РАДІОТЕХНІКА ТА ТЕЛЕКОМУНІКАЦІЇ

УДК 621.396

Євдокименко М.О.
Харківський національний університет радіоелектроніки

Шаповалова А.С.
Харківський національний університет радіоелектроніки

МЕТОД ОЦІНЮВАННЯ ВПЛИВУ АТАК НА ІНФОКОМУНІКАЦІЙНУ МЕРЕЖУ З УРАХУВАННЯМ НАЯВНИХ ВРАЗЛИВОСТЕЙ

У статті досліджуються методи оцінювання критичності вразливостей та оцінювання розповсюдження атак в інфокомунікаційній мережі. Представлено проактивний підхід до кількісного оцінювання мережної безпеки, який дає змогу оцінити ризики на рівні користувача й мережі через наявність вразливостей. Запропоновані рішення будуть корисні для прийняття рішень і додатково інтегровані в єдину метрику для відображення сукупного рівня безпеки інфокомунікаційної мережі.

Ключові слова: *інфокомунікаційна мережа, вага, оцінювання вразливості, інформаційна безпека.*

Постановка проблеми. Одним із важливих аспектів під час побудови сучасних інформаційно-комунікаційних мереж є забезпечення безпеки передачі інформації між кінцевими користувачами. Для цього натепер у процесі побудови сучасних інформаційно-комунікаційних мереж найчастіше використовують два етапи: створення інтегрованого захисту на базі таких елементів мережі, як комутатори й маршрутизатори, і використання спільного захисту, що включає побудову зв'язків між елементами мережного захисту. Однак така побудова захисту мережі в умовах постійного розвитку інфокомунікаційних технологій і, відповідно, кількості різнорідних атак, що зростає, не є повноцінним захистом і вимагає перегляду. Як і раніше, «вузьким» місцем є швидке реагування на атаки, що виникають, із мінімізацією можливості їх поширення. Тому виникає необхідність у розробці математичної моделі оцінювання поширення атаки в мережі.

Аналіз останніх досліджень і публікацій. Оцінювання вразливості мережі є досить складним завданням з огляду на гетерогенність обладнання та програмного забезпечення. Сьогодні використовується спеціалізоване апаратне або програмне забезпечення (наприклад, GFI LanGuard, Nessus, XSpider тощо), яке сканує мережу на предмет виявлення слабких місць у системі безпеки й попереджає про зони ризику в інфокомунікаційній мережі. Ці програми дають змогу оцінити мережну безпеку за допомогою активного та пасивного аналізу. Під активним аналізом (наприклад, тестування на проникнення) розуміється імітація атак зловмисника, яка перевіряє наявність вразливостей у мережі. Пасивний аналіз полягає в пошуках вразливостей за непрямими ознаками без підтвердження їх наявності, наприклад, наявність відкритих портів, перевірка заголовків протоколів тощо. При цьому для оцінювання безпеки мережі найчастіше необхідно використовувати ці два аналізи в сукупності. Насамперед варто використовувати пасивний аналіз як більш швидкий, але менш точний. Потім, після усунення виявлених вразливостей у результаті пасивного аналізу, доцільно використовувати активний аналіз, який за часом повільний, але більш точний.

Крім того, для оцінювання безпеки інфокомунікаційної мережі можуть використовуватися організаційні стандарти, оцінювання брандмауерів і їх політик безпеки для корпоративних мереж (Virtual Private Network, VPN), метод оцінювання ризиків, що базується на побудові графа атак. Також використовуються кількісні оцінки безпеки, що базуються на чутливості системи до атак, метрики безпеки, засновані на аналізі найслабшого супротивника (тобто мінімальному зусиллі, що необхідне для успішної атаки) з прогнозуванням і вимірюванням вразливостей мережі. Однак усі перераховані вище методи переважно намагаються виявити наявні ризики й

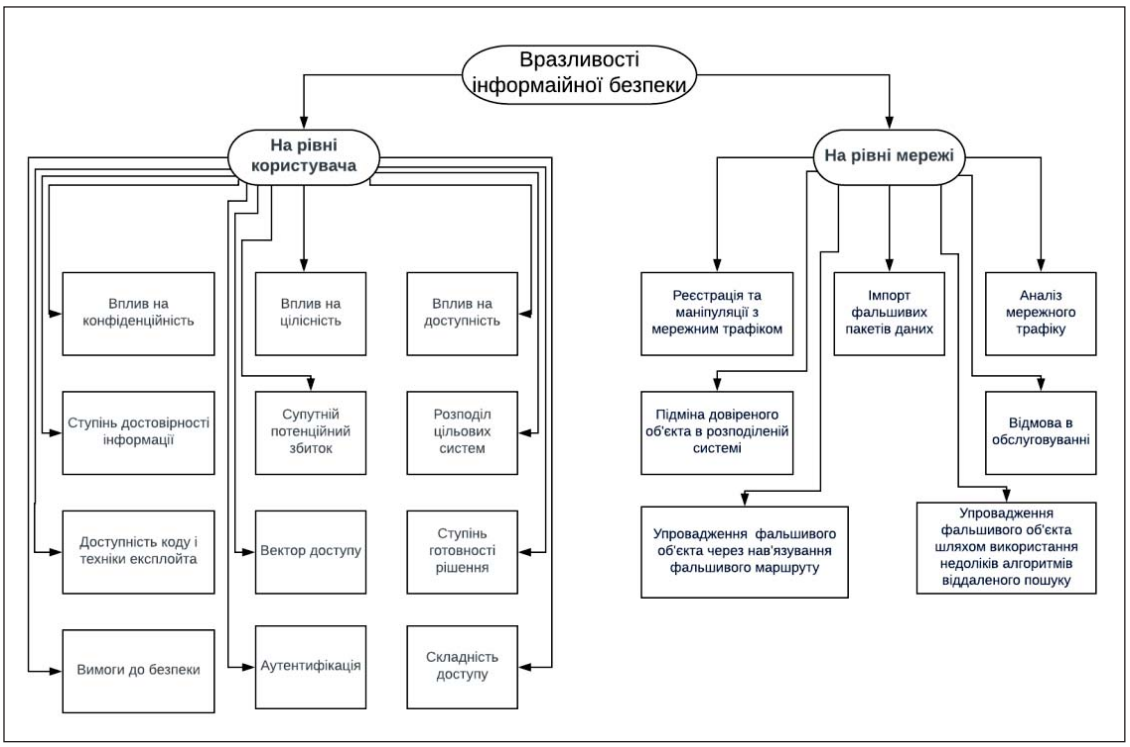

Рис. 1. Класифікація вразливостей інформаційної безпеки на рівні користувача та на рівні мережі

не вирішують проблеми кількісної оцінки безпеки системи в момент, коли вразливість використана й атака поширюється в мережі від вузла до вузла.

Для оцінювання поширення тієї чи іншої атаки в інфокомунікаційній мережі необхідно розуміти причину виникнення атаки як результат використання наявної вразливості в мережі, а також можливу шкоду, заподіяну цією атакою. Під час аналізу наявних рішень [1, с. 86; 2, с. 28; 3, с. 29] щодо оцінювання вразливостей і подальшого збитку виявлено, що основним їх недоліком є їх вузька спрямованість на певні елементи мережі, на окремі додатки, сервіси та ресурси, у результаті чого неможливо оцінити ризики та модель поширення атаки в мережі загалом. Виходячи із цього, в роботі пропонується оцінювати вразливості як на рівні мережі, так і на рівні користувача, класифікація яких представлена на рис. 1.

Постановка завдання. Мета статті – оцінити ступінь критичності завданих збитків в умовах успішної реалізації зловмисником атаки й у момент розповсюдження атаки в мережі, використовуючи вагові коефіцієнти; визначити найбільш вразливі місця мережі, використовуючи пасивний аналіз безпеки мережі для мінімізації можливих втрат.

Виклад основного матеріалу дослідження. Безпека інфокомунікаційної мережі залежить від таких факторів, як захищеність кінцевого користувача (планшета, смартфона тощо) і мережних елементів (маршрутизаторів, комутаторів тощо). І якщо захист на рівні мережі можливо забезпечити починаючи з етапу проектування за допомогою наявних контрзаходів (брендмауер, IDS/IPS тощо), то на рівні користувача забезпечення безпечної передачі даних є досить важким завданням і практично неможливим. Коли на користувальницькій стороні є вразливості (відсутність антивірусних програм, незахищене підключення до локальних мереж і мережі Internet, помилки під час авторизації тощо), то їх використання зловмисником є ризиком для інфокомунікаційної мережі.

У разі виявлення вразливості на стороні користувача потрібен час, перш ніж будуть вжиті відповідні контрзаходи (відмова в доступі, оновлення додатку тощо). Отже, протягом цього часу мережа вразлива для зовнішньої атаки. Для визначення ризику використання наявної вразливості використовуємо експоненціальний розподіл для кількісної оцінки найгіршого сценарію, коли зловмисник використав вразливість і завдав шкоди мережі. Згідно з твердженнями деяких авторів [12, с. 199], існують такі показники потенційного збитку (таблиця 1).

Нехай S_j ($j = \overline{1, J}$) – безліч послуг (наприклад, онлайн відео), що надаються користувачеві мережею, а $V(y_j)$ – безліч вразливостей, які

Таблиця 1

Показники потенційного збитку під час експлуатації вразливостей

Показник	Опис показника
Відсутнє	У результаті успішної експлуатації вразливості втрат немає
Низький	У результаті успішної експлуатації вразливості відбувається незначне зниження продуктивності, збиток мінімальний
Низький – середній	У результаті успішної експлуатації вразливості відбувається зниження пропускної здатності мережі, запити користувачів обробляються довше, ніж визначено в SLA
Середній – високий	У результаті успішної експлуатації вразливості відбувається істотне зниження продуктивності, фінансовий збиток серйозний
Високий	У результаті успішної експлуатації вразливості цими користувача й мережі завдається катастрофічна шкода

виявлені в послугах, тобто $y_j \in S$ $C(y_j)$ – показник критичності вразливості y_i, під яким розуміються завдані збитки мережі. Тоді для розрахунку ризику $R(S)$ використовується вираз, запропонований у праці [7, с. 84],

$$R(S) = w_{y_j} \cdot \ln \sum_{y_j \in V(S)} e^{C(y_j)},$$

де w_{y_i}– вагові коефіцієнти, які використовуються для оцінювання ризику, створювані вразливістю y_i.

На жаль, із практичного погляду для забезпечення безпеки мережі часто аналізують вразливості на рівні користувача вже після того, як мережа зазнала впливу. Також існують ситуації, коли всі найбільш критичні вразливості усунені, але через деякий час мережа знову зазнає впливу з боку користувача. Це відбувається через недостатній з погляду безпеки аналіз пропонованої послуги/сервісу/додатку (особливо це стосується додатків з відкритим кодом і технікою експлойту). Ця ситуація викликає необхідність прогнозування ризиків у разі виникнення нових вразливостей на рівні користувача. Тоді нехай $P_t(y_j^n)$ – імовірність виявлення нової вразливості y_j^n, а $y_j^n \in S$, що надаються в послугах/сервісах/ додатках, яке дасть уявлення про ризики, з якими зіткнеться мережа в майбутньому, $C_n(y_j^n)$ – очікуваний показник критичності вразливості, а $P_z(y_j^n)$ – імовірність використання нової вразливості зловмисником. Тоді для розрахунку очікуваного ризику $R_n(S)$ використовуємо такий вираз:

$$R_n(S) = P_t(y_j^n) \cdot \sum_{y_j^n \in S}^{\infty} C_n(y_j^n) \cdot P_z(y_j^n). \qquad (2)$$

Аналіз наявних досліджень показав [8, с. 215; 9, с. 217; 10, с. 278; 11, с. 108], що саме мережеві політики визначають схильність мережі впливу зовнішніх факторів, а також інтенсивність атаки на мережу (тобто наскільки широко може бути поширена атака). Кількісна оцінка ризику (інтенсивність атаки) на мережевому рівні включає в себе оцінку поширення можливої атаки (RA).

Тоді ступінь, до якої політика допускає поширення атаки всередині мережі, буде визначається метрикою поширення атаки (RA). Поширення атаки оцінюється складністю поширювати атаку по мережі, використовуючи вразливості послуг, що надаються, а також вразливості політики безпеки.

Для подальшого проведення аналізу введемо ймовірність наявності вразливості наданої послуги на i-му вузлі $P_{y_j,i} \in (0,1)$ та оцінку $L_{y_j,i}$, яка визначає вразливість послуги $S_{y_j,i}$ до атаки на i-му вузлі. Тоді $L_{y_j,i}$ обчислюється з $P_{y_j,i}$, комбінованого показника вразливості послуги $S_{y_j,i}$, так:

$$L_{y_j,i} = -\ln(P_{y_j,i}), \qquad (3)$$

при цьому $L_{y_j,i}$ має діапазон $[0,\circ)$ та використовується для вимірювання легкості, з якою зловмисник може поширювати атаку з одного вузла на інший, використовуючи послугу $S_{y_j,i}$ на i-му вузлі. Отже, якщо вузол i може підключатися до вузла j під час передачі трафіку з наданням послуги $S_{y_j,i}$, тоді $L_{y_j,i}$ вимірюється як стійкість вузла k до атаки, ініційованої i-м вузлом.

Для розрахунку метрики поширення атаки з i-го вузла з порушенням роботи інших вузлів, що знаходяться в межах досяжності від i-го вузла, побудуємо мінімальне остовне дерево для сегмента мережі, тобто всіх тих вузлів, які зазнають атаку через i-й вузол. Вага цього мінімального остовного дерева буде визначати, наскільки цей сегмент мережі вразливий до атаки. Чим більш вразлива мережа, тим вищою буде ця вага. Для визначення ваги використовуємо такий вираз:

$$W_i = \sum_{i \in M} (\prod P_{y_j,i}) \cdot \cos t_i, \qquad (4)$$

де $\cos t_i$ відображає вартість збитку при компрометації вузла i, а M – це безліч вузлів, наявних в остовному дереві. Тоді метрика поширення атаки визначається таким виразом:

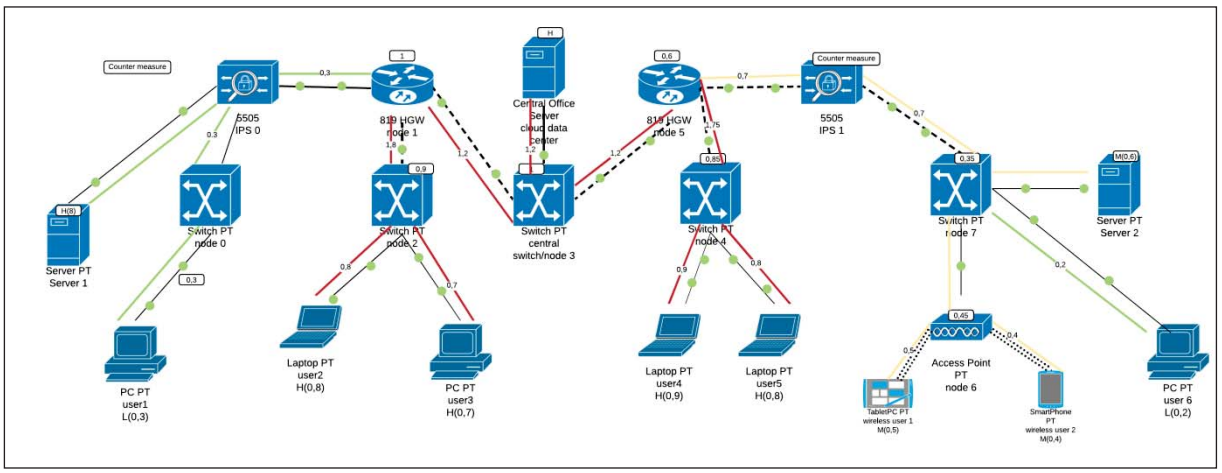

Рис. 2. Експериментальна схема мережі

$$RA = \sum_{i \in M} P_{y_j,i} \cdot W_i \,, \qquad (5)$$

де $P_{y_j,i}$ – ймовірність існування вразливості на i-му вузлі.

Розрахунок оцінки ризиків з боку зовнішніх впливів (External Factor) базується на частці адресного простору, на якому функціонує послуга, тому що саме адресний простір є найбільш «вузьким» місцем під час забезпечення безпеки мережі від зовнішніх впливів. Зовнішні впливи на послугу S_j ураховують кількість портів $Ports(s_j)$ та IP-адресів $IP(s_j)$, при цьому загальна кількість IP-адрес – 232, а загальна кількість портів – 216. Отже, діапазон цього коефіцієнта буде починатися з мінімального значення 1 для повністю прихованого від мережі сервісу й досягне максимального значення 2 для сервісу, повністю схильного до впливу всього адресного простору. Тоді метрика впливу зовнішніх факторів на мережу визначається так:

$$EF(s_j) = 1 + \frac{\log_2(IP(s_j) \cdot Ports(s_j))}{\log_2(2^{32} \cdot 2^{16})}, \qquad (6)$$

припускаючи, що ризик від зовнішньої мережі розподіляється рівномірно. Високе значення цієї метрики вказує на те, що мережа повинна бути розділена, щоб мінімізувати зв'язок у мережі й розповсюдження атак. Отже, ці метрики дають змогу оцінити поширення атаки в мережі.

Згідно із цим підходом, проведено експериментальне дослідження на базі імітованої мережі, що складається з декількох типів кінцевих пристроїв та інтегрованих послуг зв'язку. Атака імітується на рівні додатка через службовий порт 80, який використовує TCP (рис. 2). Для кожного пристрою обрано вразливості з різними вагами, що характеризують критичність самої вразливості.

Якщо розглядати стан, у якому мережа знаходиться під впливом атаки, що розповсюджується від однієї кінцевої точки або декількох кінцевих пристроїв, відповідно до (5)–(6), знаючи ваги наявних вразливостей, можливо оцінити очікуваний ризик по маршрутах передачі даних, що залежить від ваги вразливості на вузлі.

У результаті експерименту на рис. 2 отримані шляхи розповсюдження атаки в мережі від користувача до датацентру в цьому випадку. Вплив і втрати прямо залежать від ваги вразливості (критичності) на рівні кінцевого користувача. Так, від різних користувачів з різними за вагою вразливостями у випадку здійснення втручання зловмисника атака буде розповсюджуватися найкоротшим шляхом до датацентру. У результаті цього мережа розподілена на сегменти за критичністю майбутніх утрат у разі розповсюдження атаки, які показано на рис. 2 різними кольорами. Так, зеленим кольором показано шляхи розповсюдження атаки, які завдасть мінімальні втрати; жовтим і червоним – більш критичні атаки, які реалізовані за допомогою наявних вразливостей, що мають критичну для мережі вагу.

Припустимо, що ризик із зовнішньої мережі розподіляється рівномірно. Високе значення цієї оцінки вказує на те, що для мінімізації мережного з'єднання та поширення атаки мережа повинна бути розділена. Однак на мережному рівні можуть бути прийняті такі запобіжні заходи:

1) реалізація віртуальних локальних мереж;

2) перегрупування мережі, щоб пристрої з еквівалентним ризиком перебували в тій самій ділянці;

3) збільшення кількості контрольних точок (брандмауери, IDS);

4) підвищення безпеки навколо «активних» точок у мережі.

Крім того, дійсні IP-адреси й порти повинні бути ретельно перевірені, щоб гарантувати, що IP-адреса або порти не будуть ненавмисно дозволені.

Висновки. Захищеність інфокомунікаційної мережі залежить від методів вимірювання безпеки й інструментів, які дають змогу мережним адміністраторам аналізувати та оцінювати безпеку. У роботі пропонується проактивний підхід до кількісної оцінки безпеки мереж, який допомагає оцінити ризики на рівні користувача й на рівні мережі за допомогою наявності вразливостей. З урахуванням того, що кожна мережа містить різні за характером вразливості й для кожної мережі ці вразливості мають різний рівень критичності, використовувати єдиний підхід для оцінювання рівня захищеності не видається можливим. Однак, знаючи критичність тієї або іншої вразливості, за допомогою цього підходу (1)–(6) можна оцінити можливі ризики та мінімізувати їх за допомогою введення додаткових контрзаходів, що, у свою чергу, призведе до мінімізації збитку, який може бути заподіяний як користувачу, так і мережі. Так, наприклад, якщо в результаті розрахунків ризиків отримані оцінки нижчі за припустимі в рамках використовуваних політик безпеки конкретної мережі, то необхідно переглянути механізмів безпеки. Виходячи із цього, запропоновані рішення будуть корисні для прийняття рішень і надалі будуть інтегровані в єдину метрику для відображення комплексного рівня безпеки інфокомунікаційної мережі.

Список літератури:

1. Mohammad, Salim A., Al-Shaer, E., Taibah, M., Latifur K. Prediction capabilities of vulnerability discovery models. Reliability and maintain ability symposium. 2006. P. 86–91.
2. Abedin, M., Nessa, S., Al-Shaer, E., and Khan, L. Vulnerability analysis for evaluating quality of protection of security policies . 2nd ACM CCS workshop on quality of protection, Alexandria. 2006. P. 28–39.
3. Bock, F. Analgorithm to construct a minimum directed spanning tree in a directed network. Developments in Operations Research. GordonandBreach. 1991. P. 29–44.
4. NIST CloudComputingProgram. National Institute of Standards and Technology. URL: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
5. Hewitt CarlORGs for Scalable, Robust, Privacy-Friendly Client Cloud Computing. IEEE Internet Computing. 2008. Vol. 12, Issue: 5. P. 96–99.
6. AlertLogic. Cloud Security Report: Research on the Evolving State of Cloud Security. 2014. URL: https://www.alertlogic.com/resources/cloud-security-report.pdf.
7. Al-Shaer, E., andHamed, H. Discovery of policy anomalies in distributed firewalls. IEEE INFOCOM'04. 2004. P. 84–97.
8. Kamara, S., Fahmy, S., Schultz, E., Kerschbaum, F., Frantzen, M. Analysis of vulnerabilities in internet firewalls. NetworkSecurity. 2003. 22 (3). P. 214–232.
9. Ammann, P., Wijesekera, D., andKaushik, S. Scalable. Graph-based network vulnerability analysis. 9th ACM conference on computer and communication ssecurity. NewYork, USA. 2002. P. 217–224.
10. Feng, C., Jin-Shu, S.. A flexible approach to measuring network security using attack graphs. International symposium on electronic commerce and security. 2008. P. 278–304.
11. Chunlan Li, Zhonghua Deng. Value of Cloud Computing by the View of Information Resources. Network Computing and Information Security (NCIS). InternationalConferenceon. 2011. Vol. 1. P. 108–112.
12. Yevdokymenko M., MayanganiManasse, DmitriyZalushniy, Batoul Sleiman.. Analysis of Methods for Assessing the Reliability and Security of Infocommunication Network. 4th International Scientific-Practical Conference «Problems of Infocommunications. ScienceandTechnology» PIC S&T`2017. X., ХНУРЕ. 2017. P. 199–202.

МЕТОД ОЦЕНКИ ВЛИЯНИЯ АТАК НА ИНФОКОММУНИКАЦИОННУЮ СЕТЬ С УЧЕТОМ СУЩЕСТВУЮЩИХ УЯЗВИМОСТЕЙ

В статье исследуются методы оценки критичности уязвимостей и оценки распространения той или иной атаки в инфокоммуникационной сети.

Представлен проактивный подход к количественной оценке сетевой безопасности, который позволяет оценить риски на уровне пользователя и сети из-за присутствия уязвимостей. Предложенные решения будут полезны для принятия решений и дополнительно интегрированы в единую метрику для отображения интегрированного уровня безопасности инфокоммуникационной сети.

Ключевые слова: *защищенность, вес, сеть, инфокомуникации, безопасность, оценка уязвимости, информационная безопасность.*

ASSESSMENT METHOD OF THE ATTAKS INFLUENCE ON THE INFOCOMUNICATION NETWORK ACCORDING TO EXISTING VARIABILITY

The article explores methods for assessing vulnerabilities and the spread of an attack in an infocommunication network. A proactive approach to the quantitative assessment of network security, which allows us to assess risks at the user and network level through the of existing vulnerabilities is presented. The proposed solutions will be useful for decision making and will be further integrated into a single metric for displaying the integrated level of security of the infocommunication network.

Key words: *security, weight, network, infocommunications, security, vulnerability assessment, information security.*