NGHIÊN CỨU XÂY DỰNG PHƯƠNG PHÁP LƯỢNG GIÁ MỨC ĐỘ AN NINH MÁY TÍNH VÀ MẠNG MÁY TÍNH

I. ĐẶT VẤN ĐỀ

An ninh hệ thống thông tin là vấn đề đang được quan tâm rất lớn hiện nay. Đã có rất nhiều sự đầu tư cho việc xây dựng, tăng cường an ninh nhằm đảm bảo tính ổn định trong hoạt động của các hệ thống thông tin nhưng song song với quá trình đó là những vấn đề được đặt ra:

- Hệ thống hiện nay đã đảm bảo an ninh.
- Sự đầu tư ra sao là đủ.
- Cần làm gì để kiểm tra an ninh cho hệ thống.

Hoặc khi cần so sánh hai mạng máy tính với sự đầu tư, điều kiện hoạt động, lực lượng quản lý khác nhau thì chúng ta cũng cần có câu kết luận "Mạng máy tính nào đảm bảo an ninh hơn".

Còn có rất nhiều nội dung và vấn đề được đặt ra đối với một hệ thống thông tin khi cần đảm bảo cho chúng hoạt động tốt và khi đã trả lời được những vấn đề trên thì chúng ta cần làm gì để tăng cường hơn nữa an ninh cho hệ thống. Từ đó cũng thấy ngay một hướng nghiên cứu, cần phải xem xét lượng giá mức độ an ninh hệ thống sâu sắc hơn, để từ đó có thể trả lời một phần những thắc mắc, đưa ra các thước đo về an ninh cho hệ thống thông tin, từ đó tìm ra các biện pháp tăng cường an ninh cho hệ thống.

II. MỤC ĐÍCH CỦA LUẬN ÁN

Trong khuôn khổ của luận án, tác giả không có tham vọng sẽ giải quyết toàn bộ những câu hỏi và vấn đề trong lĩnh vực an ninh máy tính và mạng máy tính. Nội dung luận án sẽ tập trung vào nhiệm vụ tìm ra phương pháp lượng giá mức độ an ninh phù hợp cho máy tính, mạng máy tính, hệ thống thông tin để từ đó nhà quản lý, quản trị có được cái nhìn toàn cảnh và tổng thể về hệ thống hiện tại, đồng thời triển khai các biện pháp tăng cường an ninh khi cần thiết.

III. PHƯƠNG PHÁP NGHIÊN CỨU

Tổng hợp các nghiên cứu về lĩnh vực đánh giá, lượng giá mức độ an ninh

hệ thống cho thấy:

(1) Các phương pháp đánh giá dựa trên các mô hình, tiêu chuẩn an ninh hệ thống như ISO là rất phù hợp, tuy nhiên khâu lượng giá kết quả sau đánh giá cần tăng cường hơn nữa tính chính xác, hạn chế sai số chủ quan. Tác giả đã sử dụng công cụ tập mờ, lập luận xấp xỉ để khắc phục một số hạn chế của các phương pháp lượng giá hiện nay.

(2) Có một số hướng tiếp cận lượng giá mức độ an ninh thông qua các tham số định lượng như hiệu năng mạng, chất lượng dịch vụ,... Mỗi hướng tiếp cận đều có ưu và nhược điểm riêng. Tác giả đã phân tích và đề xuất phương pháp lượng giá mới dựa trên hướng tiếp cận rủi ro của hệ thống, qua đó lượng giá mức độ an ninh cho máy tính và mạng máy tính.

IV. NHỮNG ĐÓNG GÓP MỚI CỦA LUẬN ÁN

(1) Hệ thống hóa các phương pháp lượng giá mức độ an ninh mạng hiện có.

(2) Đưa ra một mô hình hoàn chỉnh bao gồm tham số đầu vào, tham số đầu ra, mô hình quan hệ, phương pháp tính toán cho phép lượng giá mức độ an ninh máy tính và mạng máy tính trên các hệ thống thực.

(3) Đề xuất phương pháp lượng giá mức độ an ninh mạng có ứng dụng tập mờ, lập luận xấp xỉ, đại số gia tử, hệ trợ giúp quyết định, từ đó đưa ra khả năng khắc phục một số nhược điểm đang tồn tại của các phương pháp hiện nay.

V. BỐ CỤC LUẬN ÁN

Luận án được chia làm 4 chương. Trong đó, chương 1 và chương 2 là những vấn đề tổng quan về hướng nghiên cứu của luận án, chương 3, chương 4 sẽ trình bày những nhận xét, đánh giá, đồng thời đề xuất giải pháp, mô hình, phương pháp, khắc phục một số hạn chế đang tồn tại.

VI. TÓM TẮT LUẬN ÁN

Chương 1. Tổng quan về lượng giá mức độ an ninh máy tính và mạng máy tính

1.1. Khái niệm lượng giá mức độ an ninh

Lượng giá mức độ an ninh là quá trình xác định giá trị an ninh của hệ thống sau đánh giá.

Trong đó: Đánh giá mức độ an ninh là biện pháp rà soát lại toàn bộ hoạt động của hệ thống nhằm tìm ra những nhược điểm có khả năng bị tấn công tại thời điểm hiện tại. Chúng ta tìm hiểu một số đặc điểm và tính chất trong nội dung định nghĩa:

- Lượng giá, đánh giá mức độ an ninh sẽ thực hiện xem xét toàn bộ những thành phần có liên quan đến hoạt động của hệ thống như chính sách, con người, phần mềm, phần cứng,...
- Kết quả thu được sau quá trình đánh giá là tìm ra những điểm yếu, lỗ hổng có khả năng bị tấn công, khả năng ảnh hưởng xấu tới an ninh hệ thống, hiểm họa, rủi ro,... tại thời điểm hiện tại.
- Từ kết quả thu được, chúng ta có thể tiến hành theo dõi, kiểm tra, phân tích nhằm tìm ra những biện pháp khắc phục, đối phó, giúp cho hệ thống hoạt động tốt hơn.
- Những biện pháp khắc phục áp dụng cho hệ thống không thể giúp hệ thống đảm bảo an ninh 100% mà chỉ giúp hệ thống giảm mức độ rủi ro xuống thấp hơn.

1.2. Phương pháp luận đánh giá mức độ an ninh

Đánh giá mức độ an ninh hiện nay thường qua ba giai đoạn là thu thập thông tin, phân tích, đưa giải pháp, trong đó quá trình phân tích bao gồm đánh giá, lượng giá và sử dụng chuyên gia. Áp dụng cả ba giai đoạn là rất cần thiết, nhưng trong từng hệ thống có thể chỉ áp dụng những giai đoạn cần thiết.

1.3. Phương pháp tiếp cận hệ thống

Để hệ thống bộc lộ hết những ưu và nhược điểm trong quá trình hoạt động, người đánh giá phải tạo ra những kịch bản cụ thể và đóng vai trò như đối phương muốn triệt phá hệ thống. Có thể sử dụng ba cách thức tiếp cận tới hệ thống để đánh giá: Tiếp cận bên ngoài, tiếp cận phối hợp và tiếp cận bên trong.

1.4. Kỹ thuật kiểm tra hệ thống

Bao gồm kỹ thuật giả định, kỹ thuật thâm nhập, kỹ thuật cây tấn công. Hiện nay phổ biến nhất là kỹ thuật xâm nhập và kỹ thuật cây tấn công.

1.5. Một số phương pháp đánh giá mức độ an ninh hiện nay

Các tổ chức an ninh mạng trên thế giới đã hiện thực hóa quá trình đánh giá an ninh bằng các phương pháp cụ thể, phổ biến là phương pháp của NIST, phương pháp của NSA và phương pháp OSSTMM.

1.6. Hướng tiếp cận trong xây dựng hệ thống an ninh thông tin

Có thể tiếp cận theo hướng từ trên xuống từ chính sách đến quy tắc và cuối cùng là quy trình, cũng có thể tiếp cận theo hướng ngược lại. Một số mô hình quản lý thông tin phổ biến hiện này như mô hình quản lý an ninh của NIST, mô

hình MEHARI, mô hình ISO 17799, mô hình ISO/IEC 27001, mô hình ISO 15408.

1.7. Mô hình lượng giá các yếu tố định lượng

Kết quả nghiên cứu của Jonas Hallberg, J. Hunstand, A. Bond, A. Peterson, M. Humtad, A, Pahlsson (12/2004) và Jonas Hallberg, Amund Hunstad, Mikael Peterson (2005) đã đưa ra framework có khả năng hỗ trợ lượng giá an ninh. Dựa vào framework này, Peterson (2004) đã đưa ra một phương pháp lượng giá mức độ an ninh dựa trên lưu lượng hoạt động trong hệ thống mạng máy tính, phương pháp này được gọi tên là CAESAR. Phương pháp CAESAR đã đặt trọng tâm vào lưu lượng của hệ thống để định lượng an ninh cho hệ thống. Với quan điểm đó, phương pháp CAESAR về thực chất chỉ xác định được bất thường do các tấn công dựa vào sự đột biến lưu lượng chuyển tiếp giữa các thành phần hệ thống. Trong thực tế có rất nhiều biện pháp và phương pháp tấn công gây mất an ninh mà hoàn toàn không phụ thuộc vào vấn đề lưu lượng.

1.8. Những đối tượng xem xét khi lượng giá an ninh

Tổng hợp những vấn đề cần xem xét khi lượng giá an ninh, luận án đưa ra sáu nội dung chính khi tiến hành đánh giá bao gồm kiến trúc mạng, thiết bị mạng, máy chủ và máy trạm, ứng dụng, kỹ thuật kiểm tra, chính sách và phương pháp. Trong mỗi một nội dung có thể bao gồm các bước thực hiện nhỏ hơn.

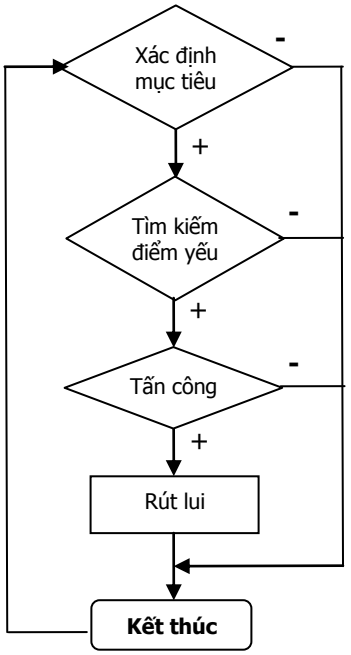
Kết luận

1. Các phương pháp lượng giá các yếu tố định lượng hiện nay chỉ đưa ra danh sách các điểm yếu của hệ thống cần khắc phục, chưa xác định được kết quả lượng giá chính xác có khả năng so sánh khả năng phòng thủ khi hệ thống đi vào hoạt động.
2. Nghiên cứu và xây dựng mô hình lượng giá an ninh hệ thống do Jonas Hallberg và các cộng sự đề xuất chỉ có thể lượng giá an ninh cho mạng máy tính mà không lượng giá được cho máy tính đơn lẻ.
3. Chưa thực sự có một mô hình hoàn thiện ứng dụng trong công tác lượng giá các yếu tố định lượng, cần phải tổng quát hóa mô hình đánh giá, đưa ra mô hình mới về mối quan hệ giữa các yếu tố ảnh hưởng tới an ninh máy tính và mạng máy tính.
4. Cách thức đưa ra quyết định khi đánh giá các yếu tố định tính hiện nay đang tồn tại nhiều yếu tố làm cho kết quả có độ chính xác không cao. Để tăng tính chính xác cần phải lựa chọn mô hình lượng giá phù hợp, giải pháp kỹ thuật thích nghi cũng như danh sách các đối tượng phù hợp để tiến hành đánh giá mức độ an ninh máy tính và mạng máy tính.
5. Các công cụ lượng giá không có khả năng kiểm soát toàn bộ an ninh của hệ thống, việc sử dụng các chuyên gia về an ninh mạng là rất cần thiết nhằm kiểm định lại toàn bộ vấn đề đã được xem xét bởi các biện pháp truyền thống.

Chương 2. An ninh hệ thống máy tính và mạng máy tính

2.1 Quy trình tấn công

Tổng quát hóa quy trình tấn công một hệ thống bao gồm các khâu: Xác định mục tiêu, tìm kiếm điểm yếu, tấn công, rút lui, kết thúc. Bước đầu tiên là xác định được mục tiêu, tiếp theo sẽ tìm kiếm điểm yếu của mục tiêu. Khi tìm kiếm điểm yếu thất bại có thể phải xác định mục tiêu khác hoặc kết thúc quá trình tấn công. Sau khi tấn công thành công kẻ tấn công sẽ thực hiện xóa đi dấu vết, thiết lập môi trường thuận lợi để quay trở lại, đây chính là các công việc thực thi để rút lui và kết thúc toàn bộ quy trình.



Hình 2.1. Quy trình tấn công.

2.2 Tấn công hệ thống

Có thể phân ra làm bốn lại tấn công bao gồm tấn công phối hợp, tấn công trực diện, tấn công vu hồi, tấn công phi cấu trúc. Trong từng loại tấn công đều có đặc điểm riêng như kịch bản, kế hoạch, mức độ khó, sức phá hoại, từ đó có được thông số về tỉ lệ rủi ro bị tấn công bằng phương pháp tương ứng.

2.3 Triển khai rút lui

Khi quá trình tấn công kết thúc đòi hỏi phải triển khai các kỹ thuật che dấu thông tin, xóa dấu vết, thiết lập môi trường,… với mục đích bảo đảm an toàn, tránh bị truy kích hoặc phục vụ cho những lần tấn công sau.

2.4 Phương pháp phòng thủ

Phương pháp phòng thủ thụ động và phòng thủ tích cực hiện nay được triển khai để chống lại các cuộc tấn công. Các phương pháp phòng thủ cho phép phát hiện, ngăn chặn, triệt phá các hình thức tấn công. Tuy nhiên phòng thủ thụ động chỉ là được điều này khi đã biết trước kịch bản, phương thức, phương pháp tấn công còn phòng thủ tích cực thì ngược lại.

Kết luận

1. Nguyên nhân chính làm máy tính và mạng máy tính mất an ninh là do sự bất cẩn của người sử dụng và người quản trị hệ thống chưa nắm vững kiến thức an ninh hệ thống.
2. Vấn đề cốt lõi trong yếu tố mất an ninh của máy tính và mạng máy tính là do tồn tại các rủi ro, lỗ hổng chưa kịp khắc phục. Kẻ tấn công sẽ xâm hại hệ thống ngay khi phát hiện ra những điểm yếu này.
3. Phải sử dụng các biện pháp chính sách an ninh, bức tường lửa, phát hiện và phòng chống xâm nhập, hệ thống giả lập mới có thể làm giảm đi những rủi ro. Tuy nhiên các phương pháp đó không ngăn chặn được toàn bộ các nguy hiểm do yếu tố tiếp cận tới hệ thống của kẻ tấn công có thể đi theo nhiều phương thức khác nhau.

Chương 3. Mô hình lượng giá an ninh của hệ thống thông qua tham số định lượng

3.1 Một số hướng tiếp cận lượng giá

Để lượng giá an ninh máy tính và mạng máy tính thông qua tham số định lượng, hiện nay phổ biến có ba hướng tiếp cận bao gồm: Hiệu năng mạng, chất lượng dịch vụ, quản lý rủi ro.

3.2 Định hướng nghiên cứu

Xem xét các yếu tố cấu thành an ninh mạng máy tính, xây dựng bộ đo an ninh mạng, đưa ra mô hình quan hệ giữa bộ đo và các yếu tố, nghiên cứu sự biến đổi topology của mạng khi bộ đo tiếp cận hệ thống, thông qua quá trình tổng hợp các kỹ thuật tấn công mạng, rà soát lỗ hổng, rủi ro của hệ thống mà tìm ra các yếu tố, thông số mô tả an ninh trên từng phân đoạn mạng, quá trình kết nhập các thống số này sẽ cho biết giá trị an ninh và độ rủi ro cho hệ thống mạng.

3.3 Mô hình hóa quy trình tấn công

Tổng quát toàn bộ quy trình tấn công qua lưu đồ thuật toán làm căn cứ cho việc xác định các rủi ro của hệ thống.

3.4 Xác định mục tiêu và tìm kiếm điểm yếu

Để tăng cường an ninh cho hệ thống, một trong những biện pháp hữu hiệu là triển khai các kỹ thuật che dấu thông tin. Để làm được điều này, phải nghiên cứu cách thức xác định mục tiêu và tìm kiếm điểm yếu của tấn công, từ đó làm căn cứ xây dựng giải pháp phòng thủ.

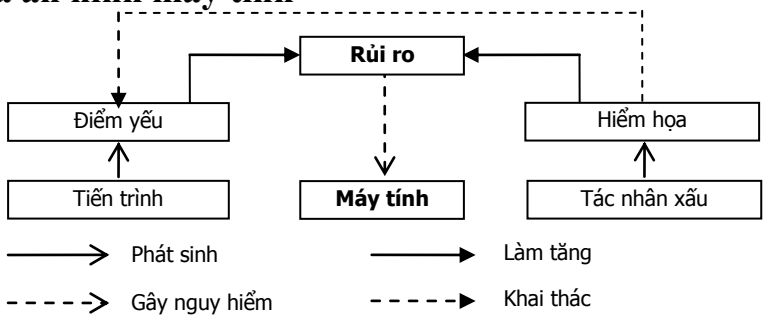
3.5 Cơ sở dữ liệu rủi ro

Hiện nay phần lớn các kỹ thuật tấn công đều được công bố, và được đánh giá bằng các tham số bao gồm tính phổ biến, tính đơn giản, tính phá hoại, tỉ lệ rủi ro bị tấn công. Các giá trị đánh giá này được tập hợp tạo ra cơ sở dữ liệu rủi ro và được sử dụng hỗ trợ cho việc tìm kiếm điểm yếu.

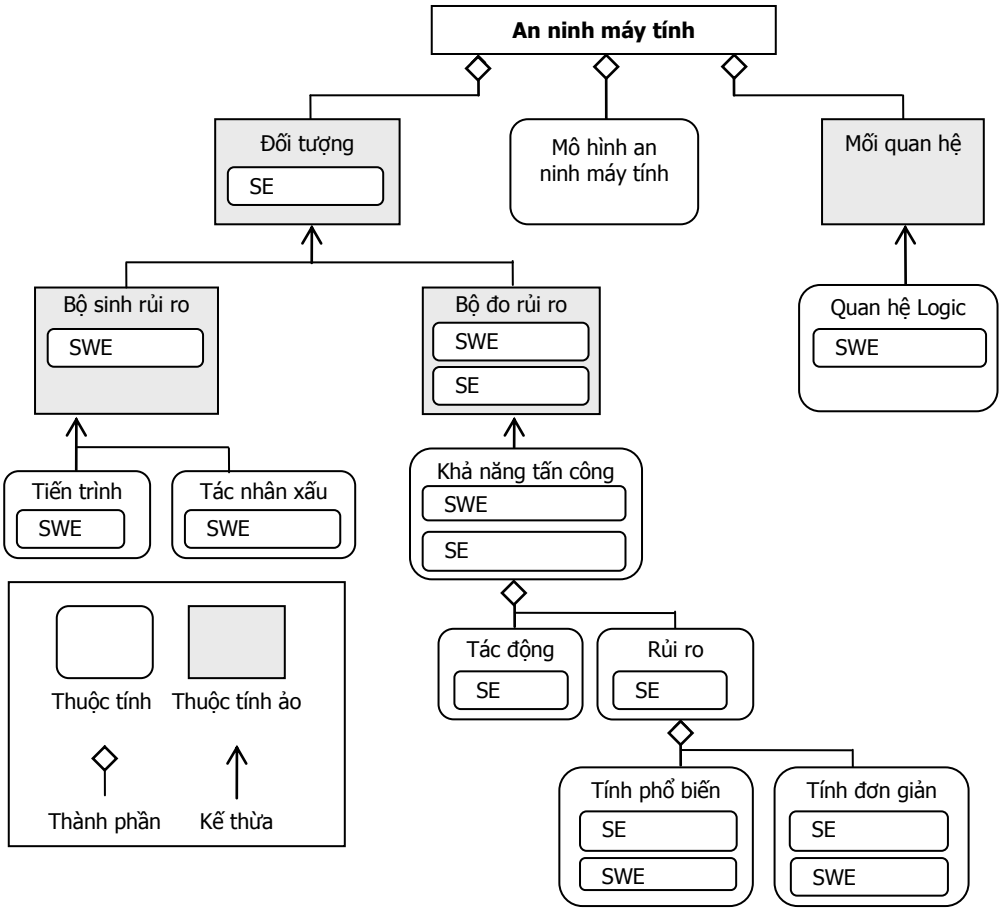
3.6 Nhận xét và hướng phát triển

Luận án thực hiện nghiên cứu theo hướng xem xét các yếu tố cấu thành an ninh mạng máy tính, xây dựng bộ đo an ninh mạng, đưa ra mô hình quan hệ giữa bộ đo và các yếu tố, nghiên cứu sự biến đổi topology của mạng khi bộ đo tiếp cận hệ thống, thông qua quá trình tổng hợp các kỹ thuật tấn công mạng, rà soát lỗ hổng, rủi ro của hệ thống mà tìm ra các yếu tố, thông số mô tả an ninh trên từng phân đoạn mạng, quá trình kết nhập các thống số này sẽ cho biết giá trị an ninh và độ rủi ro cho hệ thống mạng.

3.7 Lượng giá an ninh máy tính



Hình 3.5. Mối quan hệ giữa các yếu tố ảnh hưởng tới an ninh máy tính.



Hình 3.6. Mô hình quan hệ các thành phần lượng giá an ninh máy tính.

- **Tham số đầu vào**

Tác động: Định lượng những thiệt hại gây ra cho hệ thống, được sử dụng để đo mức độ ảnh hưởng của một cuộc tấn công có khả năng thành công.

Rủi ro: Định lượng khả năng hệ thống có thể bị xâm phạm bằng một phương pháp cụ thể tới các rủi ro đang tồn tại trên hệ thống.

Tính phổ biến: Định lượng khả năng có thể áp dụng phương pháp phá hoại cụ thể trong khai thác rủi ro của hệ thống.

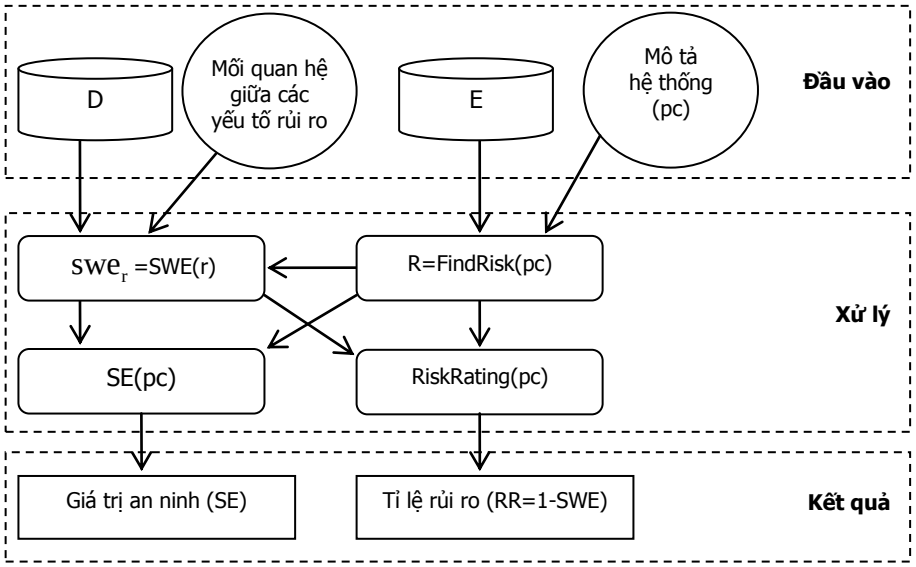
Tính đơn giản: Định lượng độ dễ dàng khi áp dụng phương pháp phá hoại cụ thể trong khai thác rủi ro của hệ thống.

- **Xử lý rủi ro**

Bộ sinh rủi ro: Tổng hợp rủi ro được cấu thành từ các tiến trình và các tác nhân xấu tồn tại trong quá trình hoạt động của hệ thống.

Bộ đo rủi ro: Sau quá trình tổng hợp của bộ sinh rủi ro sẽ thực hiện lượng giá trên từng rủi ro bằng các tham số đầu vào. Các tham số sẽ được kết nhập và tổng hợp nhằm tìm ra giá trị an ninh (SE) cho máy tính.

Để lượng giá và đo các thuộc tính trong mô hình trên luận án sử dụng hai tham số là SE ($0 \le SE \le 1$, Security Estimate - Giá trị an ninh) và SWE ($0 \le SWE \le 1$, Security Weight Estimate - Giá trị trọng số an ninh).



Hình 3.7. Mô hình triển khai lượng giá an ninh máy tính.

Căn cứ vào mối quan hệ giữa các yếu tố ảnh hưởng tới an ninh máy tính và mô hình quan hệ giữa các thành phần lượng giá an ninh máy tính, luận án đưa ra mô hình triển khai lượng giá an ninh máy tính như sau

Tìm kiếm rủi ro

- FindRisk(pc): Hàm tìm kiếm những rủi ro trên mục tiêu pc cần lượng giá.
- E: Cơ sở dữ liệu rủi ro.
- R: Cơ sở dữ liệu những rủi ro được phát hiện trên mục tiêu lượng giá ($R \subset E$), đây chính là tập kết quả trả về cho hàm FindRisk(pc).
    - e: rủi ro được lấy ra từ E ($e \in E$)
    - check(e): Kiểm tra điều kiện cần trên mục tiêu có thể được khai thác qua điểm yếu e.
    - attack(e): Tấn công mô phỏng bằng kỹ thuật thâm nhập tới mục tiêu qua điểm yếu e.

Giải thuật

```
function FindRisk(pc)
      R = ∅
           for each e in E  do
                  if check(e) then
                        if attack(e) then
                              R = R ∪ e
                        endif
                 endif
           endfor
      return R
end function
```

Tỉ lệ rủi ro

- SWE(r): hàm tính tỉ lệ rủi ro bị đối phương tấn công khi điểm yếu r tồn tại trên mục tiêu cần lượng giá.
- D: Cơ sở dữ liệu tri thức chuyên gia cho các thông số tính phá hoại, tính phổ biến, tính đơn giản.

- r: Rủi ro được lấy ra từ R ($r \in R$)
- LookupI(r,D), LookupP(r,D), LookupS(r,D): hàm lấy ra thông số tính phá hoại, tính phổ biến, tính đơn giản của rủi ro r trong cơ sở dữ liệu D, với mỗi giá trị chúng ta có thể thiết lập thêm trọng số cho từng yếu tố tương ứng swe_p, swe_s.

Giải thuật

```
function SWE(r)
      p=LookupP(r,D)
      s=LookupS(r,D)
      return  p*swe_p + s*swe_s          (5.1)
end function
```

Lượng giá an ninh và rủi ro

- SE(pc): Hàm lượng giá giá trị an ninh cho mục tiêu pc.
- RiskRating(pc): hàm tính tỉ lệ rủi ro bị đối phương tấn công mục tiêu cần lượng giá.

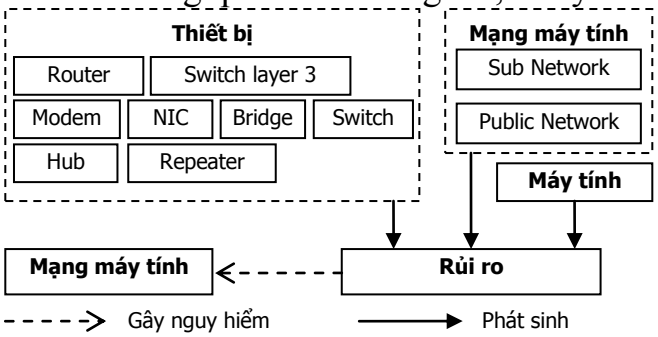
Giải thuật

```
function SE(pc)
      R = FindRisk(pc)
      for each r in R do
            swe_i =SWE(r)
            se_i =LookupI(r)
      endfor
return ( 1 - Σ(se_i * swe_i) / Σ swe_i )      (5.2)
end function
```

```
function RiskRating(pc)
      R = FindRisk(pc)
      for each r in R do
            swe_i =SWE(r)
            se_i =LookupI(r)
      endfor
return Σ(se_i * swe_i) / Σ se_i               (5.3)
end function
```

3.8 Lượng giá an ninh mạng máy tính

Mọi hiểm họa, rủi ro, lỗ hổng, điểm yếu xuất phát từ những thành phần liên quan đến các hoạt động của hệ thống mạng, vì vậy chúng được xem xét như các yếu tố làm tăng tính rủi ro trong quá trình tương tác, xử lý của mạng máy tính.

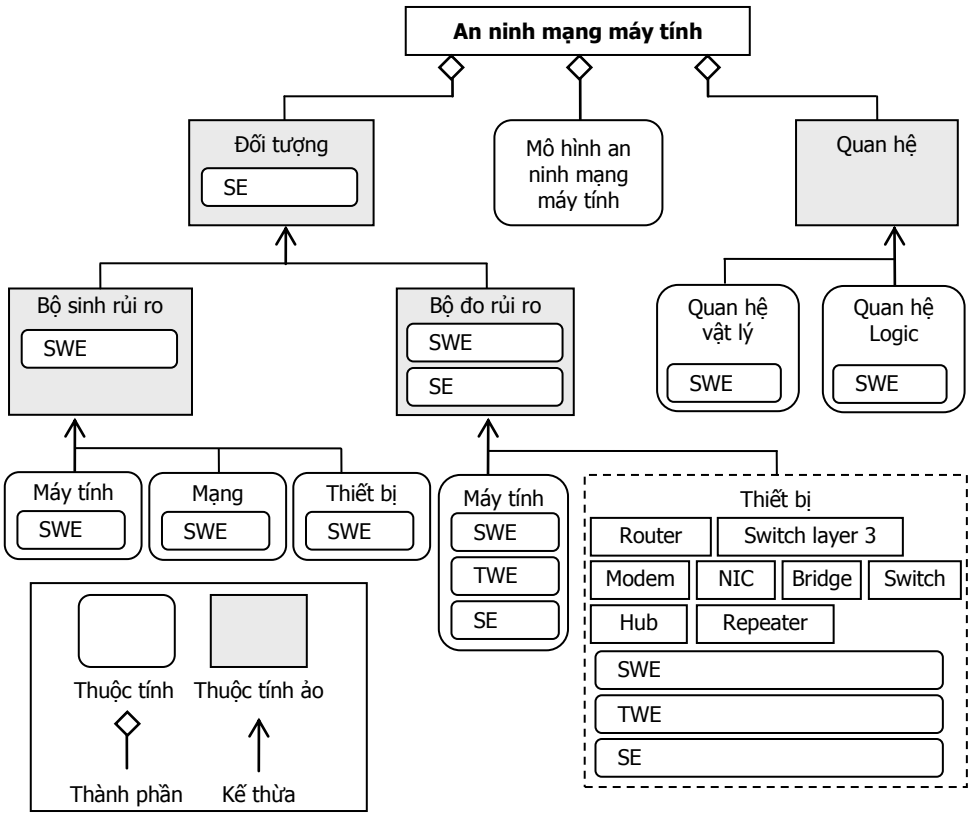


Hình 3.8. Mối quan hệ giữa các yếu tố ảnh hưởng tới an ninh mạng.

Bộ đo (Risk Mediator) sẽ tiếp nhận các giá trị an ninh (SE, $0 \le SE \le 1$) và trọng số an ninh thể hiện mối quan hệ logic (SWE, $0 \le SWE \le 1$), từ các thành phần cấu thành mạng như máy tính, thiết bị mạng. Những giá trị SE, SWE cung

cấp cho bộ đo được xác định qua việc lượng giá mức độ an ninh từng thiết bị, máy tính. Ngoài ra, vị trí tương đối của các thành phần trên topology của mạng thể hiện yếu tố thiết kế cũng ảnh hưởng tới an ninh của toàn mạng, vì vậy để xem xét quan hệ vật lý giữa các thành phần này luận án sử dụng trọng số topo (TWE, $0 \le \text{TWE} \le 1$).

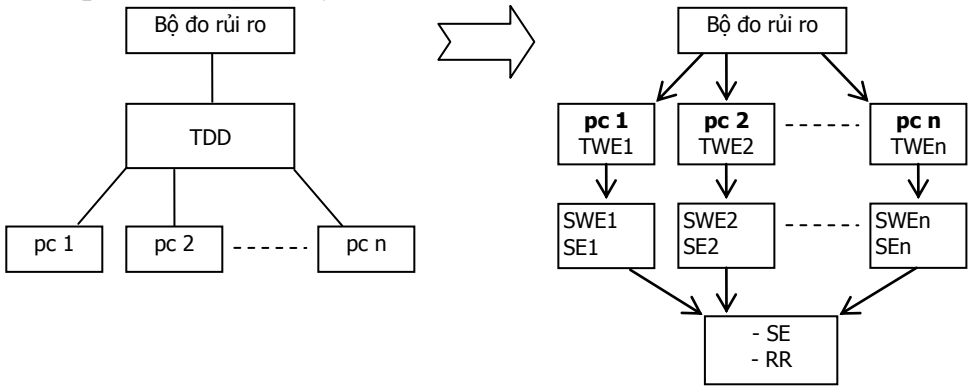
Do tính chất của đối tượng lượng giá, đồng thời cách tiếp cận tới hệ thống mạng có nhiều điểm khác biệt so với tiếp cận trực tiếp máy tính, thiết bị trong hệ thống mạng nên giá trị SE, SWE cũng sẽ biến đổi hoàn toàn phụ thuộc vào vị trí tương đối của bộ đo với topology của mạng. Điều này là hoàn toàn phù hợp với thực tế, khi hệ thống xuất hiện người tấn công thì khả năng phòng thủ và đổ vỡ của hệ thống phụ thuộc rất lớn vào vị trí tấn công, vì vậy theo mô hình này, chúng ta sẽ có các giá trị an ninh khác nhau tùy thuộc vào vị trí đặt bộ đo.



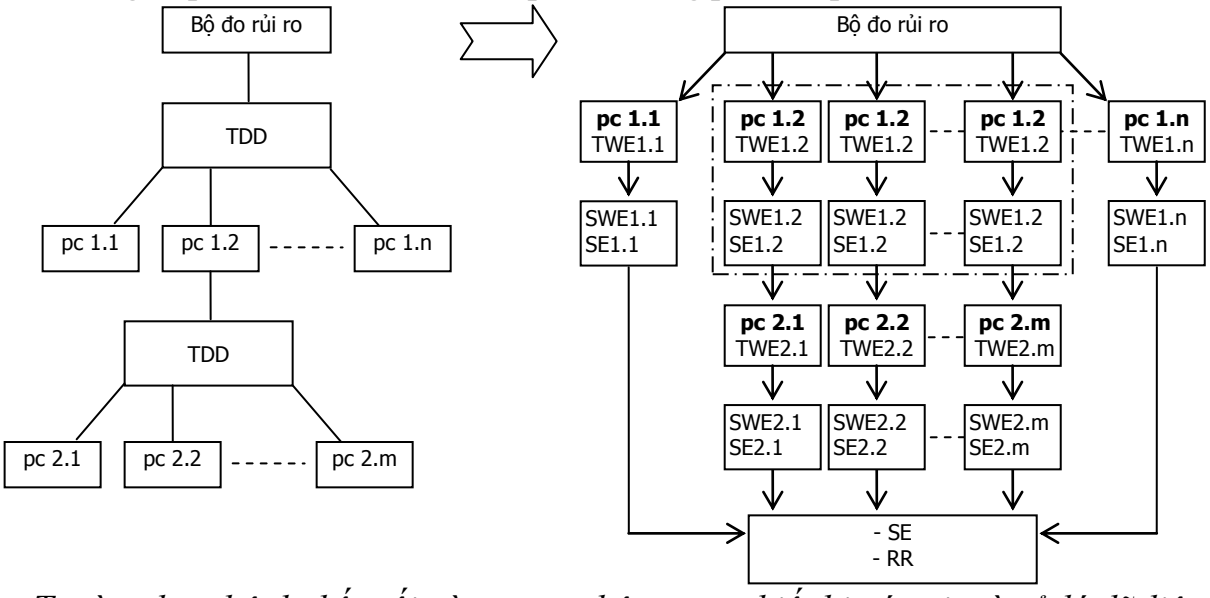
Hình 3.9. Mô hình quan hệ các thành phần lượng giá an ninh mạng.

Thực hiện xem xét topology của hệ thống mạng với gốc là bộ đo, trong phần này luận án quy ước mục tiêu cần lượng giá là pc, tổng hợp các giá trị lượng giá SE, SWE, TWE của các thành phần cấu thành mạng sẽ được giá trị an ninh (SE), tỉ lệ rủi ro (RR) của mạng máy tính đang xem xét.

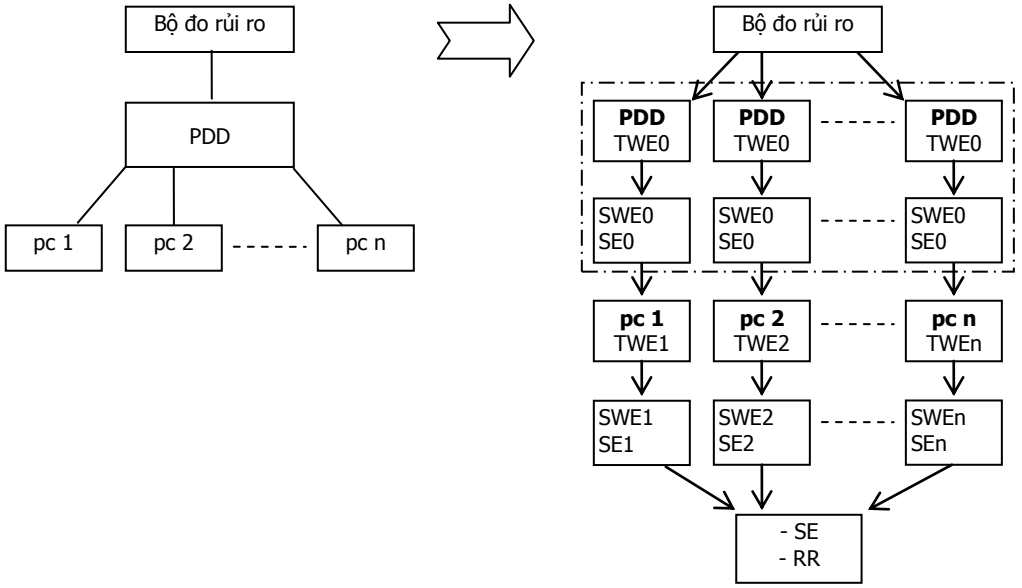
- *Trường hợp bộ đo kết nối trực tiếp vào mạng thông qua thiết bị chỉ có vai trò chuyển tiếp dữ liệu (Transfer data device)*



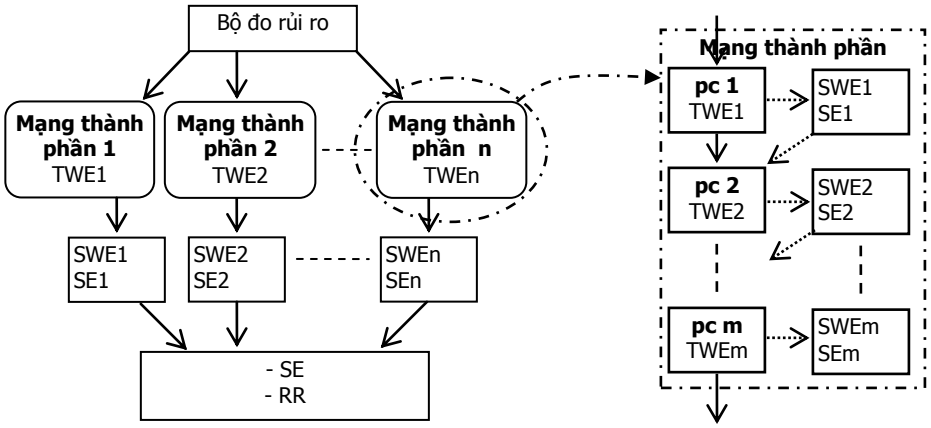
- *Trường hợp bộ đo kết nối trực tiếp vào mạng phân cấp*



- *Trường hợp bộ đo kết nối vào mạng thông qua thiết bị có vai trò xử lý dữ liệu như filter, firewall,... (Process data device - PDD)*



Nhìn vào sự biến đổi topology khi đưa bộ đo vào hệ thống cho thấy có thể xác định mô hình tổng quát khi thực hiện lượng giá bằng cách thay thế các chuỗi kết nối giữa các nút mạng bằng một mạng dạng đồng trục (bus), ta gọi cấu trúc mạng này là "mạng thành phần", như vậy mỗi mạng thành phần được hình thành dạng nối tiếp, các mạng thành phần khác nhau có thể chứa một số lượng pc khác nhau, đồng thời một pc cũng có thể tồn tại trên nhiều mạng thành phần khác nhau.



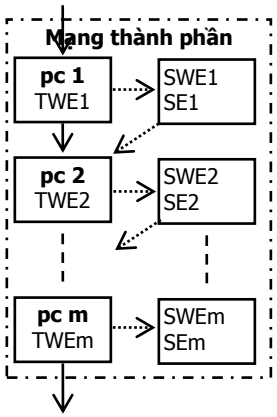
Hình 3.10. Cấu trúc mạng thành phần khi lượng giá an ninh mạng.

Từ đó, để lượng giá được giá trị an ninh (SE), tỉ lệ rủi ro (RR) của hệ thống mạng chúng ta cần có giải pháp cho hai bài toán chính bao gồm:

Bài toán 1: Tính TWEi, SWEi, SEi cho mạng thành phần i với $1 \le i \le n$.

Bài toán 2: Kết nhập các giá trị TWEi, SWEi, SEi ($1 \le i \le n$) tìm ra giá trị an ninh mạng (Network Security Estimate-NSE) và tỉ lệ rủi ro của mạng (Network Risk Rating - NRR).

Lượng giá mạng thành phần



$$TWE = Max(TWEi) \text{ với } 1 \le i \le m \qquad (3.4)$$

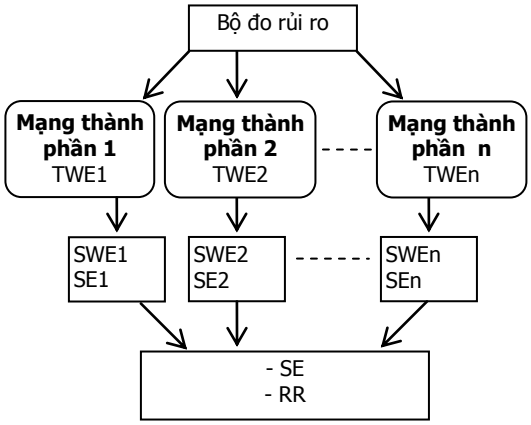
$$SWE = \frac{\sum_{i=1}^{m} TWEi * SWEi}{\sum_{i=1}^{m} TWEi} \qquad (3.5)$$

$$SE = \begin{cases} 2SE_1 - \sum_{i=1}^{m} i*SEi & \text{if } \sum_{i=1}^{m} i*SEi <= 2SE_1 \\ 0 & \text{if } \sum_{i=1}^{m} i*SEi > 2SE_1 \end{cases} \qquad (3.6)$$

- Trọng số topo (TWE) của sub network thể hiện mức độ quan trọng của chính sub network đó với những sub network khác trong topology của hệ thống mạng, vì vậy chúng được xác định bằng trọng số topo lớn nhất của pc tồn tại trên sub network.
- Trọng số an ninh (SWE) giúp xác định tỉ lệ rủi ro của hệ thống mạng sẽ được xác định thông qua trọng số topo và giá trị trọng số an ninh của các pc trên sub network.
- Giá trị an ninh (SE) của sub network sẽ được tính toán dựa trên khả năng an ninh của toàn bộ các pc trên sub network. Chính vì vậy, nếu từ vị trí bộ đo có thể tấn công tới pc m thì an ninh của hệ thống sẽ bị ảnh hưởng nghiêm trọng. Do vậy an ninh mạng sẽ suy giảm nhanh khi truy vấn tới các máy ở mức sâu. Trong trường sub network có m = 1 thì giá trị an ninh chính là SE1.

Lượng giá mạng máy tính

Thực tế, an ninh của hệ thống bị ảnh hưởng bởi những hệ thống có tính rủi ro cao nhất và giá trị an ninh thấp nhất. Do vậy, giá trị rủi ro (NRR - Network Risk Rating) bằng giá trị rủi ro cao nhất tại các sub network và giá trị an ninh (NSE - Network Security Estimate) bằng giá trị bằng giá trị an ninh thấp nhất của các nhánh mạng.



$$NRR = Max(SWEi),\ 1 \le i \le m \qquad (3.7)$$

$$NSE = SEi \text{ với } SEi*TWEi = Min(SEj*TWEj),\ 1 \le i \le m,\ 1 \le j \le m \qquad (3.8)$$

3.9 Triển khai phương pháp lượng giá

Cần tách biệt giữa tiếp cận an ninh máy tính và an ninh mạng máy tính. Tiếp cận lượng giá an ninh mạng máy tính chúng ta có thể sử dụng cách tiếp cận kiểu bên trong, tiếp cận kết hợp và tiếp cận bên ngoài. Bộ đo rủi ro sẽ hoạt động dựa trên hai kỹ thuật là kỹ thuật thâm nhập và kỹ thuật cây tấn công với cơ sở

dữ liệu rủi ro bao gồm các lỗ hổng, rủi ro được lấy từ cơ sở dữ liệu chuẩn, được công bố tại SANS, BugTraq,....

Kết luận

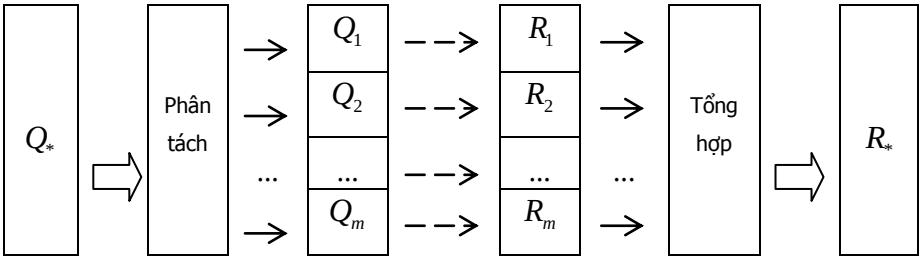
1. Các phương pháp lượng giá mức độ an ninh hiện nay đang đi theo hướng xác định các rủi ro vẫn chưa tìm được bộ tham số đầu vào có ý nghĩa giúp lượng giá chính xác an ninh hệ thống.
2. Giá trị an ninh máy tính được xây dựng từ bộ tham số bao gồm tính phổ biến, tính đơn giản, tính phá hoại, tỉ lệ rủi ro bị tấn công giúp cho kết quả lượng giá chỉ rõ được cụ thể điểm yếu của hệ thống, từ đó tìm ra phương thức khắc phục nhanh nhất. Việc xây dựng cơ sở dữ liệu rủi ro hoàn chỉnh sẽ càng làm tăng tính chính xác của kết quả lượng giá an ninh máy tính.
3. Lượng giá an ninh theo hướng tìm kiếm rủi ro đòi hỏi phải lượng giá an ninh cho từng nút trên mạng trước khi lượng giá an ninh cho toàn bộ hệ thống mạng. Như vậy, phương pháp lượng giá theo tham số định lượng cho máy tính và mạng máy tính phải sử dụng và kế thừa kết quả của giai đoạn lượng giá an ninh máy tính đơn lẻ cho lượng giá an ninh toàn bộ mạng tổng thể.
4. Để hoàn thiện phương pháp trong giai đoạn lượng giá an ninh mạng máy tính, cần bổ sung thêm giá trị trọng số topo của từng máy tính, mạng thành phần thể hiện mức độ ảnh hưởng của máy tính tới hệ thống mạng.
5. Vị trí thiết lập bộ đo có ảnh hưởng nhiều tới kết quả lượng giá toàn cục, mỗi vị trí bộ đo khác nhau có thể cho các kết quả lượng giá an ninh mạng khác nhau. Cách thức tiếp cận hệ thống mạng cũng phải lựa chọn cho phù hợp với thực tiễn khi tiếp cận hệ thống.

Chương 4. Phương pháp lượng giá các yếu tố định tính an ninh hệ thống

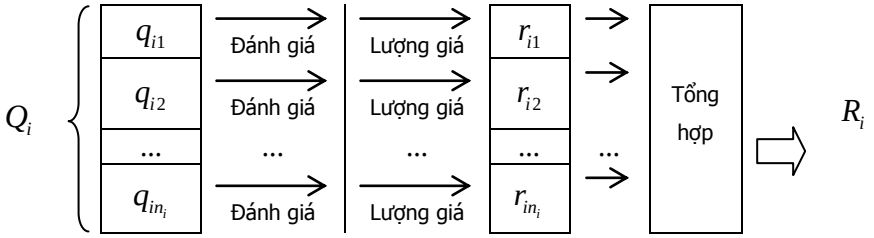
4.1. Mô hình lượng giá các yếu tố định tính

Xem xét chính sách an ninh, vấn đề con người, tài sản,...của hệ thống là bước đầu tiên trong quá trình lượng giá mức độ an ninh hệ thống mạng máy tính. Đây là giai đoạn có tính chất định tính. Để lượng giá các yếu tố này, thông thường

các đơn vị và tổ chức thường áp dụng các tiêu chuẩn an ninh thông tin. Công tác đánh giá hệ thống theo các tiêu chuẩn thường dưới hình thức trắc nghiệm hoặc kiểm tra, chất vấn nhằm mục đích thu thập thông tin về hệ thống, phân tích-đánh giá, lượng giá kết quả, tổng hợp báo cáo.



Hình 4.1. Quá trình lượng giá.



Hình 4.2. Quá trình đưa ra kết quả lượng giá trong từng nội dung.

Trong đó:

- Q_*: Tiêu chuẩn đánh giá (được phân tách thành các nội dung $Q_i (1 \le i \le m)$)
- Q_i: Nội dung thứ i cần lượng giá $(1 \le i \le m)$
- R_i: Kết quả lượng giá Q_i (R_i được tổng hợp từ r_{ij})
- R_*: Kết quả lượng giá hệ thống (tổng hợp từ R_i) theo tiêu chuẩn Q_*
- q_{ij}: Tiêu chuẩn j trong nội dung i $(1 \le i \le m;\ 1 \le j \le n_j)$
- r_{ij}: Kết quả lượng giá q_{ij}

4.2. Giải pháp lượng giá

Do các khâu thực hiện đánh giá định tính thường tồn tại sai số rất lớn và kết quả của chúng phụ thuộc vào nhiều yếu tố khác nhau. Vì vậy, để nâng cao hiệu quả của các phương pháp lượng giá mức độ an ninh trên các yếu tố định tính đòi hỏi phải giảm sai số chủ quan, định hướng đánh giá chặt chẽ và cụ thể từ đó trợ giúp cho công tác đánh giá và quyết định về mức độ an ninh của hệ thống. Kế thừa và tham khảo công trình nghiên cứu [54] của Ranjit Biswas và [60] của Shyi Ming Chen, Chia Hoang Lee, luận án đưa ra 7 hướng giải quyết như sau:

i. Mỗi nội dung và tiêu chuẩn đều có đặc điểm riêng thể hiện mức độ quan trọng và ảnh hưởng của chúng tới toàn bộ quá trình lượng giá, vì vậy quá trình phân tách nội dung sẽ được đánh trọng số nhằm xác định rõ mức quan trọng trong từng tiêu chuẩn và nội dung.

ii. Để tránh hiện tượng đánh giá phải đưa ra kết quả lượng giá trên một biên độ lớn của tiêu chuẩn làm cho quá trình lượng giá có sai số lớn, thực hiện lượng giá sẽ được làm mịn bằng phương pháp chia khoảng đánh giá thành nhiều mức độ đáp ứng khác nhau của hệ thống. Đồng thời, áp dụng phương pháp lượng giá cho các mức độ chia với hàm phù hợp.

iii. Khi tiến hành lượng giá, nếu những quyết định lượng giá chưa đủ độ chính xác thì người đánh giá có thể đưa ra sai số trong từng quyết định. Giá trị sai số này sẽ được phương pháp điều chỉnh vào giá trị lượng giá thật của hệ thống để đưa ra quyết định cuối cùng.

iv. Phân mức an ninh có thể đánh giá thành nhiều mức độ khác nhau để lượng giá cho từng tiêu chuẩn và nội dung. Các mức an ninh này sẽ hoàn toàn động và phụ thuộc vào từng hệ thống cần đánh giá đến mức độ nào. Việc quyết định số lượng các mức an ninh có thể được thực hiện tại giai đoạn chuẩn bị đánh giá.

v. Xây dựng bộ tham số và kết quả của các hệ thống chuẩn đã đánh giá và phân mức, sử dụng làm cơ sở quyết định cho các đánh giá sau này.

vi. Sau khi đánh giá xong hệ thống, có thể đối sánh kết quả thu được với tập tham số chuẩn nhằm tìm ra mức độ an ninh của hệ thống.

vii. Khi tiến hành tổng hợp kết quả từ nhiều nguồn đánh giá, ta có thể đưa ra sự chênh lệch giữa các kết quả lượng giá nhằm tìm sự đột biến trong quyết định giữa các thành viên trong nhóm thực hiện lượng giá, từ đó có những điều chỉnh thích hợp hơn.

4.3. Một số vấn đề trên tập mờ

Tác giả quy ước biểu diễn tập mờ với các thông số ý nghĩa như sau:

- Tập mờ tương đương: $\left(x, \mu_A(x)\right) \Leftrightarrow \left(\mu_A(x)/x\right)$

- Sai số: $\langle \mu, \delta \rangle$: giá trị μ có sai số là $\pm\delta$
- Biểu diễn vector tập mờ: $U = \big((\alpha_0 / x_0),(\alpha_1 / x_1),...,(\alpha_n / x_n)\big)$;

  $V = \big((\beta_0 / x_0),(\beta_1 / x_1),...,(\beta_n / x_n)\big)$
- Độ đo: $S_1(U,V) = \dfrac{U * V}{Max(U*U, V*V)}$ (4.3) ; $S_2(U,V) = \dfrac{\sum_{i=0}^{n} x_i |\alpha_i - \beta_i|}{\sum_{j=0}^{n} x_j}$ (4.4)

4.4. Trợ giúp quyết định

Các thao tác chính trong xử lý tri thức để ra quyết định là suy diễn, tổng hợp và biến đổi tri thức. Do vậy, luận án đã xem xét cách thức biểu diễn tri thức khi ứng dụng tập mờ với phương pháp lập luận xấp xỉ.

4.5. Nâng cao độ chính xác trong lượng giá mức độ an ninh mạng bằng phương pháp ứng dụng tập mờ khi ra quyết định

Tại mỗi tiêu chuẩn của hệ thống đòi hỏi người đánh giá phải xác định, lượng giá ba thông số cơ bản sau:

- *p:* Mức độ hoàn thành của tiêu chuẩn
- μ_p*:* Lượng giá tiêu chuẩn
- δ_p*:* Sai số của quyết định

Nội dung	Trọng số	Tiêu chuẩn	Trọng số	Mức độ đáp ứng				Lượng giá		Kết quả
				p_0	p_1	...	p_s	Tiêu chuẩn	Nội dung	
Q_1	W_1	q_{11}	w_{11}	$\langle \mu_{11.0}, \delta_{11.0} \rangle$	$\langle \mu_{11.1}, \delta_{11.1} \rangle$	...	$\langle \mu_{11.s}, \delta_{11.s} \rangle$	$\langle r_{11}, \delta_{11} \rangle$	$\langle R_1, \delta_1 \rangle$	$\langle R_*, \delta_* \rangle$
		...	...	...	...	...	...	...		
		q_{1n_1}	w_{1n_1}	$\langle \mu_{1n_1.0}, \delta_{1n_1.0} \rangle$	$\langle \mu_{1n_1.1}, \delta_{1n_1.1} \rangle$	...	$\langle \mu_{1n_1.s}, \delta_{1n_1.s} \rangle$	$\langle r_{1n_1}, \delta_{1n_1} \rangle$		
...	...	...	...	...	...	...	...	...	...	
Q_m	W_m	q_{m1}	w_{m1}	$\langle \mu_{m1.0}, \delta_{m1.0} \rangle$	$\langle \mu_{m1.1}, \delta_{m1.1} \rangle$	...	$\langle \mu_{m1.s}, \delta_{m1.s} \rangle$	$\langle r_{m1}, \delta_{m1} \rangle$	$\langle R_m, \delta_m \rangle$	
		...	...	...	...	...	...	...		
		q_{mn_m}	w_{mn_m}	$\langle \mu_{mn_m.0}, \delta_{mn_m.0} \rangle$	$\langle \mu_{mn_m.1}, \delta_{mn_m.1} \rangle$	...	$\langle \mu_{mn_m.s}, \delta_{mn_m.s} \rangle$	$\langle r_{mn_m}, \delta_{mn_m} \rangle$		

Bảng 4.2. Bảng lượng giá các tiêu chuẩn và nội dung.

Với mỗi kết quả lượng giá $\mu_{ij.k}$ sẽ tương ứng với tập mờ $\left(\mu_{ij.k} / p_k\right)$ chỉ ra tại mức độ đáp ứng p_k thì tiêu chuẩn q_{ij} của nội dung Q_i có giá trị là $\mu_{ij.k}$. Để đánh giá toàn diện về tiêu chuẩn này chúng ta cần xác định một vector tập mờ

dạng thức sau $\left(\left(\mu_{\text{ij.0}}/p_0\right),\left(\mu_{\text{ij.1}}/p_1\right),...,\left(\mu_{\text{ij.s}}/p_s\right)\right)$.

- Lượng giá tiêu chuẩn
  - $r_{\text{ij}}=\dfrac{\sum_{k=0}^{s}\left(\mu_{\text{ij.k}}*E\left(p_{\text{k}},\left\langle\mu_{\text{ij.k}},\delta_{\text{ij.k}}\right\rangle\right)\right)}{\sum_{k=0}^{s}\mu_{\text{ij.k}}}$; (4.7) Sai số $\delta_{\text{ij}}=\dfrac{\sum_{k=0}^{s}\left(\delta_{\text{ij.k}}*L\left(p_{\text{k}}\right)\right)}{\sum_{k=0}^{s}L\left(p_{\text{k}}\right)}$ (4.8)
- Lượng giá nội dung
  - $R_{\text{i}}=W_i*\left(\sum_{j=1}^{n_i}\left(r_{\text{ij}}*w_{\text{ij}}\right)\right)$; (4.9) Sai số $\delta_{\text{i}}=\sum_{j=1}^{n_i}\left(\delta_{\text{ij}}*w_{\text{ij}}\right)$ (4.10)
- Kết quả lượng giá hệ thống
  - $R_*=\sum_{i=1}^{m}R_{\text{i}}$; (4.11) Sai số $\delta_*=\dfrac{\sum_{i=1}^{m}\left(\delta_{\text{i}}*W_{\text{i}}\right)}{\sum_{i=1}^{m}W_i}=\dfrac{\sum_{i=1}^{m}\left(\delta_{\text{i}}*W_{\text{i}}\right)}{W_*}$ (4.12)

Nhận xét

- Phương pháp đã thể hiện được quá trình tư duy của người đánh giá từ khi thu thập thông tin đến khi ra quyết định lượng giá.
- Với mỗi quyết định lượng giá, thực chất chính là quá trình người đánh giá quyết định quan hệ giữa mức độ đáp ứng của hệ thống với tiêu chuẩn đang đánh giá. Đồng thời cũng nhận xét về quyết định của bản thân thông qua giá trị sai số.
- Việc lựa chọn các mốc đánh giá trong phân loại mức độ đáp ứng có thể rất linh hoạt, phụ thuộc vào từng hệ thống cụ thể. Tương ứng với các mốc phân loại, chúng ta có thể chọn một hàm lượng giá tương ứng, hàm này thể hiện giá trị tối đa có thể nhận được khi hoàn thành đầy đủ mốc đánh giá. Đây cũng là yếu tố thể hiện tính mềm dẻo, rất phù hợp trong lượng giá tập mờ.
- Phương pháp trợ giúp cho người ra quyết định đánh giá được mức độ chính xác của công tác lượng giá dựa vào việc xem xét giá trị sai số trong từng công đoạn đánh giá.
- Khi cần kiểm tra tính chính xác của một quyết định, chúng ta có thể thực hiện kiểm tra mức độ đột biến trong kết quả với những quyết định khác. Đây cũng

là một tính chất thể hiện quá trình nhận xét, ra quyết định khi phải kết nhập từ nhiều nguồn tin.

- Để kết quả được chính xác và phù hợp, đòi hỏi giá trị các trọng số phải phù hợp, điều này có thể thực hiện được thông qua việc hiệu chỉnh trên các tập dữ liệu mẫu đã được đánh giá.

4.6. Phân mức an ninh mạng trên cơ sở tập mờ và lập luận xấp xỉ

Mỗi hệ thống sau khi được lượng giá sẽ xác định một vector tập mờ tương ứng. Để trợ giúp cho quá trình lượng giá chính xác, cần phải xây dựng bộ ma trận tập mờ chuẩn (tập mờ mẫu) dựa trên kết quả đánh giá các hệ thống chuẩn. Những ma trận tập mờ chuẩn này là tập hợp của nhiều vector tợp mờ thể hiện sự đánh giá trên tiêu chuẩn và đã phân mức an ninh $Ai\left(1\le i\le h\right)$. Vì đã có *h* mức an ninh nên cần có *h* bộ ma trận tập mờ chuẩn (tập mờ mẫu) xác định mức an ninh bao gồm

Mức an ninh A1 ... *Mức an ninh Ah*

$$\begin{bmatrix} \left(A1_1^1/W_1\right) & .. & .. & \left(A1_m^1/W_m\right) \\ \left(A1_1^2/W_1\right) & .. & .. & \left(A1_m^2/W_m\right) \\ .. & .. & .. & .. \\ \left(A1_1^{u_1}/W_1\right) & .. & .. & \left(A1_m^{u_1}/W_m\right) \end{bmatrix}_{u_1 x m} \quad ... \quad \begin{bmatrix} \left(Ah_1^1/W_1\right) & .. & .. & \left(Ah_m^1/W_m\right) \\ \left(Ah_1^2/W_1\right) & .. & .. & \left(Ah_m^2/W_m\right) \\ .. & .. & .. & .. \\ \left(Ah_1^{u_h}/W_1\right) & .. & .. & \left(Ah_m^{u_h}/W_m\right) \end{bmatrix}_{u_h x m}$$

Trong đó $0<u_{\mathrm{i}}\left(1\le i\le h\right)$. Biểu diễn ma trận tập mờ trên qua vector tập mờ $V_k^i=\left[\left(Ai_1^k/W_1\right)\ \left(Ai_2^k/W_2\right)\ ..\ \left(Ai_m^k/W_m\right)\right]_{1xm}$, ta có

$$\begin{bmatrix} \left(Ai_1^1/W_1\right) & .. & .. & \left(Ai_m^1/W_m\right) \\ \left(Ai_1^2/W_1\right) & .. & .. & \left(Ai_m^2/W_m\right) \\ .. & .. & .. & .. \\ \left(Ai_1^{u_i}/W_1\right) & .. & .. & \left(Ai_m^{u_i}/W_m\right) \end{bmatrix}_{u_i x m} = \begin{bmatrix} V_1^i \\ V_2^i \\ .. \\ V_{u_i}^i \end{bmatrix}_{u_i x 1}$$

Lượng giá mức độ an ninh

Sử dụng bộ ma trận tập mờ chuẩn xác định mức an ninh, chúng ta đưa vào như các tham số cho bài toán SISO tương ứng với từng mức an ninh $Ai\left(1\le i\le h\right)$ chúng ta có bộ luật suy diễn sau:

Ma trận A1	..	*Ma trận Ah*
IF V_1=$\overline{V_1^1}$ THEN A(V_1)=	.	IF V_h=$\overline{V_1^h}$ THEN A(V_h)=
IF V_1=$\overline{V_2^1}$ THEN A(V_1)=		IF V_h=$\overline{V_2^h}$ THEN A(V_h)=
...	...	...
IF V_1=$\overline{V_{u_1}^1}$ THEN A(V_1)=		IF V_h=$\overline{V_{u_h}^h}$ THEN A(V_h)=

Áp dụng thuật giải lập luận xấp xỉ sử dụng độ đo tương tự giữa các tập mờ, với $V_i = V_i^0 = V_0 = \left[\left(R_1^0/W_1\right)\ \left(R_2^0/W_2\right)\ ..\ ..\ \left(R_m^0/W_m\right)\right]$ chúng ta được tập giá trị

$$A\left(V_1^0\right)=Max\left(S_1\left(V_0,V_1^1\right),S_1\left(V_0,V_2^1\right),...,S_1\left(V_0,V_{u_1}^1\right)\right)\Rightarrow V_{k_1}^1$$
$$A\left(V_2^0\right)=Max\left(S_1\left(V_0,V_1^2\right),S_1\left(V_0,V_2^2\right),...,S_1\left(V_0,V_{u_2}^2\right)\right)\Rightarrow V_{k_2}^2$$
... (4.14)
$$A\left(V_h^0\right)=Max\left(S_1\left(V_0,V_1^h\right),S_1\left(V_0,V_2^h\right),...,S_1\left(V_0,V_{u_h}^h\right)\right)\Rightarrow V_{k_h}^h$$
$$A\left(V_k^0\right)=Max\left(A\left(V_1^0\right),A\left(V_2^0\right),...,A\left(V_h^0\right)\right)\Rightarrow V_{k_j}^k;1\le k\le h,k_j\in\left(k_1,k_2,..,k_h\right)$$

Xác định kết quả lượng giá mức độ an ninh hệ thống $R_*\in\left(A1,A2,...,Ah\right)$

$$R_*=\begin{cases}Ak & \text{if } \gamma\le S_2(V_0,V_{k_j}^k)\\ \varnothing & \text{if } \gamma>S_2(V_0,V_{k_j}^k)\end{cases}$$ với γ là ngưỡng xác định tồn tại R_* (4.15)

Nhận xét

- Phương pháp đã kế thừa một số đặc điểm của phương pháp "Nâng cao độ chính xác trong lượng giá mức độ an ninh mạng bằng phương pháp ứng dụng tập mờ khi ra quyết định" (*). Tuy nhiên trong nội dung phương pháp (*) thể hiện quá trình đánh giá có tính độc lập tương đối, còn phương pháp này thực hiện lượng giá dựa trên mối tương quan của hệ thống hiện tại với các hệ thống tiêu chuẩn khác.
- Phương pháp thể hiện được quá trình tư duy của người đánh giá từ khi thu thập thông tin đến khi ra quyết định lượng giá. Quyết định lượng giá các tiêu chuẩn đã được chuẩn hóa thông qua mối tương quan giữa hệ thống thực và các hệ thống chuẩn đã lưu trữ dưới dạng bộ ma trận tập mờ chuẩn xác định

mức an ninh. Đây cũng là điểm thể hiện đúng suy nghĩ, tư duy khi lượng giá của người đánh giá.

- Kết quả thu được là mức độ an ninh của hệ thống. Số lượng mức an ninh là không hạn chế, phụ thuộc vào từng hệ thống cụ thể, đây là điểm mạnh của phương pháp vì thông thường các phương pháp đang sử dụng chỉ sử dụng ba mức an ninh mạng là [H(High), M(Medium), L(Low)].

Kết luận

1. Để giảm sai số khi lượng giá các yếu tố định tính cần cải tiến trên từng khâu của quá trình đánh giá, lượng giá.
2. Khi ứng dụng các phương pháp và công cụ toán học như tập mờ, lập luận tương tự vào trong quá trình đánh giá, đưa ra kết quả lượng giá sẽ giúp hạn chế phần nào tính chủ quan và sai số trong mỗi quyết định.
3. Phương pháp "Nâng cao độ chính xác trong lượng giá mức độ an ninh mạng bằng phương pháp ứng dụng tập mờ khi ra quyết định" thể hiện được tính độc lập tương đối của hệ thống cần đánh giá với các hệ thống khác. Đồng thời việc lượng giá một hệ thống mới không cần tham khảo giá trị đã đánh giá từ các hệ thống đã thực hiện lượng giá.
4. Phương pháp "Phương pháp phân mức an ninh mạng trên cơ sở tập mờ và lập luận xấp xỉ" có kết quả lượng giá bị ảnh hưởng nhiều bởi các hệ thống khác đã được đánh giá. Việc áp dụng phương pháp vào thực tiễn đòi hỏi phải xây dựng được một cơ sở dữ liệu "chuẩn" từ đó "đối sánh" tìm ra kết quả lượng giá mức độ an ninh tổng thể của hệ thống thông qua các yếu tố định tính và một số tiêu chuẩn an ninh quốc tế.

KẾT LUẬN VÀ KIẾN NGHỊ

Luận án đi vào nghiên cứu vấn đề về an ninh hệ thống bằng phương pháp tổng quan tiến tới nghiên cứu chuyên sâu lĩnh vực kiểm tra, đánh giá và xác định giá trị an ninh hệ thống.

I. NHỮNG ĐÓNG GÓP MỚI CỦA LUẬN ÁN

1. Đề xuất phương pháp xác định mục tiêu tấn công dựa vào sự rò rỉ thông tin và rủi ro đang tồn tại trong hệ thống thông tin, kết quả này được trình bày trong bài báo số 1.
2. Để thực hiện tăng cường an ninh cho sản phẩm kỹ thuật số, bài báo số 2 đã nghiên cứu và đề xuất phương pháp thủy ấn kết hợp với mã hóa không hoàn toàn ứng dụng trong kiểm tra bản quyền sản phẩm nhưng vẫn đảm bảo chất lượng nội dung phân phối tới người sử dụng.
3. **Lượng giá an ninh các yếu tố định tính:** Các bài báo số 3, 4,5 đề xuất phương pháp ứng dụng tập mờ để giảm sai số lượng giá các yếu tố định tính với phương thức cải tiến trên từng khâu của quá trình đánh giá. Kết quả lượng giá đã hạn chế phần nào tính chủ quan và sai số trong mỗi quyết định.
   - Bài báo số 3 đề xuất phương pháp xử lý ánh xạ từ ngôn ngữ tự nhiên khi đánh giá thành kết quả lượng án dựa trên lập luận xấp xỉ kết hợp với đại số gia tử.
   - Bài báo số 4 đề xuất ứng dụng tập mờ trong phân đoạn các quyết định lượng giá, từ đó tính toán và ra quyết định có độ chính xác cao với tham số đầu vào là bộ tập mờ đã được tiền xử lý.
   - Bài báo số 5 đề xuất xây dựng cơ sở dữ liệu chuẩn về các mức độ lượng giá an ninh đã thực hiện, từ đó áp dụng lập luận xấp xỉ tìm ra kết quả mẫu có đặc điểm phù hợp nhất với hệ thống cần đánh giá. Các hệ thống đã được lượng giá sẽ tiếp tục được bổ sung làm tăng cơ sở dữ liệu mẫu, quá trình này sẽ giúp việc lượng giá càng nhiều sẽ càng chính xác.
4. **Lượng giá an ninh các yếu tố định lượng:** Các phương pháp lượng giá các yếu tố định lượng hiện nay chỉ đưa ra danh sách các điểm yếu của hệ thống cần khắc phục, chưa xác định được kết quả lượng giá chính xác có khả năng so sánh sức mạnh phòng thủ, chưa thể hiện rõ mối quan hệ giữa các yếu tố gây mất an ninh trong hệ thống, chưa có một mô hình hoàn thiện ứng dụng

trong công tác lượng giá các yếu tố định lượng. Các kết quả trong công trình số 6 (định lượng cho máy tính) và số 7 (định lượng mạng máy tính) đã đưa ra mô hình và cách tính cụ thể giá trị an ninh để sử dụng cho mục đích trên.

- Bài báo số 6 đề xuất một mô hình quan hệ có sử dụng giá trị định lượng của các rủi ro bao gồm tính phổ biến, tính đơn giản, tính phá hoại, tỉ lệ rủi ro bị tấn công làm tham số đầu vào trong lượng giá mức độ an ninh cho hệ thống máy tính giúp cho kết quả lượng giá chỉ rõ được cụ thể điểm yếu của hệ thống, từ đó tìm ra phương thức khắc phục nhanh nhất.
- Bài báo số 7 đề xuất phương pháp lượng giá an ninh cho hệ thống mạng tổng thể theo mô hình phân cấp sau quá trình biến đổi và sử dụng tham số định lượng. Để thực hiện được quá trình này, các máy tính và mạng máy tính phải được lượng giá an ninh theo hướng tìm kiếm rủi ro đã được đề cập tại công trình số 6. Trong nghiên cứu này, các kết luận cũng chỉ ra việc để có kết quả chính xác cần quan tâm tới thiết lập vị trí bộ đo an ninh vì nó ảnh hưởng nhiều tới kết quả lượng giá toàn cục, mỗi vị trí bộ đo khác nhau có thể cho các kết quả lượng giá an ninh mạng khác nhau sau quá trình biến đổi. Cách thức tiếp cận hệ thống mạng cũng phải lựa chọn cho phù hợp với thực tiễn khi triển khai lượng giá.

II. KIẾN NGHỊ

Với mục tiêu hoàn thiện những kết quả nghiên cứu đã có, luận án kiến nghị một số hướng phát triển tiếp theo:

1) Tối ưu hóa các phương pháp lập luận xấp xỉ, nghiên cứu sử dụng các phép kết nhập hiệu quả hơn có khả năng thay thế phương pháp kết nhập đã sử dụng trong lượng giá các yếu tố định tính.
2) Triển khai trên các hệ thống thật, tìm ra bộ tham số phù hợp cho phân mức hoàn thành và bộ ma trận tập mờ làm tiêu chuẩn trong lượng giá.

3) Nghiên cứu kỹ hơn bản chất, các yếu tố liên quan tới của an ninh hệ thống từ đó xây dựng mô hình, mối quan hệ giữa chúng, ứng dụng các tham số định lượng mới trong lượng giá mức độ an ninh.
4) Tìm kiếm giải pháp, phương thức tổng hợp vấn đề an ninh cho hệ thống sau quá trình lượng giá, giúp cho công tác quản lý, quản trị được nhanh chóng và đơn giản.