# ПІДХІД ДО ОПТИМАЛЬНОГО СИНТЕЗУ СТРУКТУРИ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

*Олексій Новіков[1], Андрій Родіонов[2]*

Національний технічний університет України «Київський політехнічний інститут»,
пр-т. Перемоги 37, Київ, 03056, Україна, тел.: (044) 236-70-98
E-mail: [1]novi@ptf.ntu-kpi.kiev.ua, [2] randreymail@mail.ru

## Анотація

*Розглянуто питання впливу топології інформаційно-комунікаційних мереж, що мають однакову функціональність та однаковий набір сервісів, на рівень їх захищеності. Виходячи з цього запропонована модель за допомогою якої можна синтезувати топологію мережі оптимальну з позицій підвищення безпеки інформації. Для цього використовується цільова функція ймовірності атаки на об'єкти (ресурси) мережі, що побудована з використанням логіко-імовірнісної моделі. Приведено обчислювальний приклад по визначенню оптимальної структури мережі, який підтвердив працездатність запропонованої моделі.*

## Вступ

У зв'язку з широким використання корпоративних мереж, їх захист та аналіз стану їх захищеності є на даний момент важливою задачею. Особливістю корпоративних мереж є те, що вони мають розподілену структуру з різними рівнями вимог по безпеці, містять багато сервісів та служб, які взаємодіють між собою, утворюючи інформаційні потоки, при цьому надаючи користувачам необхідну функціональність.

Існує багато практичних рекомендацій по розробці структури (топології) корпоративних мережі (від Cisco, Microsoft та ін.), у яких вказується, де саме і як слід розміщувати відповідні сервіси мережі – Веб-сервер, сервер електронної пошти, міжмережевий екран, … Але не пропонується формалізації цього процесу та методу за допомогою якого можна було б оцінити стан захищеності корпоративної мережі.

Серед підходів та моделей, які оцінюють захищеність корпоративної мережі та її ресурсів поширеними є дерево атак (attack tree) [1, 2] та більш формалізована модель - граф атак (attack graph) [3-5]. В цих моделях розглядаються можливі атаки на систему, які експлуатують відомі вразливості кожного із сервісів мережі. Згідно з наведеними підходами, для пошуку можливих шляхів проникнення до системи, будується відповідний граф, який враховує топологію мережі. Недоліком цих підходів є необхідність виконання перебору всіх можливих шляхів атак. При цьому, необхідно враховувати можливість послідовної експлуатації вразливостей на кожному хості мережі, що для мереж великих розмірів є важко обчислювальною задачею. Також цей підхід може використовуватися для аналізу вже існуючих мереж, але не дозволяє синтезувати топологію мережі, для якої зменшується ймовірність атак.

Метою роботи є запропонувати модель та підхід який дозволяє на етапі синтезу структури інформаційно-комунікаційної мережі оцінити стан її захищеності і, виходячи з цього, оптимізувати її структури для зменшення ймовірності атак на її ресурси.

## Аналіз структури корпоративної мережі

Структура корпоративної мережі являє собою набір сервісів, склад яких та взаємодія між собою визначаються відповідно до функціональних потреб організації та прийнятої політики безпеки. При цьому під час проектування мережі може існувати декілька варіантів її топології при абсолютно ідентичному її функціонуванні. З точки зору захисту інформації деякі варіанти розміщення сервісів на хостах мережі є більше, а деякі менше прийнятними.

Розглянемо приклад двох мереж з однаковим складом сервісів та функціональністю, але різними топологіями.

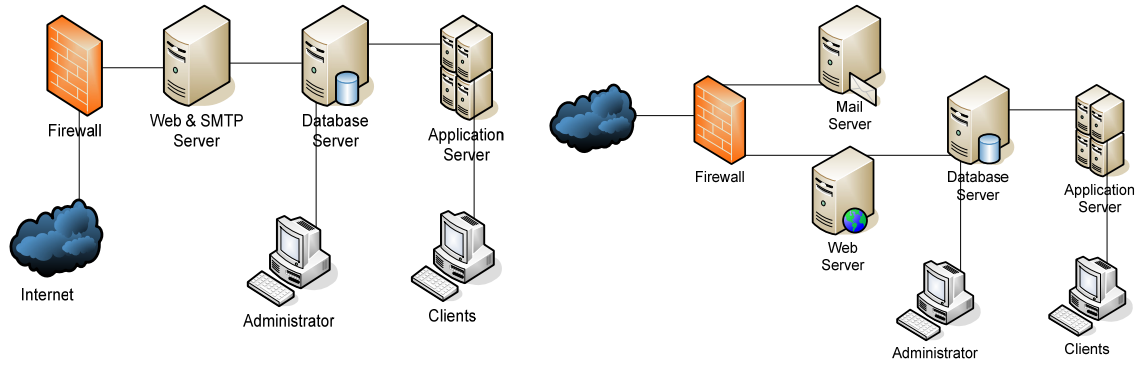
У першому випадку Веб-сервер суміщений з сервером електронної пошти - Рис1. (а), у другому випадку сервер електронної пошти та Веб-сервер розміщенні на різних хостах мережі – Рис 1, (б).

З точки зору безпеки другий варіант є більш прийнятним оскільки, у разі злому одного з серверів інший автоматично не опиниться під загрозою.

Таким чином захищеність системи буде залежати від її топології. Для локальних мереж невеликих розмірів задачу побудови (синтезу) їх топологій оптимальних з точки зору безпеки можна виконати безпосередньо, але для великих корпоративних систем це є нетривіальною задачею.

## Математична модель

Топологію мережі можна представити у вигляді графа $G(V,E)$. Де $V$ - множина сервісів мережі, $E$ - наявність зв'язку між ними, $E \subseteq V \times V$. Таким чином будується матриця зв'язаності сервісів.




(а) (б)

Рис.1. Мережі з однаковою функціональністю але різними топологіями

## Математична модель

Топологію мережі можна представити у вигляді графа $G(V,E)$. Де $V$ - множина сервісів мережі, $E$ - наявність зв'язку між ними, $E \subseteq V \times V$. Таким чином будується матриця зв'язаності сервісів.

Топологій мереж з однаковою функціональністю та складом сервісів може бути декілька. Їх структура будуть визначатися наступними обмеженнями:

- з точки зору функціональності,
- залежності сервісів один від одного,
- політики безпеки прийнятій у корпоративній системі.

Таким чином отримаємо множину $O(G) = \{G_1, G_2, ..., G_k\} \subseteq \Omega$, де $G_i$ - припустимі варіанти топологій мережі, а $\Omega$ - всі можливі варіанти топології мережі.

Нехай у загальному випадку функція $P(G): \Omega \to [0,+\infty)$ визначає стан захищеності системи і залежить від топології мережі.

Таким чином необхідно вирішити задачу структурної оптимізації: знайти топологію мережі (структуру графа), яка забезпечує екстремум цільової функції захищеності системи. У якості цільової функції буде виступати $P(G)$.

Формалізований вигляд задачі буде наступний:

$$G^* = \arg\min_{G \in O} P(G).$$

Задачі даного типу розглянуті та проаналізовані у [6]. Для загального вигляду цільової функції та структури мережі, це є задачею, складність якої збільшується експоційно з кількістю хостів.

Але завдяки обмежень на прийнятні варіанти топологій мережі розмірність $|O(G)|$ всіх можливих варіантів може бути значно зменшена.

Далі розглянемо варіант цільової функції, яка враховуючи топологію мережі дозволяє визначити ймовірність атак на її ресурси.

## Побудова цільової функції

У якості цільової функцією використаємо функцію ймовірність атаки, яка отримана за допомогою логіко-імовірнісного підходу. Цей підхід був запропонований та розвинутий І.О. Рябініним [7] для опису структурно складних систем.

Відповідно до нього, для оцінювання рівня захищеності компонентів інформаційно-комунікаційних систем, послідовність дій зловмисника та всі шляхи, якими він може отримати доступ до об'єктів системи, формують сценарії атак або функцію небезпечного стану (ФНС) логіко-імовірнісній теорії [8]. Далі ФНС записується у вигляді функції алгебри логіки

$$\varphi_l = \bigwedge_{i \in K_{\varphi_l}} Z_i,$$

де $Z_i$ - події, які необхідні виконати зловмиснику для здійснення атаки,

$K_{\varphi_l}$ - послідовність дій зловмисника у корпоративній комп'ютерній системі, що приводить, до

небезпечного стану визначеного об'єкта системи, яка відповідає l-тому сценарію атаки.

$$Z_i = \begin{cases} 1, \text{ i - та подія відбулась,} \\ 0, \text{ i - та подія не відбулась.} \end{cases}$$

Виходячи з цього, усі атаки на об'єкти корпоративної мережі можна представити у вигляді ФНС - скінченого набору сценаріїв атак (l=1, 2, …, d), та подій $Z_i$, (де $i \in K_{\varphi_l}$):

$$y(Z_1,...,Z_m) = \bigvee_{l=1}^{d} \varphi_l = \bigvee_{l=1}^{d} \left[ \bigwedge_{i \in K_{\varphi l}} Z_i \right] \quad (1)$$

Згідно з логіко-імовірнісною теорією, імовірність переходу об'єкта корпоративної мережі до небезпечного стану буде формулюватись так:

$$P\{y(Z_1,...,Z_m) = 1\} = P\left\{ \bigvee_{l=1}^{d} \left[ \bigwedge_{i \in K_{\varphi l}} Z_i \right] = 1 \right\} \quad (2)$$

Далі, маючи імовірність здійснення кожної з подій $Z_i$, то можна обчислити й $P\{y(Z_1,...,Z_m) = 1\}$. Для цього необхідно перетворити ФНС (1) у еквівалентну їй форму: ортогональна диз'юнктивна нормальна форма, доскональна диз'юнктивна нормальна форма чи безповторна функція у базисі кон'юнкцій-заперечень [9]. Для них можна виконати пряме заміщення булевих змінних $Z_i$ на їх імовірнісні значення $P\{Z_i = 1\} = P_i$.

Таким чином, атаки та сценарії атак будуть залежати від топології мережі $G$ і, функція ймовірності атаки $P(G) = P\{y(Z_1,...,Z_m) = 1\} \in [0,1]$ буде необхідною цільовою функцією.

## Приклад моделювання

Для топологій мереж, які наведені на Рис. 1, за допомогою запропонованої моделі оцінимо яка з них є оптимальною.

Виходячи з Рис.1, для $O(G) = \{G_1, G_2\}$ і необхідністю знайти $G^* = \arg\min_{G \in O} P(G)$.

Для цього, у відповідності до логіко-імовірнісного підходу необхідно записати функцію ймовірності атаки для топологій $G_1$ та $G_2$.

Відповідно до роботи [10] для кожної з топологій мереж будується матриці доступу сервісів між собою, визначаються категорії зловмисників та сервіси системи до яких зловмисники можуть отримати доступ. На основі цього отримуємо сценарії атаки та послідовну множину умов необхідних для їх здійснення. Далі здійснюється представлення сценарію атаки у вигляді графу, що складається з комбінації умов необхідних для здійснення атаки. Вершиною графу є доступ зловмисника до об'єкту захисту, листами – умови, а у якості проміжних вершин логічні комбінації цих умов. Граф спочатку записується у вигляді (1), а потім здійснюється перехід до ймовірнісної форми (2).

Після здійснення відповідно кроків для мережі з топології $G_1$ функція ймовірності атаки на сервер бази даних буде мати вигляд

$$P(G_1) = 1 - [1 - P_1(1 - (1 - P_2)(1 - P_3))][(1 - P_4)(1 - P_5 P_6)],$$

а для мережі з топологією $G_2$

$$P(G_2) = 1 - [1 - P_1 P_3][(1 - P_4)(1 - P_5 P_6)],$$

де $P_1,...,P_6$ – ймовірність реалізації кожної з умов:

$P_1$ – захоплення Firewall;
$P_2$ – захоплення Mail Server;
$P_3$ – захоплення Web Server;
$P_4$ – захоплення АРМ-а Administrator;
$P_5$ – захоплення АРМ-а Clients;
$P_6$ – захоплення Application Server.

Для того щоб вибрати з двох топологій мереж оптимальну, візьмемо значення ймовірностей

$P_1 = P_2 = ... = P_6 = 0{,}5$.

Отримаємо $P(G_1) = 0{,}77$, а $P(G_2) = 0{,}72$.

Виходячи з результатів бачимо, що варіант мережі з окремим сервером електронної пошти є більш прийнятним з точки зори безпеки.

Хоча наведений вище прикладу не є складним, але на ньому видно, як можна формально оцінити оптимальність топології мережі з точки зори інформаційної безпеки.

## Висновки

У статті запропоновано модель для визначення оптимальної топології інформаційно-комунікаційної мережі з точки зору інформаційної безпеки. Отримані результати можуть бути застосовані для мереж будь-якого розміру, як локальних так і корпоративних. Для корпоративних мереж з великою кількістю сервісів можливо багато варіантів їх топології, цільова функція ймовірності захищеності буде містити багато змінних та мати складний вигляд. Тому необхідно розробити ефективний алгоритм перебору можливих варіантів топологій та на їх основі автоматизувати процес побудови цільової функції.

Основними труднощами при застосування цієї моделі та алгоритму для великих мереж є наступне:

- зменшення кількості варіантів топологій мережі;
- складання матриці доступності сервісів між собою, її аналіз та побудова за нею сценарію атак;
- перетворення ФНС до однієї з форм, що допускає пряме заміщення булевих на їх імовірнісні значення.

Наведено обчислювальний приклад використання запропонованої моделі для визначення оптимальної топологій для двох мереж, що мають однаковий набір сервісів та функціональність.

У подальших дослідженнях необхідно розробити автоматизації процедури побудови варіантів топологій мереж, визначити характеристики топології, що підвищують захищеність, виконати дослідження моделі при загальному вигляді цільової функції з метою оптимізації алгоритму, включити до моделі механізми захисти, та розробити алгоритм по їх оптимальному розміщенню.

Запропонована модель може бути використані при (синтезі) проектуванні інформаційно-комунікаційних систем, а також під час їх експлуатації.

## Література:

[1] Брюс Шнайер. Секреты и ложь. Безопасность данных в цифровом мире. Питер; СПб. – 2003
[2] ISBN 5-318-00193-9 - 368 с.
[3] Schneier, Bruce (December 1999). "Attack Trees". Dr Dobb's Journal, v.24, n.12. Retrieved on 2007-08-16
[4] Oleg Sheyner, Jeannette Wing. Tools for Generating and Analyzing Attack Graphs. www.cs.cmu.edu/~scenariograph/sheynerwing04.pdf
[5] Sheyner O., Jha S., Wing J. Two Formal Analyses of Attack Graphs. // IEEE Computer Security Foundations Workshop, Cape Brenton, Nova Scotia, Canada. – June 2002. – P. 49–63.
[6] Todd Hughes, Oleg Sheyner: Attack scenario graphs for computer network threat analysis and prediction. Complexity 9(2) (ISSN: 1076-2787): 15-18 (2003)
[7] Воронин А.А., Мишин С.П. Оптимальные иерархические структуры - М.: ИПУ РАН, 2003 – 214 с.
[8] Рябинин И. А. Надежность и безопасность структурно-сложных систем. - СПб.: Политехника, 2000. - 248 с.
[9] Качинский А.Б. Безпека, загрози і ризики: наукові концепції та математичні методи. – К.:2003.–472 с.