5}$$

З виразу (5) знаходимо середній час виконання завдання формування керуючої команди і його дисперсію

$$t_{\tilde{n}\delta}^{(\hat{o})}=\frac{\lambda(a+b)}{2}, \tag{7}$$

ISSN 2663 - 4023

$$J^{(\hat{o})} = \frac{\lambda\left(a^2 + ab + b^2\right)}{3}. \qquad (8)$$

Проведемо аналіз взаємовпливу наведених в (2), (4) і (7), (8) часових характеристик на загальний час обробки метаданих і формування керуючих команд.

На рис.2 наведено графіки загального часу $t_{cp}(S)$ (графік 1) і часу обробки метаданих $t_{cp}^{(0)}(S)$ (графік 2) (рис. 2 а), а також графіки джиттера $D(S)$ загального часу (графік 1) і часу обробки метаданих $D^{(0)}(S)$ (графік 2) в умовах коли $a = 0{,}4$; $b = 0{,}7$; $h = 0{,}3$; $l = 1$; $\bar{p} = 0{,}3$; $\lambda = 1200$.

Із графіків видно, що врахування часових характеристик формування керуючих сигналів дозволить підвищити точність результатів оцінки часових характеристик в 1,7 разів, і характеристик джиттера в 4,5 рази.

Таким чином, розроблена і досліджена математична модель ТКС, що дозволяє оцінити часові характеристики обробки одного елемента метаданих і вироблення керуючої команди. Її відмінною рисою є врахування необхідності формування команд передачі управління програмному клієнтові ТКС, що в цілому підвищило точність результатів математичного моделювання в розглянутих умовах.

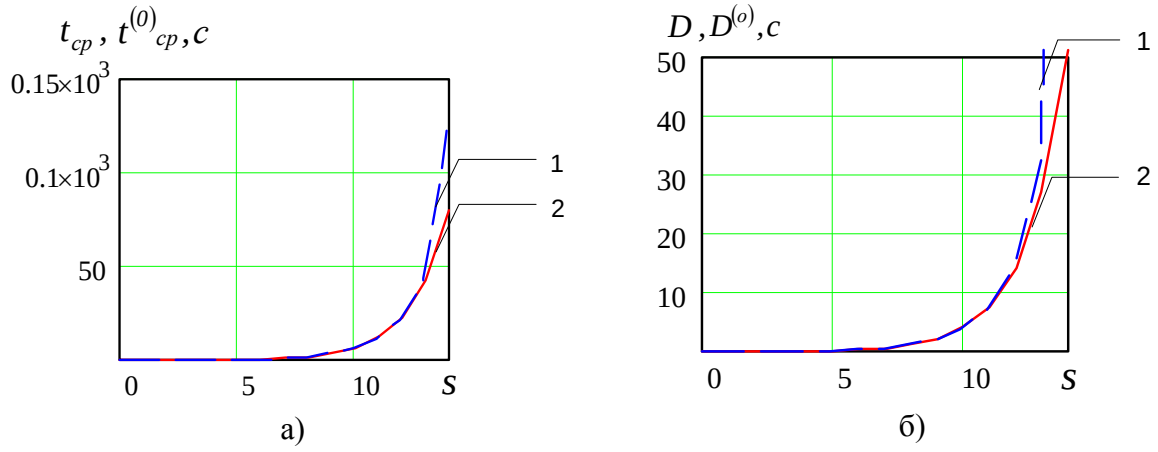


Рис.2 Графіки $t_{cp}(S)$ *і* $t_{cp}^{(0)}(S)$, $D(S)$ *і* $D^{(0)}(S)$

У більшості випадків щільність розподілу ймовірностей часу обробки одного елемента метаданих і вироблення керуючої команди має одну моду. Формули (2), (7) можна використовувати для попередньої оцінки величини розкидання розподілу на основі правила "трьох сигм". У той же час необхідність врахування факторів, наведених у підпункті 1.1 вимагає розробки більш складних моделей.

Для рішення даного завдання використовуємо графовий підхід *GERT*-структур. В якості аргументів доцільності такого підходу і адекватності отриманих результатів математичного моделювання приводять протестовані методи побудови *GERT*-мереж, а для складних технічних систем перевірені методики попередньої регуляризації складних *GERT*-структур. Наведені в роботах [1],[6]-[9] результати моделювання говорять про підвищення точності одержаних результатів до 10-15%.

ISSN 2663 - 4023

В умовах розглянутого в дисертаційній роботі прикладу, використання засобів *GERT*-моделювання дозволяє оптимізувати структуру системи створення, передачі і обробки метаданих, а також формування команд передачі управління, оцінити продуктивність і можливості її масштабування при збільшенні обсягу та складності вирішуваних завдань.

Тому для знаходження щільності розподілу ймовірностей часу обробки метаданих і вироблення керуючих команд $\varphi(\chi)$ далі будуть використані *GERT*-моделі.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

2.1 СТРУКТУРА ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ФОРМУВАННЯ, ПЕРЕДАЧІ І ОБРОБКИ МЕТАДАНИХ У ХМАРНИХ АНТИВІРУСНИХ СИСТЕМАХ

Розробка і використання сучасної високопродуктивної мікропроцесорної техніки, розвиток алгоритмів управління інформаційними потоками в ТКС, підвищений попит на хмарні технології в сукупності з великими ризиками, пов'язаними з можливістю зараження комп'ютерними вірусами визначають постійне збільшення інтенсивності передачі метаданих у хмарні антивірусні системи. При цьому виникають складності пов'язані з тим, що продуктивність і надійність каналів телекомунікаційних мереж досить складно підвищити, залишаючись у рамках схеми одного фізичного каналу. Для цього необхідно міняти протокол, а, можливо, і фізичний носій каналу, наприклад, переходити на оптоволокно із заміною портів комунікаційних пристроїв.

Підвищити продуктивність і надійність каналу можна за рахунок застосування надлишкових фізичних зв'язків. Одним із способів, що використовується на практиці є використання механізму агрегування зв'язків. Всі надлишкові зв'язки розглядаються в якості активних, і використовуються для підвищення, як надійності (у випадку дублювання даних), так і продуктивності за рахунок розподілу навантаження між каналами (прикладом може бути випадок багатошляхової маршрутизації в ТКС). Агреговані канали (надалі маршрути) або транки використовуються найчастіше в мережах *Fast Ethernet* і *Gigabit Ethernet* для підвищення продуктивності магістральних зв'язків [3], [4], [10], [11]. Комутатори *Ethernet* використовують техніку транкінгу для створення швидкісних магістральних зв'язків між комутаторами, а також для підвищення швидкості мережної роботи серверів. У загальному випадку використовуються механізми агрегування, що дозволяють об'єднати в один логічний канал, зв'язки різних швидкостей, протоколів і пристроїв. Тракт передачі інформації між вузлом-сервером (хмарним оброблювачем даних) і вузлами-клієнтами з використанням агрегованого маршруту показаний на рис.3

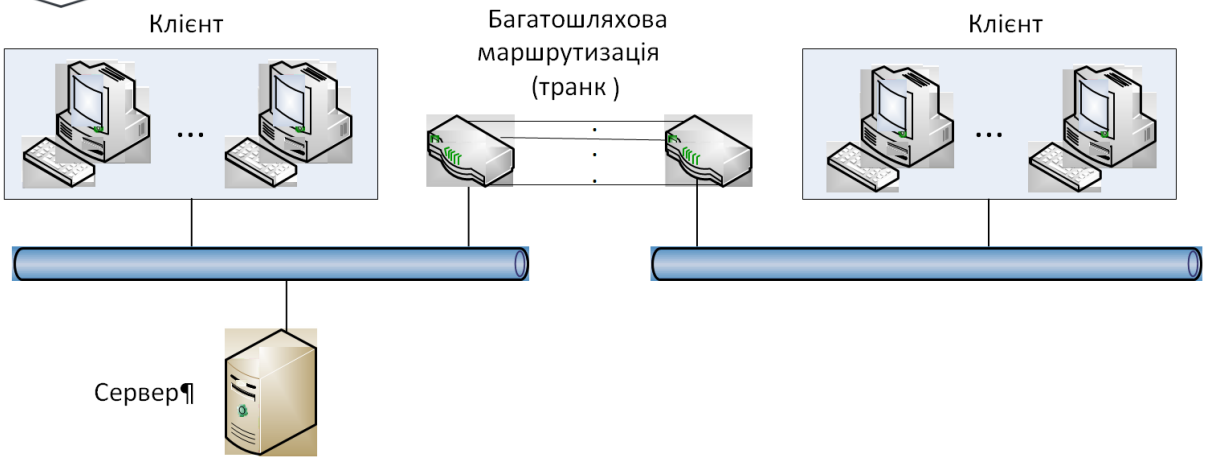


Рис. 3. Структура мережі передачі метаданих у хмарні оброблювачі даних

Аналіз відомих підходів математичного моделювання показав, що в цей час актуальним завданням є розробка математичних моделей і методів розрахунку ймовірносно-часових характеристик телекомунікаційних трактів, що складаються з множини агрегованих маршрутів, що з'єднують комутатори мережі (багатошляхової маршрутизації). Пов'язано це багато в чому з тим, що сучасні вузли зв'язку (маршрутизатори ТКС) можуть бути як безінерційними, так і ті, що вносять істотні затримки при обробці кадрів (пакетів) метаданих. У той же час варто враховувати, що алгоритми управління повинні гарантувати задані показники якості: середню швидкість передачі *CIR. (Committed Information Rate)*; кількість відхилень джиттера K_J, що відповідають середній швидкості *CIR* і періоду контролю Π. Відзначимо, що припустиме перевищення кількості відхилень джиттера:

$$K_{J\partial on} = CIR \cdot \Pi . \qquad (9)$$

Розробимо моделі агрегованих маршрутів у ТКС при передачі метаданих у хмарні антивірусні системи при наступних умовах:

– локальна ТКС має таку швидкодію, що часом передачі пакетів у її поділюваних сегментах можна зневажити;

– модель маршруту відбиває час передачі пакетів метаданих як безпосередньо в агрегованому маршруті, так і у вхідних і вихідних чергах вузлів зв'язку;

– модель враховує час формування команд передачі управління у відповідному аналізаторі (програмному сервері).

Формування множини маршрутів $\aleph_{\acute{a}\grave{a}\varsigma}$ для кожного вузла і являє собою ітераційний процес, що створює передумову мінімізації часу передачі метаданих і команд передачі управління програмному клієнтові.

Однак, незважаючи на достоїнства (використання множини шляхів передачі інформації, пропорційний розподіл потоку інформації по каналам зв'язку) такого підходу маршрутизації існує і ряд його недоліків, зокрема, відсутність врахування ймовірності спотворення інформації на базовій множині маршрутів, що росте зі збільшенням $\left|\aleph_{\acute{a}\grave{a}\varsigma}\right|$, і структурних особливостей обраних маршрутів. Для усунення зазначених недоліків необхідно знайти оптимальну множину маршрутів передачі метаданих і команд передачі управління (оптимальну топологію підмережі) у ТКС.

ISSN 2663 - 4023

Нехай для каналу $\tilde{n} \in \Im$ маршруту $s \in \aleph_{áàç}$ ймовірність спотворення одного біта дорівнює $q_s^{(c)}$, тобто ймовірність «неспотворення» біту дорівнює $p_s^{(c)} = 1 - q_s^{(c)}$. Тоді для пуассоновського потоку інформації інтенсивністю $\lambda \cdot \varphi_S$ з пакетом довжиною l_p, що проходить у с-му каналі зв'язку s-го маршруту за час Δt, імовірність «неспотворення» інформації дорівнює

$$p_s^{(c)}(\Delta t) = (1 - q_s^{(c)})^{\lambda \varphi_s l_p \Delta t}. \quad (10)$$

Відповідно імовірність $p_s(\Delta t)$ «неспотворення» інформації при передачі її по s-*му* маршруті за час Δt дорівнює

$$p_s(\Delta t) = \prod_{\tilde{N} \in \eta_s} (1 - q_s^{(c)})^{\lambda \varphi_s l_p \Delta t}, \quad (11)$$

тобто при передачі інформаційного потоку інтенсивністю λ з використанням багатошляхової маршрутизації на базовій множині $\aleph_{áàç}$ маршрутів імовірність $p(\aleph_{áàç}, \Delta t)$ «неспотворення» дорівнює

$$p(\aleph_{áàç}, \Delta t) = \prod_{s \in \aleph_{áàç}} \prod_{\tilde{n} \in \eta_s} (1 - q_s^{(c)})^{\lambda \varphi_s l_p \Delta t} \quad (12)$$

і, відповідно, імовірність $q(\aleph_{áàç}, \Delta t)$ спотворення за тих самих умов

$$q(\aleph_{áàç}, \Delta t) = 1 - \prod_{s \in \aleph_{áàç}} \prod_{\tilde{n} \in \eta_s} (1 - q_s^{(c)})^{\lambda \varphi_s l_p \Delta t} \quad . \quad (13)$$

Аналіз протоколів транспортного рівня *NGN*-мереж показав доцільність організації передачі метаданих у хмарні антивірусні системи і команд управління програмним клієнтам з квитуванням.

Дослідження відомих алгоритмів передачі даних показали, що в цей час існує три основні способи обробки відповідей на позитивні й негативні підтвердження:

– стартостопний, або передача із зупинкою і очікуванням (*SAW – Stop And Wait*), що часто називається блоковим методом передачі;

– з поверненням на *N* кадрів (*GBN – Go Back N*), що також називається потоковим методом передачі;

– метод вибіркового (селективного) повтору (*SR – Selective Repeat*).

Виходячи з логіки формування, передачі і обробки метаданих для рішення поставленого завдання хмарного антивірусного захисту ТКС видається доцільним використання алгоритму *SAW*.

Розробимо математичну модель для визначення ймовірносно-часових характеристик агрегованого маршруту і агрегованого з'єднання, яке складається з декількох послідовно з'єднаних каналів, для алгоритму передачі інформаційних пакетів *SAW*.

Розрахунок характеристик маршруту при паралельній роботі без обмеження спільності можна провести для випадку передачі файлу досить великої довжини ℓ. Переданий файл ділиться на деяке ціле число m інформаційних пакетів рівної довжини.

Кожний з *R* маршрутів передачі даних передає деяку кількість інформаційних пакетів із сумарними об'ємами $\lambda_1, \lambda_2, \ldots, \lambda_R, \lambda = \sum_{a-1}^{R} \lambda_a, \forall \lambda_a \rangle n$. Інформаційні пакети розміщуються у вихідних буферах передавального пристрою і надсилаються по

ISSN 2663 - 4023

множині маршрутів передачі даних. Після надходження всіх інформаційних пакетів у вхідні черги прийомного пристрою відбувається збирання файлу. Передбачається, що затримки на розбирання і збирання інформаційного пакета занадто малі і ними можна знехтувати, у порівнянні з часом його передачі по маршруту (каналу зв'язку).

Час передачі одного інформаційного пакету по маршруту *a* характеризується експоненціальним розподілом з параметром λ_a. Імовірність передачі інформаційного пакету через канал зв'язку без спотворень дорівнює p_a.

2.2 МАТЕМАТИЧНА МОДЕЛЬ ТЕХНОЛОГІЇ ПЕРЕДАЧІ МЕТАДАНИХ І КОМАНД ПЕРЕДАЧІ УПРАВЛІННЯ ЗА АГРЕГОВАНИМ МАРШРУТОМ ВІДПОВІДНО ДО АЛГОРИТМУ *SAW*

Проведені дослідження показали, що відповідно до протоколу обміну даними, в основу якого закладений алгоритм *SAW*, якщо кадр інформаційного пакету метаданих переданий без спотворень, то на передавальну сторону надсилається позитивна квитанція (*ACK*) і починається передача наступного кадру. Якщо кадр переданий невірно, то на передавальну сторону надсилається негативна квитанція (*NACK*).

При надходженні негативної квитанції кадр передається повторно доти, поки не буде переданий без спотворення. Число повторних передач за маршрутами обмежено, але його можна прийняти нескінченно великим, тому що для реальних каналів імовірність $1-p_a$ зазвичай мала й при збільшенні числа допустимих повторних передач β величина $(1-p_a)^{\beta}$ швидко прагне до 0. Тоді виробляюча функція моментів часу передачі кадру дорівнює $M_a(s)=\lambda_a p_a \big/ \lambda_a p_a - s$.

За маршрутом *a* передається m_a кадрів, тому виробляюча функція моментів часу його передачі за маршрутом $M_{Ea}(s)$ буде мати вигляд

$$M_{Ea}(s)=M^{m_a}(s)=\lambda_a^{m_a} p_a^{m_a} \big/ (\lambda_a p_a - s)^{m_a}. \quad (14)$$

Вираз (12) визначає виробляючу функцію моментів розподілу Ерланга порядку m_a з параметром $\lambda_a p_a$, щільністю:

$$\phi_a(\chi)=\lambda_a^{m_a} p_a^{m_a} \chi^{m_a-1} e(-\lambda_a p_a \chi)/(m_a-1) \quad (15)$$

і функцією розподілу:

$$F_a(\chi)=1-e^{-\lambda_a p_a \chi}\sum_{i=0}^{m_a-1}\frac{1}{(m_a-1-i)!}(\lambda_a p_a \chi)^{m_a-1-i}. \quad (16)$$

Для знаходження часу передачі метаданих у хмарні антивірусні системи і команд управління програмним клієнтам за агрегованим маршрутом скористаємося наступними допущеннями.

Якщо випадкові величини $\zeta_1,...,\zeta_n$ незалежні, то функція розподілу $F(y)$ часу передачі метаданих і команд управління за маршрутом, що складається з *R* логічних каналів визначається як добуток функцій розподілу окремих каналів

$$F(y)=\prod_{a=1}^{R} F_a(y). \quad (17)$$

ISSN 2663 - 4023

Функція розподілу часу передачі метаданих і команд управління для каналу a, $a \in \overline{1,R}$ за алгоритмом *SAW*

$$F_a(\chi) = 1 - e^{-\lambda_a p_a \chi} \sum_{i=1}^{m_a - 1} \frac{(\lambda_a p_a \chi)^{m_a - 1 - i}}{(m_a - 1 - i)}.$$

Звідси:

$$F(y) = \prod_{a=1}^{R} \left[1 - e^{-\lambda_a p_a \chi} \sum_{i=1}^{m_a - 1} \frac{(\lambda_a p_a \chi)^{m_a - 1 - i}}{(m_a - 1 - i)} \right].$$

Знаючи щільність розподілу часу передачі метаданих і команд управління за маршрутом $f(y)$, знайдемо його математичне очікування й дисперсію з виразів:

$$t_c^{(a)} = M(y) = \int_{-\infty}^{\infty} y f(y) dy, \quad \sigma_a^2 = D(y) = \int_{-\infty}^{\infty} (y - t_c^{(a)})^2 f(y) dy.$$

2.3 GERT-МОДЕЛЬ ТЕХНОЛОГІЇ ПЕРЕДАЧІ МЕТАДАНИХ І КОМАНД ПЕРЕДАЧІ УПРАВЛІННЯ ЗА АГРЕГОВАНИМ МАРШРУТОМ ВІДПОВІДНО ДО АЛГОРИТМУ SAW

Проілюструємо *GERT*-модель одного маршруту при використанні стартостопного методу передачі *SAW*. На рис. 4 наведена стохастична *GERT*-модель одного маршруту в режимі стартостопної передачі метаданих у хмарні антивірусні системи.

Дуга W_{12} відбиває процес передачі інформаційного пакета від формувача до аналізатора метаданих (див. рис. 1), де на транспортному рівні виконується аналіз правильності передачі інформаційного пакета і формувачу відправляється або квитанція з підтвердженням правильності передачі (дуга W_{23}, імовірність виконання $1 - p$), або їй відправляється негативна квитанція (дуга W_{21} з імовірністю p).

Дуга W_{34} відбиває процес формування команд передачі управління програмному клієнтові ТКС. Дуга W_{45} відбиває процес доставки команд передачі управління.

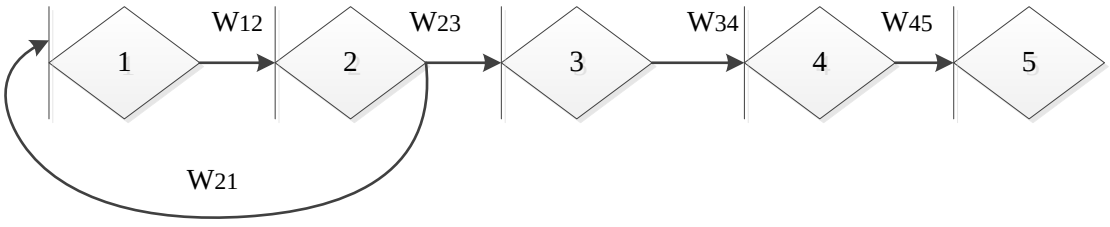


Рис. 4. Стохастична GERT-модель одного маршруту в режимі стартостопної передачі метаданих у хмарні антивірусні системи

Нехай розмір повідомлення метаданих n, що піддається антивірусному аналізу дорівнює розміру інформаційного пакета метаданих, переданого за маршрутом. Тоді виробляючі функції моментів часу передачі інформаційного пакета метаданих $M_{12}(s)$,

ISSN 2663 - 4023

часу передачі позитивної $M_{23}(s)$ і негативної квитанції $M_{21}(s)$, формування команд передачі управління програмному клієнтові ТКС $M_{34}(s)$ рівні відповідно:

$$M_{12}(s) = e^{sT_{12}},$$
$$M_{23}(s) = e^{sT_{23}},$$
$$M_{21}(s) = e^{sT_{21}},$$
$$M_{34}(s) = e^{sT_{34}},$$
$$M_{45}(s) = e^{sT_{45}},$$

де $T_{12} = n_1 / \upsilon_1$ – час передачі інформаційного пакета метаданих;

$T_{23} = T_{21} = n_1 / \upsilon_1$ – час передачі квитанції відповідно до протоколу транспортного рівня;

$T_{34} = n / \upsilon_2$ – час формування команд передачі управління програмному клієнтові ТКС;

$T_{45} = T_{12} = n / \upsilon_1$ – час доставки команди передачі управління програмному клієнтові,

n – довжина переданого за маршрутом інформаційного пакету;

n_1 – довжина переданої за зворотнім маршрутом квитанції;

υ_1 – теоретична швидкість передачі інформаційного пакету метаданих;

υ_2 – теоретична швидкість формування команд передачі управління програмному клієнтові.

У цьому випадку характеристики гілок і параметри розподілу можна звести до вигляду табл. 1.

Відповідно до алгоритмів визначення еквівалентних W-функцій $W_E(s)$, які описані в роботах [1],[6]-[9] , знайдемо еквівалентну W-функцію $W_E(s)$ стохастичної моделі для одного маршруту передачі метаданих:

$$W_E(s) = \frac{W_{12}W_{23}W_{34}W_{45}}{1 - W_{12}W_{21}} = \frac{(1-p)2e^{sT_{12}}e^{sT_{23}}e^{sT_{34}}}{1 - pe^{sT_{12}}e^{sT_{21}}} = \frac{qe^{sT_E^{(1)}}}{1 - pe^{sT_E^{(2)}}}, \qquad (18)$$

де $q = 1 - p$;

$$T_E^{(1)} = \frac{\upsilon_2(2n + n_1) + \upsilon_1 n}{\upsilon_1\upsilon_2};$$

$$T_E^{(2)} = \frac{n + n_1}{\upsilon_1}.$$

ISSN 2663 - 4023

Таблиця 1

Характеристики гілок *GERT*-моделі технології передачі і обробки інформаційних пакетів метаданих за агрегованим маршрутом відповідно до алгоритму *SAW*

№ п/п	Гілка	*W-Функція*	Імовірність	Виробляюча функція моментів
1.	*(1,2)*	W_{12}	*1*	$e^{sT_{12}}$
2.	*(2,1)*	W_{21}	*p*	$e^{sT_{21}}$
3.	*(2,3)*	W_{23}	*1-p*	$e^{sT_{23}}$
4.	*(3,4)*	W_{34}	*1*	$e^{sT_{34}}$
5.	*(4,5)*	W_{45}	*1*	$e^{sT_{45}}$

Виконуючи ділення чисельника на знаменник, отримуємо:

$$W_E(s) = qe^{sT_E^{(3)}} + qpe^{2sT_E^{(3)}} + qp^2e^{3sT_E^{(3)}} + ..., \qquad (19)$$

де $T_E^{(3)} = \dfrac{(\upsilon_2 + \upsilon_1)n}{\upsilon_1\upsilon_2}$.

Вираз (15) описує дискретний розподіл з ймовірностями qp^i в точках $T_E^{(3)}$, $2T_E^{(3)}$, $3T_E^{(3)}$... .

Для знаходження середнього часу передачі (формування) метаданих і команд передачі управління за одним маршрутом і його дисперсії σ^2 визначимо вираз для першого μ_1 і другого μ_2 моментів $W_E(s)$ відносно початку координат.

$$t_c = \mu_1 = \frac{\partial W_E(s)}{\partial s}\bigg|_{s=0} = qT_E^{(3)}\left(1 + 2p + 3p^2 + 4p^3 + ...\right) =$$

$$= qT_E^{(3)} \cdot \frac{\partial}{\partial p}\left(1 + p + p^2 + p^3 + ... - 1\right) = qT_E^{(3)} \cdot \frac{\partial}{\partial p}\left(\frac{1}{1-p} - 1\right) = \frac{T_E^{(3)}}{q},$$

$$\mu_2 = \frac{\partial^2 W_E(s)}{\partial s^2}\Big|_{s=0} = \frac{T_E^{(3)^2}}{q^2}(1 + 2p)$$

$$\sigma^2 = \mu_2 - \mu_1^2 = \frac{2T_E^{(3)^2}}{q^2}p^2$$

Однак, як було зазначено вище гетерогенність і багатозв'язковість сучасних ТКС вимагає врахування можливості використання агрегованих маршрутів при математичному моделюванні. Тому знайдемо аналітичні вирази для оцінки випадкового часу передачі метаданих у хмарні антивірусні системи і команд передачі управління за агрегованим маршрутом.

Еквівалентну W -функцію i -го маршруту можна записати як вираз:

$$W_E^{(i)}(s) = p_1^{(i)}e^{sT_{E1}^{(i)}} + p_2^{(i)}e^{sT_{E2}^{(i)}} + p_3^{(i)}e^{sT_{E3}^{(i)}} + ... ,$$

де $T_{E1}^{(i)}, T_{E2}^{(i)}, T_{E3}^{(i)}$ ... – моменти часу закінчення передачі, формування, а також доставки команд передачі управління програмному клієнтові ТКС; $p_1^{(i)}$, $p_2^{(i)}$, $p_3^{(i)}$ ... – ймовірності цих подій.

Алгоритм знаходження щільності розподілу часу, необхідного на передачу метаданих, а також формування і доставку команд управління програмному клієнтові за агрегованим маршрутом є ітераційним.

На першому кроці алгоритму знаходимо щільність імовірності часу передачі метаданих найбільш повільного із перших двох за порядком маршрутів. Отримана щільність характеризує нову випадкову величину, що разом з випадковим часом передачі по третьому за порядком маршрутом знову утворить пари величин, для яких шукається щільність розподілу максимальної із двох випадкових величин і так далі.

Розглянемо W-функції $W_E^{(1)}(s), W_E^{(2)}(s)$, пари випадкових величин, що характеризують час передачі метаданих і команд передачі управління за першим і другим маршрутами відповідно

$$W_E^{(1)}(s) = p_1^{(1)} e^{sT_{E1}^{(1)}} + p_2^{(1)} e^{sT_{E2}^{(1)}} + p_3^{(1)} e^{sT_{E3}^{(1)}} + ... + p_m^{(1)} e^{sT_{Em}^{(1)}},$$

$$W_E^{(2)}(s) = p_1^{(2)} e^{sT_{E1}^{(2)}} + p_2^{(2)} e^{sT_{E2}^{(2)}} + p_3^{(2)} e^{sT_{E3}^{(2)}} + ... + p_k^{(2)} e^{sT_E^{(2)}}.$$

Нехай p_i і p_j ймовірності дискретних розподілів, що характеризують час передачі метаданих і команд передачі управління за першим і другим маршрутом відповідно. Тоді для $\forall\left(i=\overline{1,m}\right);\ \left(j=\overline{1,k}\right)$ знаходимо $p_y = p_i p_j$, $y = \max\{i, j\}$, , де p_y – імовірність дискретного розподілу максимальної із двох випадкових величин.

Тому що алгоритм ітераційний, то ймовірності p_y в загальному випадку задають розподіл декількох випадкових величин. Якщо маршрут y не останній, то додається маршрут $y+1$, і знову знаходиться розподіл максимальної з декількох випадкових величин і так далі. Процедури повторюються доти, поки не буде врахований вплив на загальний час передачі метаданих і команд передачі управління всіх складових маршрутів.

У цьому випадку еквівалентна W-функція часу передачі метаданих у хмарні антивірусні системи, формування і доставки команд передачі управління програмному клієнтові за агрегованим маршрутом дорівнює

$$W_E^{(a)}(s) = p_1 e^{sT_{E1}} + p_2 e^{sT_{E2}} + p_3 e^{sT_{E3}} + ... + p_\beta e^{sT_{E\beta}}, \qquad (20)$$

де β – число значень розподілу.

Середній час і дисперсія часу передачі метаданих, формування і доставки команд передачі управління відповідають виразам:

$$t_c^{(a)} = \left.\frac{\partial W_E(s)}{\partial s}\right|_{s=0} = \sum_{i=1}^{\gamma} p_i T_i,$$

$$\sigma^{(a)2} = \left.\frac{\partial^2 W_E(s)}{\partial s^2}\right|_{s=0} - \left(\left.\frac{\partial W_E(s)}{\partial s}\right|_{s=0}\right)^2 = \sum_{i=1}^{\gamma} p_i T_i^2 - \sum_{i=1}^{\gamma} p_i T_i,$$

де T_i – значення розподілу;

p_i – імовірності подій;

γ – число логічних каналів.

Якщо $\overline{W_E^{(a)}(S)}$ – еквівалентна W-функція ланцюжка послідовних каналів на маршруті, то

$$\overline{W_E^{(a)}}(s) = \prod_{i=1}^{Y} W_{E_Y}^{(a)}(s), \qquad (21)$$

де Y – число послідовно прохідних повідомленням метаданих і команди передачі управління агрегованих каналів. Щільність розподілу часу проходження цієї послідовності каналів, очевидно, являє собою дискретний розподіл. Значення ймовірностей знаходяться шляхом множення рядів, кожний з яких визначається одним з виразів типу (20).

Знайдемо першу і другу похідні еквівалентної W-функція часу передачі метаданих у хмарні антивірусні системи, формування і доставки команд передачі управління програмному клієнтові за агрегованим маршрутом та проведемо дослідження залежності тимчасових характеристик від імовірності передачі негативної квитанції про доставку інформаційних пакетів при умовах коли: імовірності передачі позитивної і негативної квитанцій обчислюються відповідно до виразів (10)-(12), $\upsilon_2 = 56\,Гфлопс$, $\upsilon_1 = 10Мá/с, 12Мá/с, ..., 20Мá/с$, $\beta = 1,2,...,5$.

На рис. 5 наведені графіки залежності середнього часу і дисперсії передачі метаданих та формування і доставки команд передачі управління від імовірності передачі негативної квитанції про доставку інформаційних пакетів.

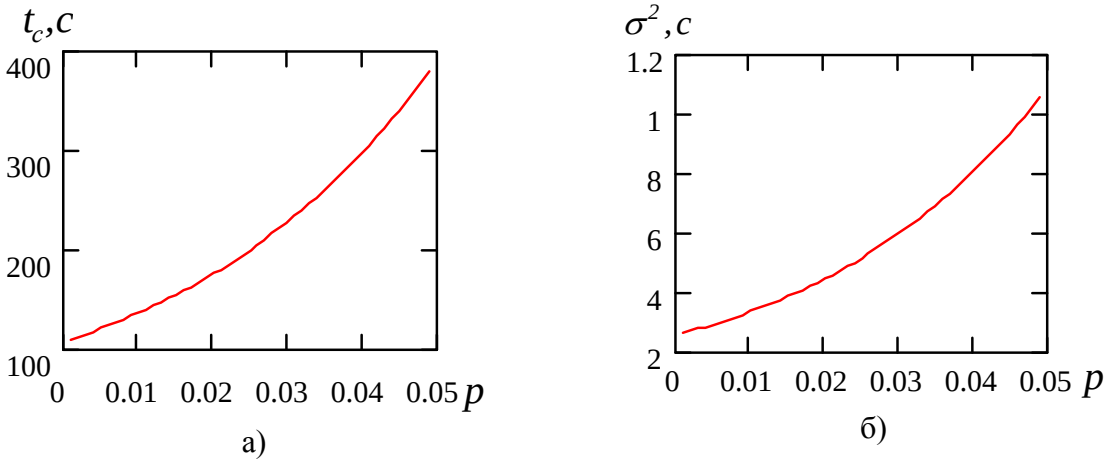


Рис. 5. Графіки залежності t_c і σ^2 від імовірності p

Як видно з рисунків ріст імовірності передачі негативної квитанції про доставку інформаційних пакетів приводить до значного (в 4 рази) збільшення часу t_c. Це підтверджує необхідність використання додаткових механізмів захисту і поліпшення якості каналів зв'язку на маршрутах.

У розглянутій моделі як допущення було визначено, що довжина повідомлення метаданих не перевищує розміру інформаційного пакета, визначеного технологією передачі даних. Однак на практиці гетерогенність технологій канального рівня має на увазі можливі зміни розмірів інформаційних пакетів на шляху проходження за маршрутом. Цей фактор доцільно врахувати і при розробці *GERT*-моделі технології передачі метаданих і команд передачі управління за агрегованим маршрутом. Для

рішення цього завдання розробимо *GERT*-модель технології передачі і обробки геш-файлу метаданих.

Таким чином, розроблена математична *GERT*-модель технології передачі метаданих і команд передачі управління за агрегованим маршрутом відповідно до алгоритму *SAW*, що відрізняється від відомих врахуванням багатозв'язковості (багатошляхової маршрутизації) ТКС.

Поява в комп'ютерних мережах нових видів даних, таких як *Ip*-телефонія, потокове аудіо і відео та інші мультимедійні додатки, файли обміну із хмарними ресурсами обумовило появу нових вимог, пов'язаних із забезпеченням мінімальних затримок інформаційних пакетів (кадрів) і їх джиттера. Як основні критерії класифікації потоку даних у комп'ютерних мережах обрані три його характеристики: відносна передбачуваність швидкості передачі даних, чутливість до затримок пакетів, чутливість даних до втрат і спотворень пакетів.

2.4 GERT-МОДЕЛЬ ТЕХНОЛОГІЇ ПЕРЕДАЧІ ГЕШ-ФАЙЛУ МЕТАДАНИХ І КОМАНД ПЕРЕДАЧІ УПРАВЛІННЯ

Одним з найбільш складних режимів передачі даних є передача спеціальних сигнатур і компресованих файлів у реальному часі. Причиною цього, зокрема, є необхідність передачі хешованої (зашифрованої) інформації в режимі діалогу. Хешована (стисла) і зашифрована інформація із чутливості даних до затримок пакетів характеризується як ізохронна або надчуттєва. Ізохронні додатки при перевищенні порогу чутливості різко знижують свою функціональність, а надчуттєві перестають функціонувати. Для кадрів таких даних виключається можливість втрати фрагментів і будь-яке спотворення інформації. Додатковою вимогою є забезпечення мінімальних необхідних витрат.

Скористаємося розробленою і описаною узагальненою *GERT*-моделлю технології передачі і обробки інформаційних пакетів метаданих за агрегованим маршрутом відповідно до алгоритму *SAW* для опису процесу передачі і обробки геш-файлу метаданих через агрегований канал. При цьому визначимо наступні допущення:

– ізохронний або надчуттєвий до затримок і чутливий до втрат геш-файл має вищий пріоритет у черзі комутатора або маршрутизатора;

– геш-файл може містити від одного до n кадрів. Число кадрів у файлі випадкове й задається дискретним розподілом з імовірностями $p_1^{(k)}, p_2^{(k)},..., p_n^{(k)}$;

– час передачі кадру описується експоненціальним розподілом з параметром λ;

– імовірність передачі кадру через канал зв'язку без спотворень дорівнюють *p*. Кадри передаються в старт-стопному режимі відповідно до алгоритму *SAW* з допущенням про нескінченність можливих повторних передач кадру у випадку спотворень (тому що величина 1-p зазвичай невелика, і при збільшенні числа допустимих повторних передач r значення $(1-p)^{\gamma}$ швидко прагне до нуля. Таким чином, при збільшенні r ациклічна модель на межі швидко сходиться до циклічної;

– при використанні додаткових фінансових витрат с якість каналу зв'язку можна підвищити, і кількісною характеристикою цього буде збільшення значення параметра *p*. Аналіз літератури [12],[1],[6]-[9],[13] показав, що функціональна залежність між цими величинами $p = f(c)$ відома. Найпоширенішої є версія, коли така залежність описується експоненціальним законом: $p = 1 - e^{(-\gamma c)}$, де γ – коефіцієнт, що задається

ISSN 2663 - 4023

користувачем. У вихідному стані якість каналу зв'язку характеризується величиною p_0. Збільшення значення p відповідає підвищенню якості каналу зв'язку, і відповідно збільшення витрат. Зменшення значення p відповідає погіршенню якості роботи каналу і можливій втраті матеріальних (фінансових) або інших засобів.

Процес передачі геш-файлу метаданих може бути описаний удосконаленою *GERT*-моделлю, яку зображено на рис. 6.

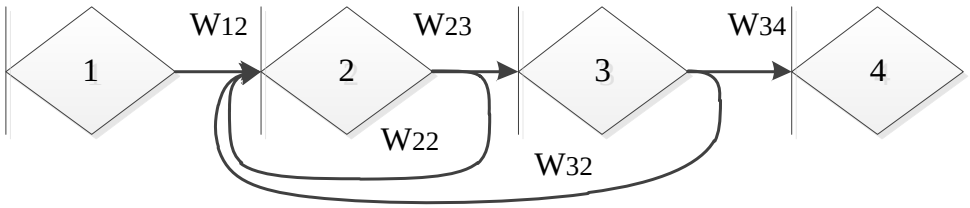


Рис. 6.GERT-модель технології передачі і обробки геш-файлу метаданих

У наведеній моделі гілка W_{12} характеризує сукупні постійні затримки передачі геш-файлу в каналі зв'язку. Гілка W_{23} відбиває операцію передачі кадру геш-файлу без спотворень і посилку позитивної квитанції. Гілка W_{22} відповідно описує операцію передачі кадру і посилку негативної квитанції. Гілка W_{32} відбиває поетапність процесу передачі декількох кадрів геш-файлу метаданих. Гілка W_{34} характеризує сукупні постійні затримки обробки передачі команд управління програмному клієнтові.

Характеристики гілок *GERT*- моделі технології передачі геш-файлу метаданих, а також обробки і доставки команд передачі управління наведені в табл. 2.

Таблиця 2

Характеристики гілок *GERT*-моделі технології передачі і обробки геш-файлу метаданих, а також команд передачі управління

№ п/п	Гілка	*W-Функція*	Імовірність	Виробляюча функція моментів
1.	*(1,2)*	W_{12}	*1*	$e^{s\tau}$
2.	*(2,2)*	W_{22}	*1-p*	$(1-p)\lambda/\lambda - s$
3.	*(2,3)*	W_{23}	*p*	$p\lambda/\lambda - s$
4.	*(3,2)*	W_{32}	*1*	*1*
5.	*(3,4)*	W_{34}	*1*	$e^{s\tau}$

ISSN 2663 - 4023

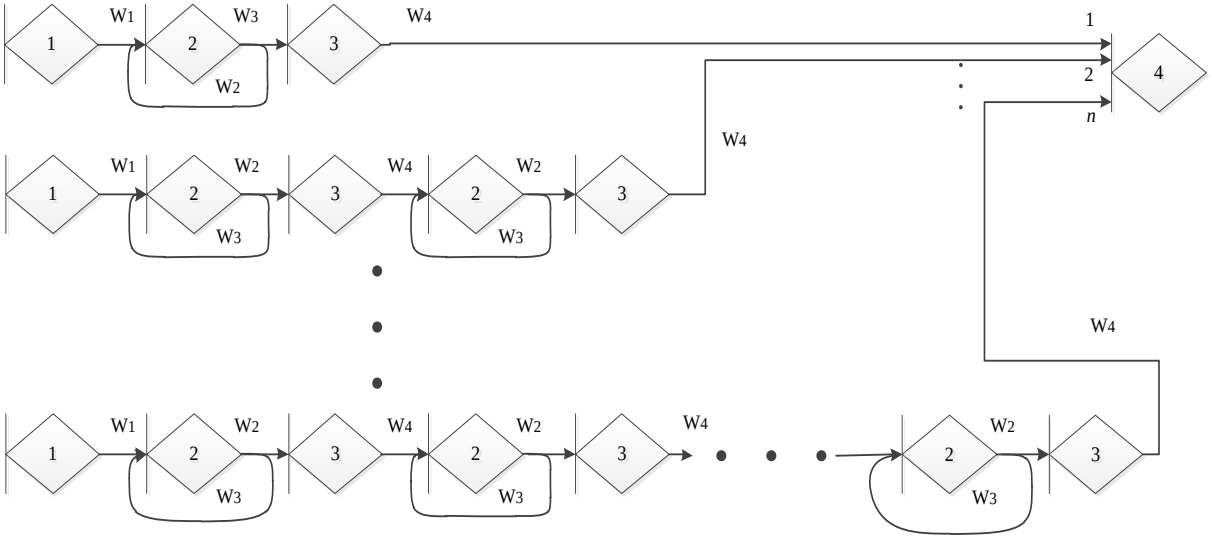


Рис. 7.GERT-модель процесу передачі і обробки геш-файлу метаданих, а також команд передачі управління при довільному n

GERT-модель процесу передачі геш-файлу метаданих і команд передачі управління при довільному n зображена на рис. 7. Її еквівалентна W -функція $W_E(s)$ визначається виразом:

$$W_E(s) = W_1 W_4 \left(\frac{W_3}{1-W_2} + \frac{W_3^{\,2}}{(1-W_2)^2} + \frac{W_3^{\,3}}{(1-W_2)^3} + \ldots + \frac{W_3^{\,n}}{(1-W_2)^n} \right). \qquad (22)$$

Підставляючи у формулу (22) дані з табл. 2, отримуємо:

$$W_E(s) = \left(e^{s\tau}\right)^2 \times$$
$$\times \left(p_1^{(k)} \frac{\lambda p}{\lambda p - s} + p_2^{(k)} \frac{(\lambda p)^2}{(\lambda p - s)^2} + p_3^{(k)} \frac{(\lambda p)^3}{(\lambda p - s)^3} + \ldots + p_n^{(k)} \frac{(\lambda p)^n}{(\lambda p - s)^n} \right) = \qquad (23)$$
$$= \sum_{i=1}^{n} p_i^{(k)} \left(e^{s\tau}\right)^2 \frac{(\lambda p)^i}{(\lambda p - s)^i}.$$

Для знаходження щільності розподілу ймовірностей часу передачі і обробки геш-файлу метаданих, а також команд передачі управління в хмарні антивірусні системи $\varphi(\chi)$ виконаємо перетворення змінних $z = -s$. Тоді функція $W_E(s)$ перетвориться в комплексну функцію $F(z)$, а значення

$$\varphi(\chi) = \sum_{r=1^{z=z}}^{n} \operatorname{Re} s\left(e^{zx} F(z)\right) = \frac{1}{2\pi i} \int_{-i\infty}^{i\infty} e^{zx} \sum_{i=1}^{n} p_i^{(k)} \left(e^{-z\tau}\right)^2 \frac{(\lambda p)^i}{(\lambda p + z)^i} dz \,. \qquad (24)$$

Функція $F(z)$ повинна мати полюси, що лежать лівіше уявної осі, і задовольняти умовам леми Жордана [14]. Для того, щоб виконувалися умови леми Жордана, необхідно, щоб у лівій напівплощині функція $F(z)$ була аналітичної за винятком кінцевого числа полюсів і прагнула до нуля при $|z| \to \infty$ рівномірно відносно *arg z*. З виразу (20) видно, що умови леми Жордана виконуються [1].

ISSN 2663 - 4023

Для знаходження щільності $\varphi(\chi)$ потрібно знайти суму відрахувань функції $e^{zx}F(z)$ щодо всіх особливих точок. Функція $e^{zx}F(z)$ має n особливих точок – полюсів порядків 1,2,..., n в точці $z_0 = -\lambda p$.

З урахуванням вищевказаного

$$\varphi(\chi) = \sum_{z=z_0} \operatorname{Res}\left(e^{zx}F(z)\right) = \frac{1}{(n-1)!}\lim_{z\to z_0}\frac{d^{n-1}(z-z_0)^n e^{zx}F(z)}{dz^{n-1}}.$$

Виходячи з того, що $F(z) = \sum_{i=1}^{n} F_i(z) = \sum_{i=1}^{n} p_i^{(k)}\left(e^{-z\tau}\right)^2 \frac{(\lambda p)^i}{(\lambda p + z)^i}$, можна знайти відрахування від функції $e^{zx}F(z)$:

$$\operatorname*{Res}_{z=z_0}\left(e^{zx}F_i(z)\right) = \frac{1}{(i-1)!}\lim_{z\to z_0}\frac{d^{i-1}(z-z_0)^i e^{zx}F_i(z)}{dz^{i-1}} =$$

$$= \frac{1}{(i-1)!}\lim_{z\to z_0}\frac{d^{i-1}\left(p_i^{(k)}\left(e^{z(\chi-\tau)}\right)^2(\lambda p)^i\right)}{dz^{i-1}} = \frac{p_i^{(k)}(\lambda p)^i}{(i-1)!}(\chi-\tau)^{i-1}\left(e^{-\lambda p(\chi-\tau)}\right)^2$$

Знаходячи суму відрахувань щодо всіх особливих точок, отримуємо щільність:

$$\varphi(\chi) = \left(e^{-\lambda p(\chi-\tau)}\right)^2 \sum_{i=1}^{n}\frac{p_i^{(k)}(\lambda p)^i}{(i-1)!}(\chi-\tau)^{i-1},$$

де $\chi > \tau$.

На рис 8. наведено графік щільності розподілу ймовірностей часу передачі геш-файлу метаданих у хмарні антивірусні системи, а також обробки і доставки команд передачі управління.

Як видно із цього графіка максимальні значення щільності розподілу часу передачі геш-файлу метаданих у хмарні антивірусні системи, а також обробки і доставки команд передачі управління припадає на проміжок від 1 до 2 мс.

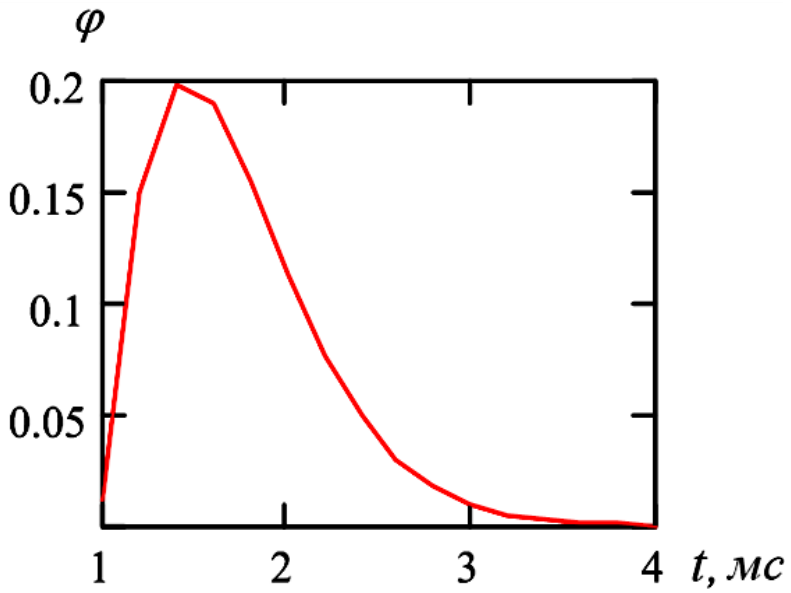


Рис. 8 Щільність розподілу ймовірностей часу передачі геш-файлу метаданих у хмарні антивірусні системи, а також обробки і доставки команд передачі управління

ISSN 2663 - 4023

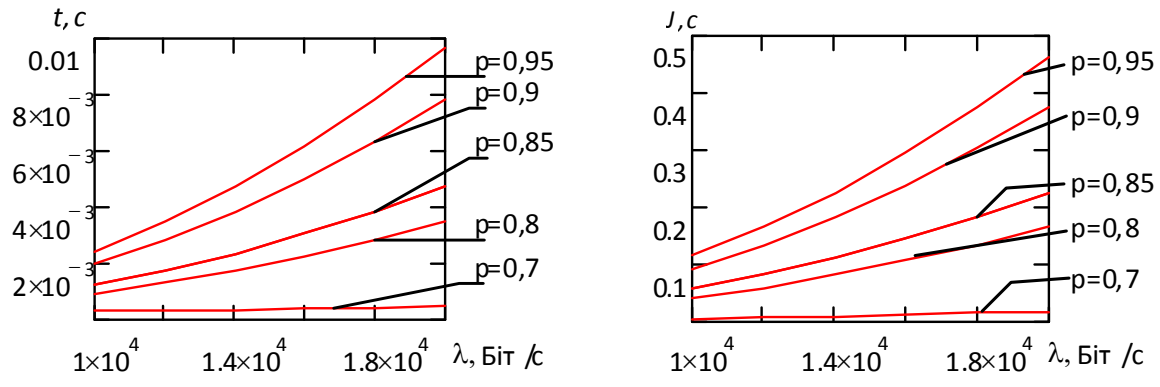
Диференціюючи вираз (19) за змінною s, знайдемо показники середнього часу передачі геш-файлу метаданих і відповідно джиттера затримки:

$$t_c = \left.\frac{\partial W_{\acute{y}}(s)}{\partial s}\right|_{s=0} = \frac{2p_1^{(k)}(\lambda p\tau+1)+2p_2^{(k)}(\lambda^2 p^2\tau+2)+\ldots+2p_n^{(k)}(\lambda^n p^n\tau+n)}{\lambda p} = \sum_{i=1}^{n} 2p_i^{(k)}\frac{((\lambda p)^i\tau+i)}{\lambda p}. \quad (25)$$

$$J = \left.\frac{\partial^2 W_{\acute{y}}(s)}{\partial s^2}\right|_{s=0} - \left(\left.\frac{\partial W_{\acute{y}}(s)}{\partial s}\right|_{s=0}\right)^2 = \frac{\left[\begin{array}{l} p_1^{(k)}((2\lambda p\tau)^2+4\lambda p\tau+2)+p_2^{(k)}((2\lambda p\tau)^2+8\lambda p\tau+6)+ \\ +p_3^{(k)}((2\lambda p\tau)^2+12\lambda p\tau+12)+\ldots+p_n^{(k)}((2\lambda p\tau)^2+4n\lambda p\tau+(n^2+n)) \end{array}\right]}{(\lambda p)^2} - \left(\frac{2p_1^{(k)}(\lambda p\tau+1)+2p_2^{(k)}(\lambda^2 p^2\tau+2)+\ldots+2p_n^{(k)}(\lambda^n p^n\tau+n)}{\lambda p}\right)^2 = \frac{\sum_{i=1}^{n} p_i^{(k)}((2\lambda p\tau)^2+4i\lambda p\tau+(i^2+i))-\sum_{i=1}^{n}(2p_i^{(k)}((\lambda p)^i\tau+i))^2}{(\lambda p)^2}. \quad (26)$$

Досліджуємо залежність тимчасових характеристик розробленої *GERT*-моделі від параметра λ (може розглядатися як інтенсивність інформаційного потоку) і ймовірності p.

На рис. 9 наведені графіки залежності середнього часу передачі геш-файлу метаданих у хмарні антивірусні системи, а також обробки і доставки команд передачі управління та джиттера затримки від параметра λ і імовірності p, отримані за умови, що $n=4$ $p_i^{(k)}=0.1\times10^{-3}, 0.2\times10^{-3},\ldots,0.4\times10^{-3}$, $\tau=0.3\times10^{-3}$.



а) б)

Рис. 9. Графіки залежності t_c і J від параметра λ і імовірності p

ISSN 2663 - 4023

Як видно із графіків збільшення λ в 2 рази спричиняє збільшення середнього часу передачі геш-файлу метаданих в 2,9 разів, а ріст імовірності передачі негативних квитанцій (що відповідає погіршенню каналів зв'язку) в 5 разів спричиняє збільшення показника t_c в 19 разів.

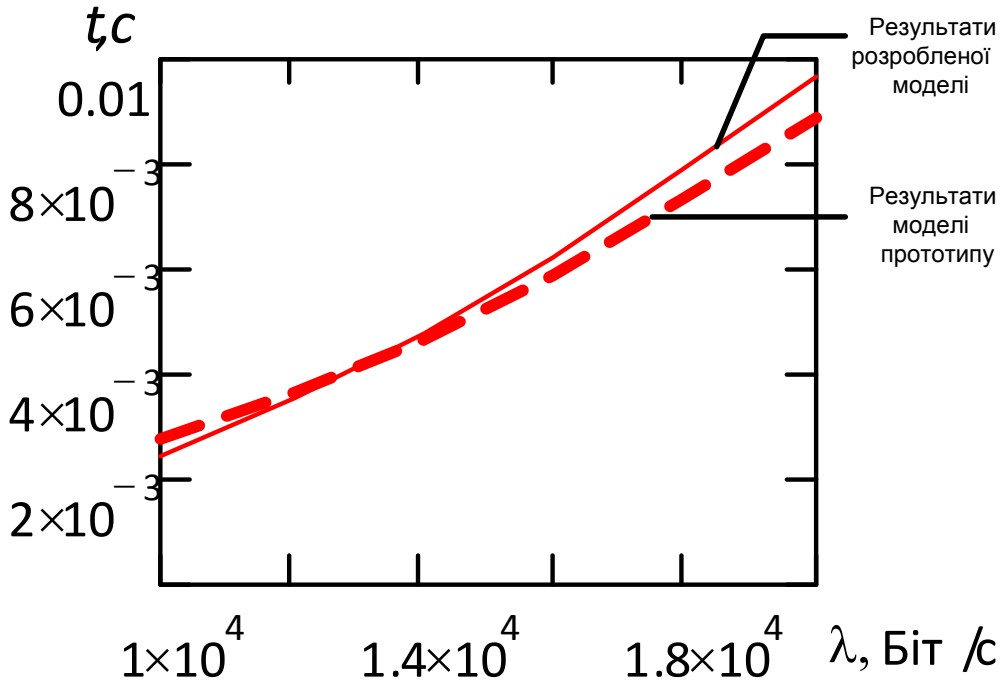
Аналогічну тенденцію можна спостерігати й при оцінці показника джиттера середнього часу затримки: при збільшенні λ в 2 рази джиттер збільшується в 4 рази, а ймовірності передачі негативних квитанцій в 5 разів джиттер збільшується в 24 рази.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Проведемо порівняльні дослідження розробленої математичної моделі технології хмарного антивірусного захисту ТКС. Для такого дослідження і відповідно оцінки в якості еталонної виберемо математичну модель технології передачі даних у процесі інформаційного обміну спеціалізованими сигнатурами із хмарними антивірусними системами на основі *GERT*-мережі, наведену в роботах [1], [6]-[9], [13], [15].

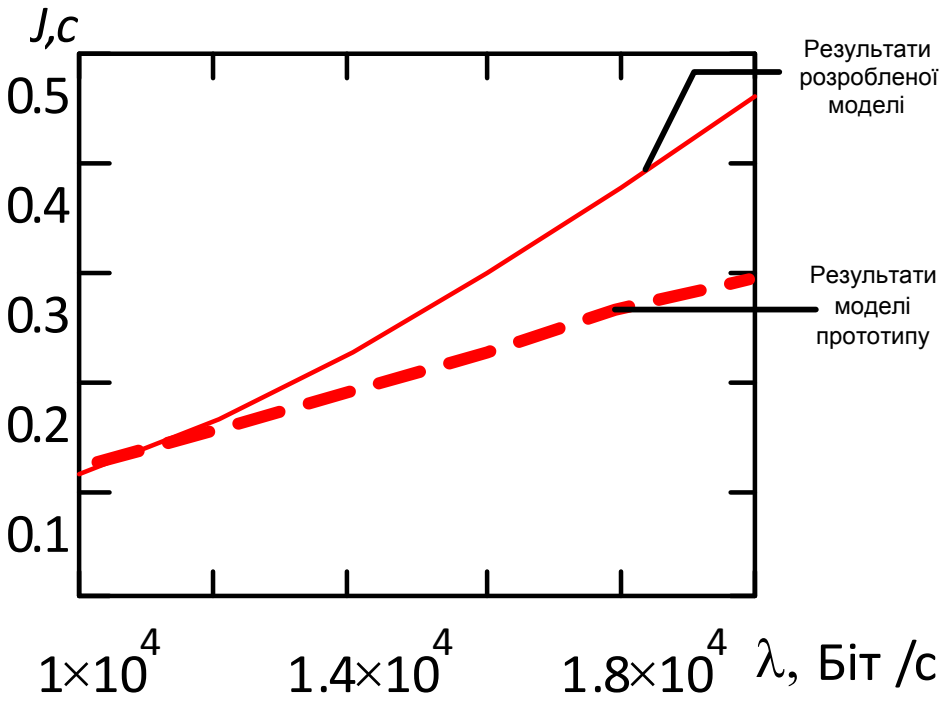
Як вихідні параметри моделювання і порівняльної оцінки були обрані числові значення характеристик процесу передачі геш-файлу метаданих, а також обробки й доставки команд передачі управління, характерні реальному процесу функціонуванню ТКС із використанням засобів доступу до хмарних антивірусних систем: $p = 0{,}9999$; $p_i^{(k)} = 0.1\times10^{-3}, 0.2\times10^{-3},...,0.4\times10^{-3}$; $\tau = 0.3\times10^{-3}$.

На рис. 10 наведено графіки залежності затримки (рис. 10.а) і джиттера (рис. 10.б) від інтенсивності потоку файлів метаданих, отримані в результаті розробленої моделі і моделі – прототипу.



а)

ISSN 2663 - 4023



б)

Рис. 10. Графіки залежності затримки і джиттера від інтенсивності потоку файлів метаданих

Як видно із графіків використання розробленої *GERT*-моделі технології передачі файлів метаданих, а також обробки і доставки команд передачі управління та врахування в ній можливості розбивки файлу метаданих і команд передачі управління на кадри дозволить в 1,2 рази підвищити точність при оцінці тимчасової характеристики, і в 1,4 разів при оцінці джиттера часу передачі і обробки файлів метаданих і команд передачі управління.

Таким чином, результати оцінки точності результатів моделювання підтверджують факт доцільності використання розробленої *GERT*-моделі технології передачі геш-файлу метаданих і команд передачі управління при проектуванні систем антивірусного захисту сучасних ТКС.

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті розроблений комплекс математичних GERT-моделей технології хмарного антивірусного захисту ТКС. Їхньою відмінною рисою є врахування необхідності обробки метаданих і формування команд передачі управління в хмарних антивірусних системах для забезпечення інформаційної безпеки.

У ході рішення поставленого завдання на першому етапі розроблені математична модель і проведено дослідження ймовірносно-часових характеристик алгоритмів і програм формування та обробки метаданих у хмарних антивірусних системах. Її відмінною рисою є врахування необхідності формування команд передачі управління

програмному клієнтові ТКС. Це дозволило підвищити точність результатів оцінки тимчасових характеристик в 1,7 разів, і характеристик джиттера в 4,5 рази.

На другому етапі моделювання розроблені GERT-моделі ТКС формування і обробки метаданих у хмарних антивірусних системах, що відрізняються від відомих врахуванням багатозв'язковості ТКС та можливості розбивки файлу метаданих і команд передачі управління на кадри. Використання розроблених GERT-моделей дозволить в 1,2 рази підвищити точність при оцінці тимчасової характеристики, і в 1,4 рази при оцінці джиттера часу передачі та обробки файлів метаданих і команд передачі управління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] С.Г. Семенов, В.В. Давыдов, и С.Ю. Гавриленко, *Защита данных в компьютеризированных управляющих системах*. Саарбрюккен, Германия: LAP Lambert Academic Publishing GmbH & Co. KG, 2014.

[2] Cloud security, Deep Dive series, August 2011. [Online]. Available: http://www.slideshare.net/kimrenejensen/cloud-security-deep-dive-2011#14375029197881&fbinitialized

[3] В.Г. Олифер, и Н.А. Олифер, *Компьютерные сети. Принципы, технологии, протоколы*. Санкт-Петербург, Россия: Питер, 2007.

[4] Ш. Одом, и Х. Ноттингем, *Коммутаторы CISCO*. Москва, Россия: Кудиц-Образ, 2003.

[5] Дж. Кингман, *Пуассоновские процессы*. Москва, Россия: МЦНМО, 2007.

[6] С.Г. Семенов, та О.О. Сур, " Математична модель системи криптографічного захисту електронних повідомлень на основі GERT-мережі ", *Системи управління, навігації та зв'язку. ЦНДІ навігації і управління*, т. 1, № 1(21), с. 131-137, 2012.

[7] С.Г. Семенов, В.В. Босько, та І.А. Березюк, " Исследования вероятностно-временных характеристик мультисервисного канала связи с использованием математического аппарата GERT-сети ", *Системи обробки інформації. ХУПС*, т. 1, № 3(101), с. 139-142, 2012.

[8] С.Г. Семенов, и А.А. Можаев, " Моделирование защищенного канала связи с использованием экспоненциальной GERT-сети ", *Информатика, математическое моделирование, экономика. Смоленский филиал АНО ВПО ЦС РФ "Российский университет кооперации"*, т. 1, с. 152-160, 2012.

[9] С.Г. Семенов, " Методика математического моделирования защищенной ИТС на основе многослойной GERT-сети ", *Вісник Національного технічного університету «Харківський політехнічний інститут»*, №62(968), с. 173-181, 2012.

[10] Г.Ф. Конахович, и В.М.Чуприн, *Сети передачи пакетных данных*. Киев, Украина: МК-Пресс, 2006.

[11] Ю.Н. Лавренков, " Исследование и разработка комбинированных нейросетевых технологий для повышения эффективности безопасной маршрутизации информации в сетях связи ", дис. канд. техн.наук., 2014.

[12] В.М. Вишневский, *Теоретические основы проектирования компьютерных сетей*. Москва, Россия: Техносфера, 2003.

[13] S.G. Semenov, V.V. Davydov, and S.O. Engalichev, " Mathematical Modelling of the Spreading of Software Threats in Computer Network ", in *Proceedings of the XIth International Conference TCSET'2012 «Modern problems of radio engineering, telecommunications and computer science»*, Lviv, 2012, p. 329.

[14] В. Е. Гмурман, *Теория вероятностей и математическая статистика*. Москва, Россия: Высшая школа, 2003.

[15] S. Semenov, and V. Davydov, " Mathematical Model for Technology for Spreading Malicious Software across Heterogeneous Networks based on Markov Chains ", *European Researcher*, vol. 66, no. 1-1, pp. 21-30, 2014.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (2), 2018
ISSN 2663 - 4023

Oleksii A. Smirnov
Doctor of technical sciences, professor, head of department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
OrcID: 0000-0001-9543-874X
dr.smirnovoa@gmail.com

Serhii A. Smirnov
Candidate of Science (Engineering), senior lecturer
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
OrcID: 0000-0002-7649-7442
smirnov.ser.81@gmail.com

Liudmyla I. Polishchuk
Senior lecturer
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
OrcID: 0000-0001-5093-1581
pli_80@ukr.net

Oksana K. Konoplitska-Slobodeniuk
Lecturer
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
OrcID: 0000-0001-9981-5194
ksuha80@gmail.com

Tetyana V. Smirnova
Candidate of Science (Engineering)
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
OrcID:0000-0001-6896-0612
sm.tetyana.gmail.com

GERT- MODELS OF TECHNOLOGY OF CLOUDY ANTI-VIRUS DEFENCE

Abstract. The complex of the mathematical GERT- models of technology of cloudy anti-virus defence of the telecommunication system (TCS) is worked out in this article, that allowed to get analytical expressions for timing of transmission of files of metadatas and forming and delivery of commands of control transfer. A mathematical model is worked out and a study of probabilistic-temporal descriptions of algorithms and programs of forming and treatment of metadatas is undertaken in anti-virus nephystems. Her distinctive feature is an account of necessity of forming of commands of control transfer to the programmatic client of TCS. On the second stage of design GERT- of model of technology of forming and treatment of metadatas is worked out in cloudy anti-virus nephystems. The feature of these models is an account of row of technological features of TCS (heterogeneity, much connectedness, possibility of breaking up of file of metadatas and commands of control transfer on the shots of and other). Use of the worked out GERT- models of technology of transmission of files of metadatas, and also treatments and deliveries of commands of control transfer and account in her possibilities of breaking up of file of metadatas and commands of control transfer on shots allowed to 1,2 time to promote exactness at the estimation of temporal description, and to 1,4 times at the estimation of jitter time of transmission and treatment of files of metadatas and commands of control transfer. The results of estimation of exactness of design results confirmed the fact of expediency of the use of the worked out GERT-model of technology of transmission hash - file of metadatas and commands of control at planning of the systems of anti-virus defence transfer modern TCS.

Keywords: telecommunication systems; anti-virus defence; treatment of metadatas; anti-virus nephystems.

REFERENCES

[1] S.G. Semenov, V.V. Davydov, i S.Ju. Gavrilenko, *Defence the systems given in the computerized managers*. Saarbrjukken, Germany: LAP Lambert Academic Publishing GmbH & Co. KG , 2014. (In Russian).

[2] Cloud security, Deep Dive series, August 2011. [Online]. Available: http://www.slideshare.net/kimrenejensen/cloud-security-deep-dive-2011#143750291978 81&fbinitialized (in English).

[3] V.G. Olifer, i N.A. Olifer, *Computer networks. Principles, technologies, protocols*. Sankt - Petersburg, Russia : Piter, 2007. (In Russian).

[4] Sh. Odom, i H. Nottingem, *Switchboards of CISCO*. Moscow, Russia: Kudic-Obraz, 2003. (In Russian).

[5] Dzh. Kingman, *Puasson's processes*. Moscow, Russia: MCNMO, 2007. (In Russian).

[6] S.H. Semenov, ta O.O. Sur, " A mathematical model of the system of cryptographic defence of electronic reports is on the basis of GERT- network ", *Systemy upravlinnia, navihatsii ta zviazku. TsNDI navihatsii i upravlinnia*, v. 1, № 1(21), pp. 131-137, 2012. (In Ukrainian).

[7] S.G. Semenov, V.V. Bos'ko, ta I.A. Berezjuk, " Researches of probabilistic-temporal descriptions of multiservice communication channel with the use of mathematical vehicle of GERT- network ", *Sistemi obrobki informacii. HUPS*, v. 1, № 3(101), pp. 139-142, 2012. (In Russian).

[8] S.G. Semenov, i A.A. Mozhaev, " Design of the protected communication channel with the use of the exponential GERT- network ", *Informatika, matematicheskoe modelirovanie, jekonomika. Smolenskij filial ANO VPO CS RF "Rossijskij universitet kooperacii "*, v. 1, pp. 152-160, 2012. (In Russian).

[9] S.G. Semenov, " Methodology of mathematical design of protected ИТС on the basis of the multi-layered GERT- networ ", *Visnik Nacional'nogo tehnichnogo universitetu «Harkivs'kij politehnichnij institut»,* №62(968), pp. 173-181, 2012. (In Russian).

[10] G.F. Konahovich, i V.M.Chuprin, *Networks of communication of package data*. Kyiv, Ukraine: MK-Press, 2006. (In Russian).

[11] Ju.N. Lavrenkov, " Research-and-development the combined nejronetwork technologies for the increase of efficiency of the safe routing of information in communication networks ", work of candidate of engineering sciences, 2014. (In Russian).

[12] V.M. Vishnevskij, *Theoretical bases of planning of computer networks*. Moscow, Russia: Tehnosfera, 2003. (In Russian).

[13] S.G. Semenov, V.V. Davydov, and S.O. Engalichev, " Mathematical Modelling of the Spreading of Software Threats in Computer Network ", in *Proceedings of the XIth International Conference TCSET'2012 «Modern problems of radio engineering, telecommunications and computer science»*, Lviv, 2012, p. 329. (in English).

[14] V. E. Gmurman, *Theory of chances and mathematical statistics*. Moscow, Russia: Vysshaja shkola, 2003. (In Russian).

[15] S. Semenov, and V. Davydov, " Mathematical Model for Technology for Spreading Malicious Software across Heterogeneous Networks based on Markov Chains ", *European Researcher*, vol. 66, no. 1-1, pp. 21-30, 2014. (in English).