УДК 004.657

Володимир Миколайович Чернега

Національний університет оборони України імені Івана Черняховського, Київ, Україна

МАТЕМАТИЧНА МОДЕЛЬ ПРОЦЕСУ ОБСЛУГОВУВАННЯ ЗАМОВЛЕНЬ В РОЗПОДІЛЕНІЙ БАЗІ ДАНИХ ІНФОРМАЦІЙНОЇ СИСТЕМИ В УМОВАХ ВПЛИВУ КІБЕРАТАК

В статті запропоновано удосконалену математичну модель процесу обслуговування замовлень в розподіленій базі даних інформаційної системи, яка враховує вплив кібератак на доступність інформації. Досліджується розподілена інформаційна система, що має клієнт-серверну архітектуру. Розглянуті найбільш небезпечні кібератаки, що впливають на ефективність функціонування розподілених баз даних, їх об'єкти впливу та можливі наслідки. Проаналізовані існуючі підходи до математичного моделювання інформаційного обміну в розподілених базах даних. Обґрунтовано застосування математичного апарату, який базується на теорії масового обслуговування та теорії ймовірностей. Запропонована модель дозволяє визначити залежність середнього часу обслуговування замовлень в розподіленій базі даних від інтенсивності потоку шкідливих замовлень з урахуванням частки реплікованих даних на локальному вузлі.

Ключові слова: *розподілена база даних; процес обслуговування замовлень; реплікація даних; кібератака.*

Вступ

Постановка проблеми. Автоматизація процесу управління в Збройних Силах (ЗС) України є одним з пріоритетних напрямків розвитку. Це здійснюється за рахунок впровадження комп'ютерних та телекомунікаційних систем (ТКС), але це також відкриває додаткові можливості для навмисних деструктивних дій на об'єкти інформаційної інфраструктури ЗС України. База даних (БД) є основою використання інформаційних ресурсів в системі управління ЗС України. Але, не зважаючи на впровадження різноманітних рішень, спрямованих на підвищення рівня захищеності інформаційних ресурсів в інформаційних системах (ІС), динаміка та наслідки кіберзагроз залишаються достатньо високими [1]. Загрозами об'єктам інформаційної інфраструктури ЗС України є кібератаки, несанкціонований доступ до інформаційних ресурсів та шкідливе програмне забезпечення [1-4], метою впливу яких є порушення доступності, цілісності та секретності (конфіденційності) інформації. Але найбільшу небезпеку представляють атаки, які направлені на порушення доступності інформації, до таких відносяться атаки типу "відмова в обслуговуванні" (DoS-атаки) та порушення маршрутизації пакетів в комутаційному обладнанні [2-4]. Інформаційна інфраструктура ЗС України представляє розподілену інформаційну систему (РІС), в якій інформація зберігається в БД. Актуальним є питання оцінювання кількісних та якісних показників процесу функціонування розподіленої БД (РБД) ІС в умовах впливу кібератак. Одним з таких показників є середній час обслуговування замовлень РБД.

Аналіз досліджень і публікацій. Дослідженням та розробкою моделей інформаційних процесів в РІС присвячено багато сучасних вітчизняних та зарубіжних робіт. Певні складнощі рішення цієї задачі пояснюються відсутністю універсальних методів та моделей, які б давали змогу враховувати усі особливості функціонування. Так, в дослідженнях [5], модель функціонування РІС військового призначення представлена у вигляді графа, а задача оптимізації зводиться до пошуку такої структури РІС, яка буде функціонувати в умовах впливу дестабілізуючих внутрішніх та зовнішніх факторів (в тому числі і кіберзагроз) за рахунок надмірності зв'язків між вершинами графу. Ця модель не враховує реплікацію даних та оперативність надходження інформації до посадових осіб в умовах інформаційного протиборства.

Інший підхід для математичного опису функціонування РБД розглянутий в роботах [6,7] в межах теорії ймовірності та теорії масового обслуговування. РБД представлена як сукупність деякої множини незалежних файлів із заданими до них підмножинами замовлень на оновлення та отримання даних. При цьому обсяг даних залежать від вузлів-джерел. Дана модель описує особливості замовлень на рівні транзакцій, але не враховує зміну характеристик телекомунікаційної мережі (ТКМ), що впливають на властивості РБД, та особливостей реплікації даних. В роботі [8] модель враховує процес реплікації, але основним недоліком є припущення, що середній час проходження повідомлення в каналах передачі даних є постійною величиною.

Отже, розглянуті існуючі підходи моделювання процесу функціонування РБД не враховують вплив кібератак на доступність інформації в БД РІС.

Метою статті є удосконалення математичної моделі процесу обслуговування замовлень в розподіленій базі даних в умовах впливу кібератак.

Виклад основного матеріалу дослідження

Для побудови математичної моделі процесу обслуговування замовлень РБД обраний математичний апарат теорії масового обслуговування, що використовується при аналізі та проектуванні комп'ютерних мереж [8-10]. Для повного опису такої системи вказуються імовірнісні процеси, що описують вхідний потік замовлень на обслуговування, час обслуговування замовлень, структуру системи та дисципліну обслуговування.

Визначимо вихідні дані та обмеження для побудови математичної моделі. В межах даного дослідження, РІС складається з центрального вузла та N локальних вузлів, що об'єднанні ТКМ. Центральний вузол містить сервер з основним (еталонним) екземпляром РБД, яка отримує всі оновлення з інтенсивністю λ_u. Кожний вузол представляє собою локальну обчислювальну мережу із сервером БД та сукупністю автоматизованих робочих місць із спеціальним програмним забезпеченням, що мають прямий зв'язок лише з цим сервером РБД, до інших серверів РБД зв'язок здійснюється через ІТМ. Кожний локальний сервер РБД містить деяку частку $h \in [0;1]$ центральної БД. Рівень відповідності репліки (копії) оригіналу виразимо через коефіцієнт $d \in [0;1]$, якщо $d = 1$, то репліка відповідає оригіналу на 100%. Кожний з N локальних серверів РБД приймає від АРМ замовлення на вибірку даних з інтенсивністю λ_q. Передбачається, що для окремо взятого вузла інформаційні потреби користувачів мають чітку направленість, яка враховується під час формування локальної БД. Щоб кількісно виразити більш високу імовірність звернення до локальної БД, вводиться додатковий параметр $f \in [1; 1/h]$. З урахуванням вказаного параметру імовірність локальної обробки замовлення на вибірку даних дорівнює $h \cdot f$, а відправка замовлення для обробки в центральній БД здійснюється з імовірністю $1 - h \cdot f$.

Кожний сервер РБД має один процесор, який відповідає за обробку замовлень як на вибірку даних, так і на оновлення даних, з дисципліною обслуговування FIFO ("перший прийшов, перший вийшов"). В якості джерел замовлень на обслуговування виступають замовлення до серверів РБД від АРМ, які надходять з інтенсивністю λ. Нехай вихідний потік замовлень класифікується за ознаками стаціонарності, ординарності та відсутності післядії, тобто тривалість інтервалу між замовленнями розподілена по експоненційному закону із щільністю $f(t) = \lambda e^{-\lambda t}$. Тоді ймовірність надходження k замовлень до РБД складатиме: $P(k) = \frac{(\lambda t)^k}{k!} e^{-\lambda t}$, $k = 0,1,2,...$. Значення часу перебування замовлення в РБД випадкове і залежить від багатьох незалежних факторів, таких як: пріоритет і тип замовлення, місце розміщення даних для його обробки, обсягу даних що передаються, кількості релевантних (достовірних) даних, завантаженість і працездатність серверів РБД та елементів ТКС, а саме непередбачуваних – моменти та наслідки впливу кіберзагроз. В моделі розглядаються лише кібератаки направлені на порушення доступності інформації. Кожна підсистема РБД, яка бере участь в обробці замовлень, представляє окремий тип СМО. До таких підсистем можна віднести: фрагменти локальної мережі інформаційно-телекомунікаційного вузла із сервером РБД – СМО 1-го типу, комунікаційне обладнанням (КО) – СМО 2-го типу, канали передачі даних (КПД) – СМО 3-го типу (Рис. 1).

При моделюванні складних динамічних систем, в яких підсистеми можуть бути представлені системами масового обслуговування, їх необхідно представляти у вигляді мереж масового обслуговування (МеМО) [9,10].

Так як, розглядається РБД з можливістю реплікації даних, тоді загальна інтенсивність надходження замовлень $\lambda = \lambda_q + \lambda_u$ складається із замовлень на вибірку даних – λ_q та на оновлення даних або реплік даних – λ_u. У випадку впливу кібератак (розглядаються лише атаки направлені на порушення доступності інформації) зменшується пропускна спроможність комутаційного обладнання та каналів передачі даних. Тому кібератаки будуть представлені інтенсивністю шкідливих замовлень λ_{cyb}, які надходять до СМО, і будуть враховуватися в загальній інтенсивності надходження замовлень до конкретного вузла $\lambda_j = \lambda_{q_j} + \lambda_{u_j} + \lambda_{cyb_j}$, де $j \in \{1,...,N\}$ – номер вузла, при відсутності кібератаки на вузол, $\lambda_{cyb_j} = 0$.

Одним з основних показників ефективності МеМО є середній час перебування замовлення в системі, тому в нашому випадку – це середній час обслуговування замовлення в розподіленій базі даних $\overline{T}_{obc}$, який розраховується за формулою:

$$\overline{T}_{obc} = \frac{1}{I_{in}} \left(\sum_{j}^{N} \lambda_j \cdot \overline{T}_{obc_j} \right), \qquad (1)$$

де: $I_{in} = \sum_{j=1}^{N} \lambda_j$ – загальна інтенсивність вихідного потоку замовлень;

$\overline{T}_{obc_j}$ – середній час перебування замовлення в j-ої СМО.

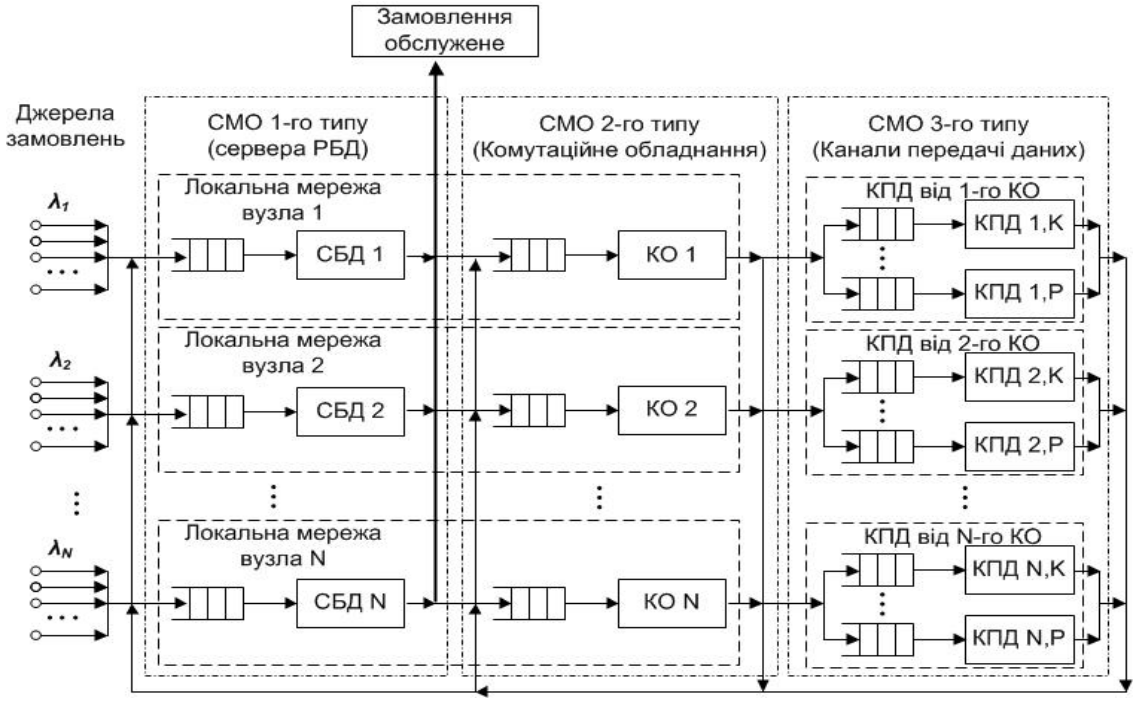

Рис. 1. Узагальнена структура модель процесу обслуговування замовлень в РБД

Загальна формула розрахунку середнього часу перебування замовлення в СМО з очікуванням має вираз:

$$\overline{T}_{obc_j} = W_j + M[\tau_j], \qquad (2)$$

де: W_j – середній час очікування обробки замовлення, $M[\tau_j]$ – середній час обробки замовлення у відповідній СМО, який дорівнює своєму математичному сподіванню (МС).

Час обробки замовлень τ в кожній підсистемі РБД визначається відповідно до технічних характеристик та алгоритмів роботи обладнання, що використовуються. А середній час очікування обробки замовлення W в кожній СМО розраховується відповідно до її типу, тому потребує більш детального огляду. Модель роботи серверів РБД представлена як СМО типу M/G/1 з очікуванням [9] і в нашому випадку визначається за формулою Поллачека-Хінчина. В моделі розглядаються два типи серверів РБД: центральний і локальний (клієнтський).

Розглянемо локальний сервер РБД, він обробляє два типи замовлень:

замовлення на вибірку даних з інтенсивністю $\lambda_{qr} = h \cdot f \cdot \lambda_q$ (h – частка реплікованих даних, f – додатковий параметр звернення до локальної БД) та МС часу обробки замовлення $M[\tau_{qr}]$;

замовлення на оновлення локальної БД з інтенсивністю $\lambda_{ur} = h \cdot d \cdot \lambda_u$, ($d$ – коефіцієнт відповідності реплік) та МС часу обробки замовлення $M[\tau_{ur}]$.

Середній час очікування обробки замовлення на локальному сервері W_r буде дорівнювати:

$$W_r = \frac{\lambda_{qr} M^2[\tau_{qr}] + \lambda_{ur} M^2[\tau_{ur}]}{1 - \left(\lambda_{qr} M[\tau_{qr}] + \lambda_{ur} M[\tau_{ur}]\right)}, \qquad (3)$$

де $M^2[\tau_{qr}]$ – другий момент випадкового часу обробки замовлення у відповідності до кожного приладу обробки, при умові, що $0 < \lambda_{qr} M[\tau_{qr}] + \lambda_{ur} M[\tau_{ur}] < 1$.

Центральний сервер РБД обробляє три типи замовлень:

замовлення на оновлення центральної БД від локальних серверів РБД з інтенсивністю λ_u та МС часу обробки $M[\tau_{ug}]$;

вимоги на відправлення повідомлень про оновлення локальних БД з інтенсивністю $\lambda_{ur} = h \cdot d \cdot \lambda_u$ та МС часу обробки замовлень $n \cdot M[\tau_{ugr}]$, де n – кількість серверів локальних БД в яких знаходиться відповідні репліки центральної БД, $M[\tau_{ugr}]$ – МС часу для відправлення одного повідомлення з центрального серверу РБД на оновлення локальної БД;

замовлення на вибірку даних для n віддалених локальних серверів БД з інтенсивністю $n \cdot (\lambda_q - \lambda_{qr})$ та МС часу обробки замовлення $M[\tau_{qg}]$.

Середній час очікування обробки замовлення на центральному сервері РБД W_g дорівнює:

$$W_g = \frac{\lambda_u M^2[\tau_{ug}] + \lambda_{ur} \cdot n^2 \cdot M^2[\tau_{ugr}] + n(\lambda_q - \lambda_{qr}) M^2[\tau_{qg}]}{1 - \left(\lambda_u M[\tau_{ug}] + \lambda_{ur} \cdot n \cdot M[\tau_{ugr}] + n(\lambda_q - \lambda_{qr}) M[\tau_{qg}]\right)}, \qquad (4)$$

при умові, що

$$0 < \lambda_u M[\tau_{ug}] + \lambda_{ur} \cdot n \cdot M[\tau_{ugr}] + n(\lambda_q - \lambda_{qr}) M[\tau_{qg}] < 1.$$

Функціонування комутаційного обладнання та каналів передачі даних доцільно розглядати, як єдину ТКС. СМО, яка моделює роботу ТКС між локальним сервером РБД та центральним, дозволяє оцінити середній час очікування передачі замовлення.

Розглянемо ділянку ТКС від локального серверу до центрального. В такій СМО існує два типи замовлень:

вимоги на передачу замовлень на вибірку даних на центральному сервері з інтенсивністю $\lambda_q - \lambda_{qr}$ та МС часу обробки замовлення $M[\tau_{qrg}]$. У випадку дії впливу кібератак інтенсивність надходження замовлень до ТКС буде складати $\lambda_q - \lambda_{qr} + \lambda_{cyb}$.

вимоги на передачу замовлень на оновлення центральної БД з локального серверу з інтенсивністю $\frac{\lambda_{ur}}{n}$ та МС часу обробки замовлення $M[\tau_{urg}]$. У випадку дії впливу кібератак інтенсивність надходження замовлень до ТКС буде складати $\frac{\lambda_{ur} + \lambda_{cyb}}{n}$.

Середній час очікування обробки замовлення в ТКС у напрямку центральної БД з урахуванням впливу кібератак визначається наступним чином:

$$W_{rg} = \frac{\left(\lambda_q - \lambda_{qr} + \lambda_{cyb}\right)M^2[\tau_{qrg}] + \frac{\left(\lambda_u + \lambda_{cyb}\right)}{n}M^2[\tau_{urg}]}{1 - \left(\left(\lambda_q - \lambda_{qr} + \lambda_{cyb}\right)M[\tau_{qrg}] + \frac{\left(\lambda_u + \lambda_{cyb}\right)}{n}M[\tau_{urg}]\right)}, \quad (5)$$

при умові, що

$$0 < \left(\lambda_q - \lambda_{qr} + \lambda_{cyb}\right)M[\tau_{qrg}] + \frac{\left(\lambda_u + \lambda_{cyb}\right)}{n}M[\tau_{urg}] < 1.$$

Тепер розглянемо ділянку ТКС від центрального серверу РБД до локального. В такій СМО існує також два типи замовлень:

вимоги на передачу замовлень на оновлення реплік в локальній БД з центрального серверу РБД з інтенсивністю λ_{ur} та МС часу обробки замовлення $M[\tau_{ugr}]$. У випадку дії впливу кібератак інтенсивність надходження замовлень до ТКС буде складати $\lambda_{ur} + \lambda_{cyb}$;

вимоги на передачу відповіді на замовлення з центрального серверу РБД на локальний з інтенсивністю $\lambda_q - \lambda_{qr}$ та МС часу обробки замовлення $M[\tau_{qgr}]$. У випадку дії впливу кібератак інтенсивність надходження замовлень до ТКС буде складати $\lambda_q - \lambda_{qr} + \lambda_{cyb}$.

Середній час очікування обробки замовлення в ТКС у напрямку до локальної БД з урахуванням впливу кібератак визначається наступним чином:

$$W_{gr} = \frac{\left(\lambda_u + \lambda_{cyb}\right)M^2[\tau_{ugr}] + \left(\lambda_q - \lambda_{qr} + \lambda_{cyb}\right)M^2[\tau_{qgr}]}{1 - \left(\left(\lambda_u + \lambda_{cyb}\right)M[\tau_{ugr}] + \left(\lambda_q - \lambda_{qr} + \lambda_{cyb}\right)M[\tau_{qgr}]\right)}, \quad (6)$$

при умові, що

$$0 < \left(\lambda_u + \lambda_{cyb}\right)M[\tau_{ugr}] + \left(\lambda_q - \lambda_{qr} + \lambda_{cyb}\right)M[\tau_{qgr}] < 1.$$

Таким чином, виведена загальна формула розрахунку значення середнього часу перебування замовлень в РБД з урахуванням процесу реплікації даних та впливу кібератак:

$$\overline{T}_{obc} = h \cdot f \cdot \left(W_r + M[\tau_{qr}]\right) + \left(1 - h \cdot f\right) \cdot \left(W_{rg} + M[\tau_{qrg}] + W_g + M[\tau_{qg}] + W_{gr} + M[\tau_{qgr}]\right). \quad (7)$$

де W_r – середній час очікування обробки замовлення на локальному сервері; W_g – середній час очікування обробки замовлення на центральному сервері РБД; W_{rg} – середній час очікування обробки замовлення в ТКС у напрямку центральної БД; W_{gr} – середній час очікування обробки замовлення в ТКС у напрямку до локальної БД.

Для отримання оцінки залежностей у досліджуємої РБД ІС виберемо в якості умовної одиниці часу (уоч) величину $M[\tau_{qg}]$ – МС часу обробки замовлення на вибірку даних на центральному сервері РБД. Тоді формула (7) перетвориться до наступного вигляду:

$$\overline{T}^*_{obc} = \frac{\overline{T}_{obc}}{M[\tau_{qg}]} \quad (8)$$

Під час моделювання були отримані залежності середнього часу обслуговування замовлень в РБД від ступеню реплікації даних та від інтенсивності надходження шкідливих замовлень під час дії кібератак. В графічному виді результати моделювання для РБД з урахуванням процесу реплікації даних представлені на рис. 2

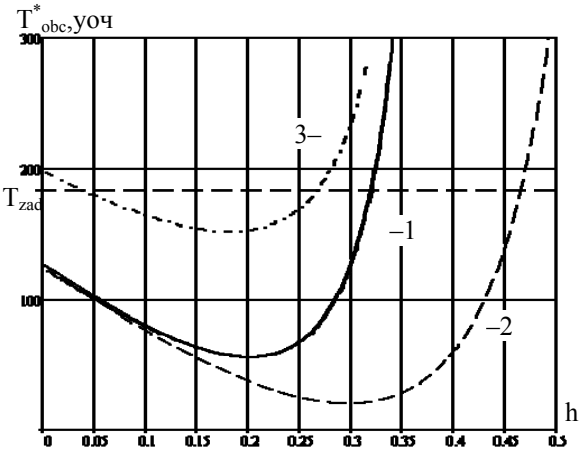

Рис. 2. Залежність середнього часу обслуговування замовлення від частки реплікованих даних (криві 1 та 2) та від інтенсивності впливу кібератак (крива 3).

З графіка видно, що при значенні $h = 0$ на локальних серверах база даних відсутня, тобто всі замовлення на вибірку даних обробляються на центральному сервері БД – архітектура "тонкий клієнт". Якщо $h = 0{,}2$, то кожний локальний сервер РБД містить 20% даних зі складу центральної БД – "товстий клієнт". При $d = 1$ (крива 1) репліки даних відповідають оригіналу, тобто дані достовірні та актуальні, при $d = 0{,}6$ (крива 2) – відповідність актуальних даних

60%. Зокрема, при збільшені $h \to 1$ навантаження, яке створюється обслуговуванням замовлень на вибірку даних, поступово переноситься з центрального сервера РБД на локальні. Проте при цьому на центральному сервері збільшується обсяг роботи по розсилці оновлень даних в локальних БД. Так при $h = 0{,}2$ (крива 1) починає виникати ефект перевантаженості каналів передачі даних та локальних серверів БД, які окрім обслуговування замовлень на вибірку даних від своїх користувачів повинні ще проводити оновлення локальних реплік даних. При моделюванні кібератаки на комутаційне обладнання одного локального вузла, збільшується загальна інтенсивність замовлень, які відправлені на обслуговування до центрального серверу РБД із середнім час обслуговування в каналі передачі даних. Відповідно до формули (5) збільшується середній час очікування обробки замовлення. З графіка (крива 3) видно що при $h = 0$ (відсутність локальної бази даних), середній час перебування замовлення в РБД збільшився і став перевищувати заданий час T_{zad}, тобто ефективність функціонування РБД не відповідає висунутим вимогам. У випадку застосування технології реплікації даних при раціональному $h = 0{,}25$ середній час перебування замовлення в РБД збільшився, але він не перевищує T_{zad}.

Висновки

Таким чином, удосконалена математична модель процесу обслуговування замовлень в розподіленій базі даних інформаційної системи враховує вплив кібератак на доступність інформації. Запропонована модель, базується на методах теорії масового обслуговування, але відрізняється новим диференційованим підходом до визначення середнього часу обслуговування замовлень в РБД в залежності від частки реплікованих даних та інтенсивності кібератак.

Напрямком подальших досліджень може бути широке коло питань щодо оцінювання ефективності функціонування РБД ІС спеціального призначення в умовах впливу кіберзагроз та розробка методик підвищення їх ефективності функціонування.

Література

1. Звіт CERT-UA за 2014 рік [Електронний ресурс] / CERT-UA – Режим доступу до ресурсу: http://cert.gov.ua/?p=2019. **2. Радько Н. М.** Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. / Н.М. Радько, И.О. Скобелев. – М.: Радиософт, 2010 – 232с. **3. Есин В. И.** Безопасность информационных систем и технологий / В.И. Есин, А.А. Кузнецов, Л.С. Сорока – Х.: ООО "ЭДЭНА", 2010. – 656 с. **4. Рубан І. В.** Аналіз основних аспектів впливу DoS-атак на працездатність комп'ютерної мережі. / І. В. Рубан, Є. С. Лошаков, Д. В. Прибильнов // Сучасні інформаційні технології у сфері безпеки та оборони. – К.:НУОУ, 2013. – №3(18).– С. 90-92. **5. Барабаш О. В.** Построение функционально устойчивых распределенных информационных систем. / О.В. Барабаш К.: НАОУ, 2004. 226 с. **6. Цегелик Г. Г.** Системы распределенных баз данных. / Г. Г. Цегелик – Львов: Свит, 1990. – 168 с. **7. Телятников О. О.** Динамическая модель распределенной базы данных компьютерной информационной системы. / О.О. Телятников, С.В. Лаздынь // Наукові праці ДонДТУ Випуск 38 –Донецьк: РВА ДонДТУ, 2002. – С. 115–121. **8. Мейкшан Л. И.** Анализ двухуровневой информационной системы с репликацией данных / Л. И. Мейкшан / Инфокоммуникационные технологии. 2009. – №2 С. 56-60. **9. Довгий С. О.** Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання. Видання друге (доповнене). / С.О. Довгий, П.П. Воробієнко, К.Д. Гуляєв За загальною ред. Довгого С.О. – К.:"Азимут-Україна". – 2013. – 608 с. **10. Ложковский А. Г.** Теория массового обслуживания в телекоммуникациях: учебник / А.Г. Ложковский. – Одесса: ОНАС им. А. С. Попова, 2012. – 112 с.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПРОЦЕССА ОБСЛУЖИВАНИЯ ЗАЯВОК В РАСПРЕДЕЛЕННОЙ БАЗЕ ДАННЫХ ИНФОРМАЦИОННОЙ СИСТЕМЫ В УСЛОВИЯХ ВОЗДЕЙСТВИИ КИБЕРАТАК

Владимир Николаевич Чернега

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье предложена усовершенствованная математическая модель процесса обслуживания заявок в распределенной базе данных информационной системы, которая учитывает воздействие кибератак на доступность информации. Исследуется распределенная информационная система с клиент-серверной архитектурой. Рассмотрены наиболее опасные кибератаки, которые влияют на эффективность функционирования распределенных баз данных, их объекты воздействия и возможные последствия. Проанализированы существующие подходы математического моделирования информационного обмена в распределенных базах данных. Обосновано применение математического аппарата, основанного на теории массового обслуживания и теории вероятности. Предложенная модель позволяет определить зависимость среднего времени обслуживания заявок в распределенной базе данных от интенсивности потока "вредоносных" заявок с учетом доли реплицированих данных на локальном узле.

Ключевые слова: *распределенная база данных; процесс обслуживания заявок; репликация данных; кибератака.*

THE MATHEMATICAL MODEL OF QUERY PROCESSING IN DISTRIBUTED DATABASE INFORMATION SYSTEM UNDER CYBERATTACKS

Volodymyr M. Cherneha

National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

The paper gives an improved mathematical model of service process in a distributed information system database that takes into account the impact of cyberattacks on the availability of information. The distributed information system with client-server architecture is researching. It is considered the most dangerous cyberattacks, which affect the efficiency of the distributed databases, their objects of the impact, and the possible consequences. The existing approaches of mathematical modeling of information exchange in distributed databases are analyzed. The application of mathematical apparatus, based on the queuing theory and probability theory is provided. The article represent the dependence of the average service time of requests in a distributed database on the malicious requests flow rate by means of replicating data to local sites. Direction of further researches is on the efficiency evaluation of information system distributed database operating under cyberthreats and methodologies development for its efficiency increasing.

Keywords*: distributed database; request processing; data replication; cyberattack.*

References

1. Zvit CERT-UA za 2014 rik [Elektronnyi resurs], Rezhym dostupu do resursu: http://cert.gov.ua/?p=2019. **2. Rad'ko N.M.** (2010), Risk model information and telecommunication systems in the implementation of remote access and direct threats. [*Risk-modeli informacionno-telekommunikacionnyh sistem pri realizacii ugroz udalennogo i neposredstvennogo dostupa*], N.M. Rad'ko, I.O. Skobelev, Moscow, Radiosoft, 232 p. **3. Esin V.I.** (2010), Security of information systems and technologies. [*Bezopasnost' informacionnyh sistem i tehnologij*], V.I. Esin, A.A. Kuznecov, L.S. Soroka, Kharkov: OOO "JeDJeNA", 656 p. **4. Ruban I.V.** (2013), Analysis of the main aspects of the impact of DoS-attacks on the performance of a computer network. [*Analiz osnovnykh aspektiv vplyvu DoS-atak na pratsezdatnist kompiuternoi merezhi*], I.V. Ruban, Ye.S. Loshakov, D.V. Prybylnov, Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, Kyiv, NUOU, No 3(18), pp. 90-92. **5. Barabash O.V.** (2004), Construction of functional stability of distributed information systems. [*Postroenie funkcional'no ustojchivyh raspredelennyh informacionnyh system],* O.V. Barabash, Kyiv, NAOU, 226 p. **6. Cegelik G.G.** (1990), Systems Distributed Databases. [*Sistemy raspredelennyh baz dannyh*], G.G. Cegelik, Lviv, Svit, 168 p. **7. Teljatnikov O.O.** (2002), A dynamic model of distributed database of computer information systems. [*Dinamicheskaja model' raspredelennoj bazy dannyh komp'juternoj informacionnoj sistemy*], O.O. Teljatnikov, S.V. Lazdyn', Naukovi praci DonDTU Vipusk 38, Donec'k, DonDTU, pp. 115–121. **8. Mejkshan L.I.** (2009), Analysis of a two-tier information system with data replication. [Analiz dvuhurovnevoj informacionnoj sistemy s replikaciej dannyh], L.I. Mejkshan, Infokommunikacionnye tehnologii, No 2 pp. 56-60. **9. Dovhyi S.O.** (2013), Modern telecommunications, network, technology, security, economics and management. Second edition (updated). [*Suchasni telekomunikatsii: merezhi, tekhnolohii, bezpeka, ekonomika, rehuliuvannia*]. Vydannia druhe (dopovnene), S.O. Dovhyi, P.P. Vorobiienko, K.D. Huliaiev, Kyiv, "Azymut-Ukraina", 608 p. **10. Lozhkovskij A.G.** (2012), Queueing theory in telecommunications: the textbook. [*Teorija massovogo obsluzhivanija v telekommunikacijah: uchebnik*], A.G. Lozhkovskij, Odessa, ONAS, 112 p.

Отримано: 04.04.2015 року.