WILL. / О.О. Шорін, Г.О. Бокк // Економіка та якість систем зв'язку. 2019. №1(11). С. 9-13.
[15]. W-Fi мережі: проникнення та захист. Ч.1. Матчастина (Електронний ресурс). Режим доступу: https: //habr.com/ru/ post/224955, вільний.
[16]. Wi-Fi мережі: проникнення та захист. 4.2. Кай. Приховування SSID. MAC-фільтрація WPS (Електронний ресурс]. Режим доступу: https://tabir. com /ru/post/225483, вільний. Заголовок з екрана (25.08.2020).
[17]. Wi-Fi мережі: проникнення та захист. 4.3. WPA. OpenCL/CUDA. Статистика підбору (Електронний ресурс]. Режим доступ https://habe.com/ru/ post/220431, вільний Заголовок з екрана (25.08. 2020).
[18]. Ahson, S. Wimax: Standards and Security/S. Ahson, M. Ilyas-CRC Press, 2007. 276 p.
[19]. Злом і захист Wi-Fi. Опис технології. Hacking and Protection wi-fi. Description of technology [Електронний ресурс]. Режим доступу: https: // youtube.com/watch?v=uh0R:94408O, вільний.
[20]. Vanhoef, M. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2/M. Vanhool, F. Piessens [Електронний ресурс] Режим доступу: https:// papers.mathyvanhoef.com/ cos2017.pdf, вільний.

THE PROBLEM OF ENSURING THE SECURITY OF PROFESSIONAL RADIO COMMUNICATION SYSTEMS IN CRITICAL INFRASTRUCTURES

This paper reviews the existing and expected scenarios of unauthorized impacts on communication systems in critical information structures. It has been established that the area of increased risk of such impacts is focused on the interfaces between external devices and the SoC chip. Examples are given of grouping a large number of subscriber terminals operating under a single program of unauthorized influences, and the level of penetration can be increased many times over. It is noted that such possibilities become more realistic with the introduction of 5G generation systems that provide for M2M operation. The purpose of this review is to determine an approach to modeling the processes of protecting information from leakage through radio channels of communication systems and to develop engineering and technical measures for the design and implementation of appropriate information security systems.

Keywords: SoC chip, tampering, peripherals, 5G, X.200 open system model.

Шавловський Ярослав Сергійович, аспірант кафедри Систем інформаційного та кібернетичного захисту Державного університету інформаційно-комунікаційних технологій.

Yaroslav Shavlovsky, PhD student of the Department of Information and Cyber Defense Systems of the State University of Information and Communication Technologies.
E-mail: redwaveplus@ukr.net.
Orcid ID: 0009-0002-4737-9049.

Передерій Сергій Андрійович, завідуючий лабораторією кафедри Систем інформаційного та кібернетичного захисту Державного університету інформаційно-комунікаційних технологій.

Serhii Perederii, Head of the Laboratory of the Department of Information and Cyber Defense Systems at the State University of Information and Communication Technologies.
E-mail: seriy127@gmail.com.
Orcid ID: 0000-0002-1949-7868.

Бичков Володимир В'ячеславович, старший викладач кафедри безпеки інформаційних технологій Національного авіаційного університету, помічник ректора Державного університету інформаційно-комунікаційних технологій.

Volodymyr Bychkov, Senior Lecturer at the Department of Information Technology Security at the National Aviation University, Assistant to the Rector of the State University of Information and Communication Technologies.
E-mail: bychkov.v@duikt.edu.ua.
Orcid ID: 0000-0002-1054-9182.

DOI: 10.18372/2410-7840.26.18820
УДК 336.71:004.056

МАТЕМАТИЧНИЙ АПАРАТ ЗНАХОДЖЕННЯ ОПТИМАЛЬНОЇ КОНФІГУРАЦІЇ ЗАХИЩЕНОЇ МЕРЕЖІ ЗВ'ЯЗКУ ІЗ ЗАДАНИМ ЧИСЛОМ АБОНЕНТІВ

Олександр Лаптєв, Аблуллах Аль-Далваш

Інформаційні потоки у світі зростають дуже швидко. Швидко зростає обмін інформацією. У зв'язку з цим фактом постійно розвивається існуючий математичний апарат та його практичне застосування. Науково-математичний апарат спрямовано на знаходження оптимальної конфігурації мережі інформаційного зв'язку, вирішенню проблеми побудови захищених каналів передачі великої кількості даних. Виникає наукове завдання щодо розробки нового та удосконалення існуючого математичного апарату для знаходження оптимальної конфігурації захищеної мережі зв'язку із заданим числом абонентів. Вирішенню цього актуального завдання і присвячена дана наукова робота. У ній сформульовано та доведено чотири Леми. Формулювання Леми дозволили довести дві нові теореми, які дозволяють вирішити завдання ефективного рішення

знаходження оптимальної конфігурації захищеної мережі зв'язку із заданим числом абонентів. Наведено рішення як часткових, так і загальних завдань процесу оптимізації та захисту каналів передачі великої кількості даних. Таким чином у роботі запропоновано рішення наукове завдання знаходження оптимальної конфігурації захищеної мережі зв'язку із заданим числом абонентів. Напрямком подальших досліджень може бути розробка програмної реалізації наведеного математичного апарату.

***Ключові слова**: захищені мережі, оптимальна конфігурація, захист інформації, безпека даних, кібербезпека.*

ВСТУП

Інформаційні потреби прикладних галузей знань постійно збільшуються. Тому процес підвищення ефективності комп'ютерів і інформаційних технологій дуже актуальний і продовжується безперервно. Функція систем зв'язку - забезпечення споживачів технічною можливістю для обміну інформацією за даними показниками надійності та якості. Забезпечити споживачів обміном інформації захищеною мережею. Для здійснення цієї мети необхідно мати можливість будувати оптимальні за конфігурацією мережі обміну інформацією або мережі зв'язку.

Набагато простіше було вчинити за принципом: менше пристроїв, тим краще. Однак цей принцип неможливо застосувати у нашому інформаційному світі. Проблематика існує як у побудові оптимальної конфігурації мережі, так і у захисті інформації, яка циркулює у мережі.

Хоча формальна теорія захисту інформації почала розвиватися порівняно нещодавно, сьогодні є багато математичних моделей, які описують різні аспекти безпеки та надають доказову теоретичну базу для побудови захищеної мережі зв'язку. Існують таки класичні моделі, як Харрісона-Руззо-Ульмана, Take-Grant, Бела-ЛаПадула, Біба та ін., вони достатньо описані та досліджені у наукових роботах. Вони надають можливість формального доказу захищеності інформації у мережі. Модель матриці доступів Харрісона-Рузо-Ульмана побудована з використанням апарату теорії відносин.

Модель розподілу прав доступу Take-Grant [34, 35] побудована з використанням апарату теорії графів.

Класична модель Белла-ЛаПадулла та моделі, що базуються на ній (модель безпечного переходу, модель з уповноваженими суб'єктами, модель спільного доступу, модель безпечного переходу для системи спільного доступу, модель спільного доступу з уповноваженими суб'єктами), побудовані з використанням апаратів теорії відносин та грат. У цих моделях вводяться поняття функції безпеки та ґрати рівнів безпеки, які визначають усі дозволені відносини між сутностями системи. У моделях, що розвивають класичну, вводяться також різні додаткові правила, що регламентують можливість здійснення переходів, що змінюють рівні безпеки сутності системи.

Модель Trusted Mach побудована з використанням теорії предикатів. Вона являє собою модель станів і подій, в якій використовується оператор наступного значення, що визначає нові значення змінних стану після подій, що відбулися.

Модель Law-Water-Mark (LWM) побудована з використанням теорії відносин. Незважаючи на формальну відмінність даних моделей, спільними між ними є те, що у всіх тим чи іншим чином вводиться безліч суб'єктів (користувачів) U, об'єктів (захищених ресурсів) R, повноважень доступу L, запитів доступу Q(U,R), правил надання доступу чи відмови у доступі F (U,R,L).

На жаль, жодна з наведених моделей не оперує такими поняттями, як загроза або механізм захисту, тому вони представляють скоріше теоретичний інтерес з точки зору можливості формального доказу захищеності інформації в мережі, ніж практичний – з точки зору можливості їх застосування при побудові оптимальної захищеної конфігурації. мережі зв'язку із заданим числом абонентів. Таким чином, наукове завдання по побудові оптимальної конфігурації захищеної мережі зв'язку із заданим числом абонентів залишається актуальним.

Метою даної роботи є математичний апарат знаходження оптимальної конфігурації захищеної мережі зв'язку із заданим числом абонентів. Для цього потрібно вирішити наукове завдання щодо розробки варіантів ефективних рішень знаходження оптимальної конфігурації захищеної мережі на основі доведених теорем.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Сучасні мережі передачі даних є складний комплекс технічних засобів, програмного забезпечення, пристроїв управління організаційною структурою, що дозволяє спільно функціонувати елементам комплексу та експлуатувати їх з територіально розподіленими абонентами. Завданню проблеми інформатизації різних структур, вирішенню завдання інформаційної безпеки та розробці оптимальної структури зв'язку присвячено багато публікацій.

Так, у роботах [1, 2] наведено опис функцій, що реалізуються різними рівнями стека протоколів еталонної моделі мережі, а у [3] – характеристика найбільш широко використовуваних стеків мережевих протоколів та їх співвідношення з рівнями стеку протоколів еталонної моделі інформаційної мережі. Але описано процес загального обміну інформацією, який не відповідає на питання побудови оптимальної, захищеній мережи зв'язку.

У роботі [4] розглядаються особливості синтезу оптимальної топології мережі передачі. Визначено показники якості у вигляді сукупності імовірнісно-часових характеристик щодо трафіку передачі інформаційних пакетів. Проведений аналіз показав наявність впливу зміни параметрів на пропускну здатність передачі даних. Але процесу оптимізації мереж не гранично достатньо уваги.

У роботах [5, 6] розглянуто принципи моделювання комп'ютерних мереж на різні архітектурних рівнях. Досліджено моделі процедур управління окремою ланкою передачі даних і багатоланковою транспортною сполукою, що враховують фактори спотворень у каналах зв'язку, блокування обмеженої буферної пам'яті транзитних вузлів комутації, а також рівень навантаження на мережеві з'єднання та конвеєрний ефект. Запропоновано методи розрахунку операційних характеристик мережевих топологічних структур, оптимізації протокольних параметрів і структури пакетів передачі даних. Але процеси оптимізації мереж та захисту інформації не розглядаються у повної мірі.

У роботі [7] розглянуто загальні підходи, пов'язані з використанням поняття «механізм» в системі кібербезпеки. Представлено первинне визначення механізму в системах аналітичної динаміки. Простежено трансформацію поняття «механізм» від механічних систем до економічних, соціальних і організаційно-технологічних. Сформульовано визначення механізму, яке може бути використано при аналізі і проектуванні систем прийняття рішень, розглянуті особливості використання цього поняття в системах кібербезпеки. Особливу увагу приділено аналізу та розробки алгоритмічних механізмів, використовуваних в теорії аукціонів, а також додатків, заснованих на використанні як класичної теорії ігор, так і теорії динамічних ігор.

У роботах [8,9] запропоновано розглядати механізм прийняття рішень в системах кібербезпеки як систему відносин різних (індивідуальних, групових, організаційних) агентів, взаємодія яких спрямована на вирішення проблеми забезпечення захисту належного рівня. Зазначено, що одним з варіантів такого підходу є механізм прийняття рішень. Нажаль розглянуто тільки конкретні випадки. Узагальнення не зроблено.

У роботах [10, 11] розглянуто ряд модулів безпеки в інформаційних мережах, що дозволяє оптимально регламентувати доступ до локальної інформаційної мережі із зовнішніх мереж з точки зору безпеки інформації; визначено чисельні значення можливостей несанкціонованого доступу для даного виду з'єднання, вибраного на основі отриманих даних, для оптимального вибору захисних механізмів. Але математичний апарат не дозволяє вирішувати проблему у загальному вигляді.

Таким чином, у результаті вивчення наукових публікацій за темою статті, дисертацій, патентів та монографій встановлено, що на сьогодні існує актуальне наукове завдання по удосконаленню математичного апарату знаходження оптимальної конфігурації захищеної мережі зв'язку із заданим числом абонентів.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У завданнях знаходження оптимальної конфігурації захищеної мережі зв'язку із заданим числом абонентів, потрібно вибрати множину X_O за умови, що відомо лише число його вершин $[X_O]=p$, тобто задане число абонентів мережі [12, 15].

Для цього випадку, у зв'язному орграфі $G=(X,U)$, $|X|=n$, з принесеними довжинами дуг $l(u)>0$ необхідно знайти підмножину, $X_O \subset X$, $[X_O]=p,(p<n)$, для якого відповідний мінімальний вихідний $T^*=\left(X,U^*\right)$, $U^* \subset U$, з базою $X_O \subset X$ буде найменшим.

Це завдання взагалі можливо вирішити шляхом перебору можливих підмножин $Y \subset C$, $|Y|=p$, але кожне рішення, при *p,* близьких к *n*/2, потребує розгляду $\left(p^n\right)$ варіантів, що є дуже важким завданням.

При p=1 розглянуту задачу можна звести до спрощеної задачі для деякого допоміжного орграфа $G_1=(X_1,U_1)$. Він виходить з G шляхом додавання нової вершини Z як кореня та нових дуг $V_1,V_2,...,V_n$, що виходять із Z і заходять у відповідні вершини $x_1 \in X$; довжини $l(V_1)=C$, i = 1,2,

..., n, де $C = \sum_{u \in v} l(u)$. Вирішуючи задачу для орграфа G_1, знаходимо мінімальне (за сумою довжин дуг) дерево, що виходить,, з коренем z = X_1. Легко помітити, що дерево, що виходить $T_1^* = \left(X_1, U_1^*\right)$ $U_1^* \subset U$, містить рівно одну дугу V_{i0}, з безлічі доданих дуг $V_1, V_2, ..., V_n$. Якщо з цього дерева видалити V_{i0} разом з Z, то отриманий орграф буде для орграфа, що знаходиться, мінімальним вихідним деревом T^* з коренем в шуканій вершині. Для загального випадку (довільного p) не відомі хороші (в сенсі алгоритму Едмонда) алгоритм вирішення сформульованої задачі [13, 14]. Наведемо деякі вихідні дані, на основі яких описуватиметься ефективний алгоритм її вирішення. Вихідним шляхом подальших міркувань послужать такі процедури:

1) наводимо алгоритм G з $\sigma_G\left(\{x\}\right), \forall_x \in X$;

2) беремо *i* = 0;

3) знаходимо орграф $\hat{G}^i = (X\ \hat{U}^i)$, де $\hat{U}^i$ - безліч всіх отриманих виділених дуг;

4) перевіряємо, чи є $\hat{G}^i$ дуже зв'язаним. Якщо так, то переходимо до пункту 8, інакше – до п.5;

5) знаходимо в орграфі $\hat{G}^i$ сильно зв'язкові компоненти $\hat{G}^i = (\hat{X}^i_j, \hat{U}^i_j)$, *j = 1,2, ..., g.*

6) проводимо орграф G, $\sigma_G(\hat{X}^i_j)$ *j = 1,2 .....,g;*

7) замінюємо i на i + 1 та переходимо до п.3;

8) процедура закінчена.

При проведенні цієї процедури може виникнути питання про існування сильно зв'язний компоненти $\hat{X}^i_r = \left(\hat{X}^i_r, \hat{U}^i_r\right)$, такий, що, якщо орграф $\sigma\hat{G}_i\left(\hat{X}^i_r\right) \neq \varphi$, не є дуже зв'язаним.

Відповідь це питання дає наступна лема.

Лема 1. Нехай $G^1 = \left(X_1 U^1\right)$ $U^1 \subset U_1$ довільний орграф *G*. Тоді орграф *G* будє сильно зв'язковим тоді і лише тоді, коли $\sigma G^1(Y) \neq \varphi$ для будь-кого $Y \subset X$.

Отже, якщо орграф $\hat{G}^i$ на і-й ітерації процедури не дуже зв'язковий, то обов'язково існує його зв'язна компонента $\hat{G}^i_r = \left(\hat{X}^i_r, \hat{U}^i_r\right)$ така, що $\sigma_{\hat{G}^i}\left(\hat{X}^i_r\right) \equiv \varphi$.

Вважатимемо, що орграф $\hat{G}^i = \left(X, \hat{U}^i\right)$, при i = 0 (тобто при нульовій ітерації) є орграф $\hat{G}^o = (X, \varphi)$, де кожна вершина є зв'язною компонентою. Нехай M-множина всіх X^i_j, $i = 0, 1, 2, ..., k-1$; $g = 1, 2, ..., g$, що утворюється у процесі виконання цієї процедури (до-кількість її ітерацій). Розглянемо функцію g: M→D, де $g\left(\hat{X}^i_j\right)$ значення константи приведення по множині $\hat{X}^i_j$ після виконання і-й ітерації процедури.

Для довільної множини $M_1 \subset M$ і будь-якого Y⊂X введемо такі обов'язки:

$$N_{M_1}(Y) = \left\{X^i_j \in M_1 / X^i_j \cap Y \neq \varphi\right\};$$

$$R_{M_1}(Y) = \sum_{X_j \in N_{M_1(Y)}} g\left(\hat{X}^i_j\right).$$

Неважко перевірити, що для будь-яких $X_1, X_2 \subset X$ і $M_1 \subset M$ справедливі співвідношення:

$$R_{M_1}(X_1 \cup X_2) = R_{M_1}(X_1) + R_{M_1}(X_2),$$
$$M_2 = M_1 / N_{M_1}(X_1), \qquad (1)$$

де:

$$R_{M_1}(X_1 \cup X_2) = R_{M_1}(X_1) + R_{M_1}(X_2) -$$
$$- \sum_{X^i_j \in N_{M1}(X_1) \cap N_{M1}(X_2)} g\left(\hat{X}^i_j\right). \qquad (2)$$

Припустимо тепер, що для орграфа G застосований алгоритм розв'язання задачі з $t(G) = X_0$, де X_0 – довільне p-елементне підмножина з X. В результаті прямого ходу алгоритму отримаємо множину $A = \left\{X^i_j\right\}$, i = 0,1,2, ..., k; j=1,2,…,g.

Лема 2. Якщо $A^1 = \left\{X^i_j \in A / \ f\left(X^i_j\right) \succ 0\right\}$, а $M^1 = \left\{X^i_j \in M / g\left(\hat{X}^i_j\right) \succ 0\right\}$, то:

$$A^1 = M^1 / N_{M^1}(X_0); \qquad (3)$$

більш за це, функції *f* та g^1 на множині $M^1 / N_{M^1}(X_0)$ співпадають.

Доведення. Нехай $A\big|_g \subseteq A$, де g=1, 2, …, k-1, де $A\big|_g = \left\{X^g_j \in A / f\left(X^g_j\right) \succ 0\right\}$, а $M\big|_r \subseteq M_1$, r=1, 2,

…,k-1, де $M_r^1 = \left\{ X_j^r \in M \middle/ g\left(\hat{X}_j^g\right) \succ 0 \right\}$; за іншим A_g^i є безліч тих X_j^g, які утворюються безпосередньо під час проведення і - й ітерації процедури, у яких заходять зазначені дуги і-$\hat{U}^z$, що виходять ззовні множені $\hat{X}_j^r$.

Легко помітити, що й g-й інтервалі прямого ходу алгоритму утворюється сильно зв'язкова компонента $G_{j_0}^q = \left(X_{j_0}^q, U_{j_0}^q \right)$, на яку $f\left(X_{j_0}^q\right) > 0$, тобто $X_{j_0}^q \in A_q^1$, то на відповідній q-й ітерації процедури повинні утворитися така ж сильно зв'язкова компонента, причому $f\left(X_{j_0}^q\right) = q\left(X_{j_0}^q\right)$.

Має місце й протилежне: якщо і-й ітерації процедури утворюється сильно зв'язкова компонента $\hat{G}_{j_1}^r = \left(\hat{X}_{j_1}^r, \hat{U}_{j_1}^r \right)$, яка містить вершин X_0 така, що $g\left(X_{j_1}^r\right) > 0$, тобто $\hat{X}_{j_1}^r \in M_r$, то на відповідній і-й ітерації прямого ходу алгоритму повинна утворитися така сама зв'язна компонента, причому $g\left(\hat{X}_{j_1}^r\right) = f\left(\hat{X}_{j_1}^r\right)$. Отже, $\hat{k} \geq k$ і $A_q^1 = M_q^1 / N_{M_q^1}\left(X_0\right)$, *q=1 ,1…,k;* $M_r^1 / N_{M_r^1}\left(X_0\right) = \varphi$, *r = k+1, k+2, …,* $\hat{k}$.

Оскільки $A^1 = \bigcup_{g=1}^{k} A_g^1$, а $M^1 = \bigcup_{r=1}^{\hat{k}} M_r^1$, то $A^1 = M^1 / N_{M^1}\left(X_0\right)$ функції *f* та *g* цей множені співпадають.

Теорема 1. Якщо $T^* = \left(X_1 U^*\right)$ – мінімальний виходить з базою $X_0 \subset X$ для орграфа G з $t(G) = X_0$, тоді:

$$L_{T^*} = \sum_{\hat{X}_j \in M} g\left(\hat{X}_j^i\right) - \sum_{X_j \in \hat{N}_M\left(X_0\right)} g\left(\hat{X}_j^i\right). \quad (4)$$

Доведення. Припустимо, що з орграфа G з $t(G) = X_0$ був застосований алгоритм розв'язання задачі. В результаті утворилося множина $A = \left\{ X_j^i \right\}$, i =0, 1, 2, ..., k, j = 1,2, ..., qi. Тоді, використовуючи лему 2 (співвідношення 3), отримаємо:

$$L_{T^*} = \sum_{X_j^i \in A} f\left(X_j^i\right) = \sum_{X_j^i \in A^1} f\left(X_j^i\right) = \sum_{\hat{X}_j^i \in M^1 / N_{M^1}(X_0)} g\left(\hat{X}_j^i\right) =$$

$$\sum_{\hat{X}_j^i \in M / N_M(X_0)} g\left(\hat{X}_j^i\right) = \sum_{\hat{X}_j^i \in M} g\left(\hat{X}_j^i\right) - \sum_{\hat{X}_j^i \in N_M(X_0)} g\left(\hat{X}_j^i\right)$$

Що й потрібно було довести.

З формули (4) безпосередньо випливає, що задача (1) зводиться до наступної допоміжної задачі: знайти в множині X кількість X_0^*, $\left|X_0^*\right| = p$ для якого $R_M\left(X_0^*\right)$ максимально.

Теорема 2. Нехай $X^0 \subset X$, $X^0 = \left\{x_1^0, x_2^0, ..., x_p^0\right\}$, де елементи $x_1^0 \in X^0$ виходять наступним чином: за x_1^0 беремо вершину, для котрій $R_M\left(\left\{x_1^0\right\}\right) = \max_{x \in X} R_M\left(\{x\}\right)$, за x_2^0 – вершину, для котрої $R_{M1}\left(\left\{x_2^0\right\}\right) = \max_{x \in X / \left\{x_1^0\right\}} R_{M_1}\left(\{x\}\right)$, де за x_3^0 – вершину, для котрій $R_{M2}\left(\left\{x_3^0\right\}\right) = \max_{x \in X / \left\{x_1^0, x_2^0\right\}} R_{M2}\left(\{x\}\right)$, де $M_2 = M_1 / N_{M_1}\left(\left\{x_2\right\}\right)$ та т. п., за x_p^0 – обираємо вершину, для котрої $R_{M\,p-1}\left(\left\{x_p^0\right\}\right) = \max_{x \in X / \left\{x_1^0, ..., x_{p-1}^0\right\}} R_{Mp-1}\left(\{x\}\right)$, де $M_{p-1} = M_{p-2} / N_{Mp-2}\left(\left\{x_{p-1}^0\right\}\right)$. Тоді кількість X_0 є оптимальним рішенням допоміжної задачі, отже, і завдання (1), тобто $X_0 = X_0^*$.

Доказ теореми передує.

Лема 3. Нехай $M^1 \in M$, $Y \subset X$ – довільні множини, а $x \in X$ – довільна вершина. Тоді в множині Y існує вершина y така, що:

$$N_{M^1}\left(\{x\}\right) \cap N_{M^1}\left(\{y\}\right) = N_{M^1}\left(\{x\}\right) \cap N_{M^1}(y).$$

Доведення. Нехай i_1 – найменша з тих j, для яких $\hat{X}_{j_1}^{i_1} \in N_{M_1}\left(\{x\}\right) \cap N_{M_1}(Y)$. Оскільки структура множин $\hat{X}_j^i \in M^1$ така, що будь-які з них або не мають загальних вершин, або одне з них повністю міститься в іншому, то:

$$N_{M^1}\left(\{x\}\right) \cap N_{M^1}(Y) = \left\{ X_j^i \in M^1 / \hat{X}_j^i \cap \hat{X}_{j_1}^{i_1} \neq \varphi \right\},$$

отже: $N_{M^1}\left(\{x\}\right) \cap N_{M^1}(Y) = N_{M^1}\left(\{x\}\right) \cap N_{M^1}\left(\hat{X}_{j_1}^{i_1}\right)$.

Можливо відмітити, що $\forall y \in \hat{X}_{j_1}^{i_1}$, $N_{M^1}(\{x\}) \cap N_{M^1}\left(\{y\}\right) = N_{M^1}\left(\{x\}\right) \cap N_{M^1}\left(\left\{\hat{X}_{j_1}^{i_1}\right\}\right)$.

Сумісно з попередньою рівністю отримуємо:
$N_{M^1}(\{x\}) \cap N_{M^1}(\{y\}) = N_{M^1}(\{x\}) \cap N_{M^1}(Y)$.

Лема доведена.

Для доказу теореми 2 необхідна ще одна властивість кінцевих множин, що доводиться лемою 4.

Лема 4. Якщо Y_1, Y_2, Y_3, Y_4 – довільні кінцеві множини і якщо $Y_1 \cap Y_3 \subset Y_2 \cap Y_3$, то $Y_1 \cap (Y_3 / Y_4) \subseteq Y_2 \cap (Y_3 / Y_4)$.

Доказ леми очевидний.

Тепер після доказів Леми 3 та Леми 4 можна приступити до доказу теореми 2.

Доказ теореми 2. Нехай $X_0^* = (x_1^*, x_2^*, ..., x_p^*)$ – оптимальне вирішення допоміжного завдання. Припустимо, що $X_0^* \neq X^0$. Розглянемо першу з вершин, яка виходить згідно з правилом, викладеним у теоремі, і не належить множені X_0^*.

Множину X_0^* представимо у вигляді $X_0^* = X_r^o \bigcup X_r^*$, де $X_r^0 = \{x_i^0 \in X^0 / i \prec 0\}$, а $X_r^* = X_0^* / X_r^0$. Беремо довільну вершину $x_s^* \in X_r^*$ та будуємо множину:

$$Y_1^* = (X_0^* / \{x_s^*\}) \cup \{x_r^0\} = X_r^0 \cup (X_r^* / \{x_s^*\}) \cup \{x_r^*\}.$$

Згідно (1) маємо:

$$R_M(X_0^*) = R_M(X_r^0) + R_{M_1}(X_r^*), \qquad (5)$$

де:

$$M_1 = M / N_M(X_r^0);$$
$$R_M(Y_1^*) = R_M(X_r^0) + R_{M_1}[(X_r^* / \{x_s^*\}) \cup \{x_r^0\}]. \qquad (6)$$

Використавши співвідношення (2) для $R_M(X_r^*)$ і $R_{M_1}[(X_r^* / \{x_s^*\}) \cup \{x_r^0\}]$, отримуємо:

$$R_M(X_r^*) = R_{M_1}(\{x_s^*\}) + R_{M_1}(X_r^* / \{x_s^*\}) - \sum_{X_j^i \in \hat{N}_{M_1}(\{x_s^*\}) \cap N_{M_1}(X_r^S / \{x_s^*\})} g(\hat{X}_j^i), \qquad (7)$$

$$R_{M1}[(X_r^* / \{x_s^*\}) \cup \{x_z^0\}] = R_{M_1}(\{x_r^0\}) + R_{M_1}(X_r^* / \{x_s^*\}) - \sum_{X_j^i \in \hat{N}_{M_1}(\{x_r^*\}) \cap N_{M_1}(X_r^* / \{x_s^*\})} g(\hat{X}_j^i). \qquad (8)$$

Згідно Леми 3 у множині X_r^* існує вершина x_q^*, така, що:

$$N_{M_1}(\{x_r^0\}) \cap N_{M_1}(\{x_q^*\}) = N_{M_1}(\{x_r^0\}) \cap N_{M_1}(X_r^*). \qquad (9)$$

Маємо до уваги, що $N_{M_1}(\{x_q^*\}) \subseteq N_{M_1}(X_r^*)$, $N_{M_1}(\{x_r^0\}) \cap N_{M_1}(\{x_q^*\}) \subseteq N_{M_1}(\{x_q^*\}) \cap N_{M_1}(X_r^*)$.

З цього виразу та зі (9) слідує:

$$N_{M_1}(\{x_r^0\}) \cap N_{M_1}(\{x_r^*\}) \subseteq N_{M_1}(\{x_q^0\}) \cap N_{M_1}(X_r^*),$$

тобто

$$N_{M_1}(\{x_r^0\}) \cap [N_{M_1}(X_r^* / \{x_q^*\}) \cup N_{M_1}(\{x_q^*\})] \subseteq \subseteq N_{M_1}(\{x_q^*\}) \cap [N_{M_1}(X_r^* / \{x_q^*\}) \cup N_{M_1}(\{x_q^*\})],$$

звідки на основі Леми 4 отримуємо:

$$N_{M_1}(\{x_r^0\}) \cap N_{M_1}(X_r^* / \{x_q^*\}) \subseteq \subseteq N_{M_1}(\{x_q^*\}) \cap N_{M_1}(X_r^* / \{x_q^*\})]. \qquad (10)$$

Таким чином, якщо обрати, $X_s^* = X_q^*$, то через отримане співвідношення (10) завжди виконуватиметься нерівність:

$$\sum_{X_j^i N_{M_1}(\{x_r^0\}) \cap N_{M_1}(x_r^* / \{x_s^*\})} g(\hat{X}_j^i) \leq \sum_{X_j^i \in N_{M_1}(\{x_s^*\}) \cap N_{M_1}(x_r^* / \{x_s^*\})}.$$

Маємо на увазі, що $R_M(\{x_r^0\}) \geq R_M(\{X_s^*\})$, з урахуванням виразів (4) - (8) та $R_M(\{X_r^0\}) \leq R_M(\{Y_1^*\})$.

Звідси і з того, що X_0^* є оптимальним рішенням допоміжного завдання, випливає те, що $R_M(X_0^*) = R_M(Y_1^*)$ також оптимальне рішення для цього завдання.

Якщо $Y_1^* \neq X^0$, то відносно Y_1^* можна провести аналогічні міркування та знайти нове рішення Y_2^*. Продовжуючи цей процес, через кілька кроків отримуємо множену $Y_1^* = X^0$, що і буде оптимальним рішенням допоміжного завдання, а отже, і нашого завдання. Тобто, Теорему 2 доведено.

Зауважимо, що завдання можна вирішувати ефективно і у випадку, коли множина X_0^* визначається в деякому підмножині $Y \subset X$, $|Y| = P_1 \succ P$. Правила вибору множини за такого обмеження можна отримати, якщо в умовах Теореми 2 замінити X на Y.

Зазначимо також, що розглянута допоміжна задача є окремим випадком іншої, більш загаль-

ної, яку зручно формулювати на підставі теорії гіперграфів: заданий гіперграф, $\xi=(X,\varepsilon)$, $|X|=n$, де кожному гіпер ребру $E_j\subset\varepsilon$ поставлено у відповідність число $g(E_j)\geq 0$; потрібно знайти підмножину $Y^*\subset X$, $|Y^*|=p$, для якого $R(Y^*)=\max\limits_{\substack{Y\subset X\\|Y|=p}}P(Y)$, де $R(Y)=\sum\limits_{\substack{E_i\subset\varepsilon\\E_i\cap Y\neq\varphi}}g(E_i)$.

Справді, пара (X,Y) визначає гіперграф, а кожному підмножині $\widehat{X}_j^i\in M$ поставлено у відповідність число $g=(\widehat{X}_j^i\geq 0)$. Одного гіперграфа (X, M) має таку властивість: будь-які два гіперграфи або не мають загальних вершин, або одне з них вкладено в інше. Як було показано (Теорема 2), у цьому випадку завдання вирішується ефективно. У загальному випадку, коли гіперграф може і не мати цієї властивості, навряд чи існують оптимальні алгоритми її вирішення, оскільки неважко показати, що її можна віднести до класу комбінаторних завдань.

ВИСНОВКИ

Запропоновано обґрунтований математичний апарат знаходження оптимальної конфігурації захисної мережі зв'язку із заданим числом абонентів. Новизна запропонованого математичного апарату базується на доведених чотирьох лемах та доведених двох теоремах. Таким чином, мета роботи з розробки нового варіанту математичного апарату забезпечує оптимальну конфігурацію захищеної мережі зв'язку із заданим числом абонентів досягнуто. Напрямком подальших досліджень може бути розробка програмної реалізації наведеного математичного апарату.

ЛІТЕРАТУРА

[1]. Boryseiko, O.; Laptiev, O.; Perehuda, O.; Ryzhov, A. Optimizing Energy Conversion in a Piezo Disk Using a Controlled Supply of Electrical Load. Axioms 2023, 12, 1074. https: // doi.org / 10.3390 /axioms-12121074.

[2]. Barabash O., Laptiev O., Grushina O. The conceptual model of the intelligent network. Сучасний захист інформації, No4 (56), 2023, pp. 1-9. https:/ /doi.org/ 10.31673/2409-7292.2023.030202.

[3]. Лаптєв О., Зозуля С. Метод виключення відомих сигналів при скануванні заданого радіодіапазону. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». Том 2 № 22 (2023). С. 31-38. https: // doi.org / 10.28925/2663-4023.2023.22.3138.

[4]. Sobchuk V., Sobchuk A., Laptiev S., Laptieva T., Hrebennikov A., Bobrov S. Investingation of dynamic processes in information networks with the application neural networks. International independent scientific journal. Poland. Vol.1, №26, 2021. pp. 36-42.

[5]. Sobchuk V., Breslavsky V., Laptiev S., Laptieva T., Zahynei A., Kovalenko O. Development of routing algoritm for self-organizing information networks. German International Journal of Modern Science №7, Vol. 2, 2021. pp. 32-35, ISSN (Print) 2701-8369, ISSN (Online) 2701-8377.

[6]. Замрій І.В., Собчук А.В., Лаптєв С.О., Лаптєва Т.О., Копитко С.Б. Алгоритм контролю та прогнозування функціональної стійкості складних інформаційно-технічних систем. Телекомунікаційні та інформаційні технології. № 1 (74). 2022. С. 4-15.

[7]. Laptiev O., Lukova-Chuiko N., Laptiev S., Laptieva T., Savchenko V., Yevseiev S. Development of a method for detecting deviations in the nature of traffic from the elements of the communication network. International Scientific and Practical Conference "Information Security and Information Technologies": Conference Proceedings. 13-19 September 2021. Kharkiv, Odesa, Ukraine. pp. 1-9, ISBN 978-966-676-818-9.

[8]. Lukova-Chuiko, N., Herasymenko, O., Toliupa, S., Laptieva, T., Laptiev, O. The method detection of radio signals by estimating the parameters signals of eversible Gaussian propagation. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021, Proceedings, 2021, pp. 67-70.

[9]. Al-Dalvash A. Models of optimal fuel functioning of remote access security in information networks. Ukrainian Scientific Journal of Information Security, vol. 26, issue 3. 2021.P. 126-131. DOI: 10.18372 /2225-5036.27.16513

[10]. В. О. Хорошко, Ю. Є. Хохлачова, А. Аясрах, А. Аль-Далваш Оптимізація інформаційних структур локальних мереж. Інформатика та математичні методи в моделюванні. Т. 10, № 1-2. 2020. С. 45-54.

[11]. Володимир Хорошко, Юлія Хохлачова, Олена Скоробогатько, Микола Тимченко. Синтез оптимальної топології мережі передачі даних. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2 (28), С. 20-28.

[12]. Oleksandr Laptiev, Volodymyr Tkachev, Oleksii Maystrov, Oleksandr Krasikov, Pavlo Open'ko, Volodimir Khoroshko, Lubomir Parkhuts. The method of spectral analysis of the determination of random digital signals. International Journal of Communication Networks and Information Security (IJCNIS). Vol 13, No 2, August 2021 pp .271-277. ISSN: 2073-607X (Online). DOI: 10.54039/ijcnis. v13i2.5008.

[13]. Lukova-Chuiko, N., Herasymenko, O., Toliupa, S., Laptieva, T., Laptiev, O. The method detection of radio signals by estimating the parameters signals of

eversible Gaussian propagation. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021. Proceedings, 2021, pp. 67-70.

[14]. Roman Kyrychok, Oleksandr Laptiev, Rostyslav Lisnevsky, Valeri Kozlovsky, Vitaliy Klobukov. Development of a method for checking vulnerabilities of a corporate network using bernstein transformations. Eastern-European journal of enterprise technologies. Vol. 1 №9 (115), 2022, pp. 93-101. ISSN (print) 1729-3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2022.253530.

[15]. Valentyn Sobchuk, Iryna Zelenska and Oleksandr Laptiev. Algorithm for solution of systems of singularly perturbed differential equations with a differential turning point. Bulletin of the Polish Academy of Sciences Technical Sciences, Vol.71, No 3, 2023, Article number: e145682 DOI: 10.24425/bpasts.2023.145682 WoS.

MATHEMATICAL APPARATUS FOR FINDING THE OPTIMAL CONFIGURATION OF A SECURED COMMUNICATION NETWORK WITH A GIVEN NUMBER OF SUBSCRIBERS

Information flows in the world are growing very quickly. The exchange of information is growing rapidly. In connection with this fact, the existing mathematical apparatus and its practical application are constantly developing. The scientific-mathematical apparatus is aimed at finding the optimal configuration of the information communication network, solving the problem of building protected channels for the transmission of a large amount of data. A scientific task arises to develop a new and improve the existing mathematical apparatus for finding the optimal configuration of a protected communication network with a given number of subscribers. This scientific work is dedicated to the solution of this urgent task. The paper formulated and proved four Lemmas. The Lemma's formulation made it possible to prove two new theorems that allow solving the task of finding the optimal configuration of a protected communication network with a given number of subscribers. Solutions to both partial and general tasks of the process of optimization and protection of transmission channels of a large amount of data are provided. Thus, the paper proposes a solution to the scientific task of finding the optimal configuration of a protected communication network with a given number of subscribers. The direction of further research may be the development of a software implementation of the given mathematical apparatus.

Keywords: secure networks, optimal configuration, information protection, data security, cyber security.

Лаптєв Олександр Анатолійович, доктор технічних наук, старший науковий співробітник, доцент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка, Київ, Україна.

Oleksandr Laptiev, Doctor of Technical Science, Senior Researcher, Associate Professor the Department of Cyber Security and Information Protection, Faculty of Information Technology, Taras Shevchenko National University of Kyiv.
E-mail: olaptiev@knu.ua.
Orcid ID: 0000-0002-4194-402X.

Аль-Далваш Аблуллах Фоуад, аспірант Національного авіаційного університету, Київ, Україна.

Al-Dalvash Ablullah Fowad, graduate student of the National Aviation University, Kyiv, Ukraine.
E-mail: abdullah.dalosh@gmail.com.
Orcid ID: 0000-0001-1003-9182.

DOI: 10.18372/2410-7840.26.18821
УДК 004.056.52:004.056.53

ДОСЛІДЖЕННЯ ВЗАЄМОЗВ'ЯЗКІВ МІЖ СЕМАНТИЧНИМИ ПАРАМЕТРАМИ ДЛЯ ГАЛУЗІ БЕЗПЕКИ СИСТЕМ ДОСТУПУ

Анатолій Давиденко, Олена Висоцька, Михайло Пригара, Володимир Бичков

Системи розмежування доступу привертають увагу за рахунок першочерговості під час контакту з інформаційною системою та критичністю збоїв при її роботі. Тому вона є важливою типовою підсистемою будь-якої інформаційної системи. Перед розробником нової інформаційної системи завжди виникає дилема – або розробка цієї підсистеми з нуля або адаптація вже готового рішення. Якщо виключити аспекти вартості та авторського права, критичним для вирішення дилеми є технічна можливість та складність такої адаптації. У цій статті досліджується потенційне застосування типової підсистеми розмежування доступу в різних предметних областях, з акцентом на унікальність сфери застосування та визначення вимог та обмежень, що виникають при процедурі адаптації. Інтуїтивно зрозуміло що близькість предметних областей інформаційних систем впливає на ефективність адаптації, але для попередньої оцінки доцільності її використання потрібна методологія, яка дозволяє отримати якісний або кількісний результат. Можливим підходом є семантичний аналіз та експертна оцінка на основі різних математичних методів в тому числі нечітких. Метою статті є дослідження можливостей та перспективи використання технології адаптації систем розмежування доступу при розширенні предметної області. Методи дають можливість створювати більш гнучкі засоби оцінювання на основі семантичного аналізу. Використання методів дозволяє отримувати результати, як в кількісній, так і в якісній формі.

***Ключові слова**: розмежування доступу, ідентифікація, надання прав користувачу, семантичний аналіз, міра семантичної надмірності.*