XÂY DỰNG CHÍNH SÁCH AN TOÀN THÔNG TIN CHO CÁC CƠ QUAN THÔNG TIN-THƯ VIỆN VỚI ISO 17799 – 27001

ThS Nguyễn Văn Hiệp
Khoa TT-TV, Trường Đại học KHXH&NV, ĐHQG Tp. Hồ Chí Minh

Tóm tắt: Chính sách an toàn bảo mật thông tin là cốt lõi, là trung tâm để có thể bắt đầu xây dựng các giải pháp an toàn thông tin cho một hệ thống thông tin nói chung và các cơ quan thông tin-thư viện nói riêng. Bài viết trình bày những vấn đề cơ bản về an toàn thông tin, chính sách an toàn thông tin, sự cần thiết của việc xây dựng chính sách an toàn thông tin, các tiêu chuẩn an toàn thông tin-cơ sở để xây dựng chính sách an toàn thông tin cho các cơ quan thông tin-thư viện.

Từ khóa: Chính sách an toàn thông tin; an toàn thông tin; thông tin-thư viện.

Developing information security policies for information-library agencies with ISO 17799 – 27001

Abstract: The information security policy is the core factor, which is the center to be able to start building information security solutions for an information system in general and information agencies - libraries in particular. The paper presents the basic issues related to information security, information security policy, the necessity of building information security policy, as well as the information security standards - the foundation for building information security policies at information agencies - libraries.

Keywords: Information security policies; information security; information library.

ĐẶT VẤN ĐỀ

Sự phát triển như vũ bão của công nghệ thông tin và truyền thông đang ngày một tác động sâu sắc đến kinh tế, chính trị và đời sống xã hội. Ngày càng nhiều tổ chức, đơn vị, doanh nghiệp hoạt động lệ thuộc gần như hoàn toàn vào hệ thống mạng máy tính, máy tính và cơ sở dữ liệu. Nói cách khác, khi hệ thống thông tin hoặc cơ sở dữ liệu gặp sự cố thì hoạt động của các đơn vị này bị ảnh hưởng nghiêm trọng, thậm chí có thể bị tê liệt hoàn toàn. Chưa bao giờ vấn đề an toàn bảo mật thông tin lại nhận được nhiều sự quan tâm như hiện nay. An toàn thông tin giờ đây được xếp ngang hàng với những vấn đề thiết thực trong cuộc sống như: An toàn thực phẩm, An toàn y tế, An toàn lao động,... Nó không chỉ là mối quan tâm của các công ty, tổ chức liên quan trực tiếp tới tiền tệ như: ngân hàng, các tổ chức thương mại, tín dụng,… mà nó là mối quan tâm chung của tất cả các cơ quan, tổ chức, doanh nghiệp hoạt động có sử dụng máy tính, mạng máy tính và internet, trong đó có các cơ quan thông tin-thư viện (TT-TV), đặc biệt là các thư viện điện tử, thư viện số.

Hãy tưởng tượng điều gì sẽ xảy ra nếu cơ sở dữ liệu nội sinh mà thư viện đã xây dựng với hàng triệu tài liệu, hệ thống mục lục trực tuyến với hàng chục ngàn biểu ghi tự nhiên biến mất? Các thông tin về bạn đọc của thư viện tự nhiên "không cánh mà bay", hay website, hệ thống phần mềm quản trị thư viện, các thông tin/dữ kiện khác do thư viện tạo ra không còn tồn tại hay vận hành không như mong đợi? Chắc hẳn không ai mong muốn những rủi ro trên xảy ra.

Tuy nhiên, để xây dựng được một hệ thống đảm bảo an toàn, bảo mật thông tin toàn diện, hiệu quả thì không phải là một công việc dễ dàng, đặc biệt đối với các cơ quan TT-TV, nơi vấn đề an toàn bảo mật thông tin còn là một khái niệm khá mới mẻ, nơi cán bộ thư viện còn nhiều hạn chế về công nghệ, nơi mà vấn đề an toàn bảo mật thông tin thường được mặc định dành cho bộ phận IT,… do đó chúng ta cứ loay hoay trong một mớ các câu hỏi, an toàn thông tin phải thực hiện từ đâu, cái gì làm trước, cái gì làm sau, ai chịu trách nhiệm thực hiện công việc này, an toàn thông tin cần có những yếu tố nào,… nhằm trả lời những câu hỏi nêu trên. Bài viết mong muốn góp phần cung cấp một cái nhìn cơ bản về an toàn bảo mật thông tin,

chính sách an toàn bảo mật thông tin- thành phần quan trọng đầu tiên trong tiến trình xây dựng hệ thống đảm bảo an toàn thông tin, các tiêu chuẩn an toàn thông tin thường được sử dụng khi xây dựng các chính sách an toàn thông tin (ATTT).

1. AN TOÀN BẢO MẬT THÔNG TIN LÀ GÌ?

Theo Nghị định số 64/2007/NĐ-CP ngày 10 tháng 04 năm 2007 về Ứng dụng công nghệ thông tin trong hoạt động của các cơ quan nhà nước: "*An toàn thông tin: bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. Việc bảo vệ thông tin, tài sản và con người trong hệ thống thông tin nhằm bảo đảm cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng*" [Nghị định 64/2007/NĐ-CP].

Theo ISO 17799, "*An toàn bảo mật thông tin là khả năng bảo vệ đối với môi trường thông tin kinh tế xã hội, đảm bảo cho việc hình thành, sử dụng và phát triển vì lợi ích của mọi công dân, mọi tổ chức và của quốc gia. Thông qua các chính sách về ATTT, lãnh đạo thể hiện ý chí và năng lực của mình trong việc quản lý hệ thống thông tin. ATTT được xây dựng trên nền tảng một hệ thống các chính sách, quy tắc, quy trình và các giải pháp kỹ thuật nhằm mục đích đảm bảo an toàn tài nguyên thông tin mà tổ chức đó sở hữu cũng như các tài nguyên thông tin của các đối tác, các khách hàng trong một môi trường thông tin toàn cầu*" [ISO 17799].

Tựu chung lại, an toàn bảo mật thông tin là sự duy trì tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin, trong đó:

- Tính bí mật: Thông tin chỉ được phép khai thác bởi những đối tượng (người, chương trình máy tính,…) được phép.

- Tính toàn vẹn: Đảm bảo tính toàn vẹn của thông tin, tức là thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được cấp phép và phải đảm bảo thông tin vẫn còn chính xác khi được lưu trữ và truyền đi.

- Tính sẵn sàng: Đảm bảo độ sẵn sàng của thông tin, tức là thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn.

Cũng như vậy, an toàn bảo mật thông tin trong hoạt động thư viện "là việc đảm bảo phần cứng, các dịch vụ, các chương trình và thông tin luôn ở trạng thái sẵn sàng cho người sử dụng" [Banerjee, K, 2003]. Nói cách khác, đảm bảo ATTT trong thư viện là việc bảo vệ thông tin và hệ thống thông tin khỏi các truy cập, chỉnh sửa hoặc sử dụng thông tin trái phép. Việc đảm bảo ATTT trong thư viện cũng gồm 3 yêu cầu: tính bí mật, tính toàn vẹn và tính sẵn sàng.

- Bí mật: Chỉ những người dùng được cấp quyền mới được phép truy cập vào các cơ sở dữ liệu, nguồn tài liệu điện tử và các tài nguyên khác của thư viện. Thư viện không được phép tiết lộ thông tin của người sử dụng như: các thông tin cá nhân, thông tin về lịch sử mượn-trả,…).

- Toàn vẹn: Đảm bảo sự chính xác, không thay đổi của thông tin gốc (ví dụ như các thông tin thư mục trong các cơ sở dữ liệu, thông tin được đăng tải trên website của thư viện,…).

- Sẵn sàng: Các nguồn tin của thư viện luôn ở trong trạng thái sẵn sàng cho người sử dụng truy cập vào bất cứ thời gian nào (ví dụ: hệ thống Opac, website thư viện, các cơ sở dữ liệu điện tử,…)

2. SỰ CẦN THIẾT CỦA VIỆC XÂY DỰNG CHÍNH SÁCH AN TOÀN THÔNG TIN TRONG CÁC CƠ QUAN THÔNG TIN - THƯ VIỆN

Theo các tài liệu về ATTT, để đảm bảo an toàn cho một hệ thống, cần phải có các yếu tố: con người, quy trình, giải pháp, và các tiêu chuẩn quốc tế.

Hiện nay, các thư viện đã quan tâm tới vấn đề an toàn bảo mật thông tin, bằng chứng là việc một số thư viện đã trang bị cho mình hệ thống tường lửa (firewall), hệ thống phát hiện xâm nhập IDS (Intrusion Detection Systems), hệ thống phòng chống xâm nhập IPS (Intrusion prevention system), hệ thống phòng chống virus (Antivirus),… Tuy nhiên, tất cả mới chỉ là các giải pháp công nghệ. Một câu hỏi được đặt ra là hệ thống đã được trang bị giải pháp bảo mật nhưng mức độ

an toàn đến đâu, giải pháp đã tốt chưa, đã đầy đủ chưa, tổ chức thực hiện giải pháp đã tốt hay chưa, con người thực hiện giải pháp thế nào, họ đã ý thức các vấn đề về ATTT và đã được gán trách nhiệm phải đảm bảo an toàn hệ thống thông tin hay chưa? Thông thường, các giải pháp lúc xây dựng xong thì tốt nhưng chỉ sau một thời gian hoạt động sẽ bộc lộ nhiều điểm yếu mà nguyên nhân chính là do yếu tố con người.

Hạ tầng công nghệ thông tin xây dựng tốt, hệ thống bảo mật xây dựng tốt nhưng sau khi đưa vào sử dụng, chất lượng sẽ phụ thuộc vào chính bản thân đối tượng sử dụng nó. Họ có tuân thủ theo đúng giải pháp hay không, trách nhiệm của họ thế nào, ý thức ra sao? Chúng ta biết bảo mật đi kèm với việc mang lại sự không thuận tiện cho người dùng và dễ dàng làm cho họ từ bỏ các biện pháp bảo mật. Tuy nhiên, trong các thư viện, ATTT luôn phải được đưa lên hàng đầu và tất cả các nhân viên đều phải tuân thủ điều này.

Có thể thấy rằng, các cơ quan TT-TV đang chủ yếu thực hiện khâu giải pháp. Các yếu tố khác như con người, qui trình, tiêu chuẩn quốc tế chưa được chú trọng. Các yếu tố đó chưa tốt và chưa gắn kết, chưa được giám sát bởi còn thiếu một yếu tố rất quan trọng, đó là chính sách an toàn bảo mật thông tin.

Chính sách an toàn bảo mật thông tin (Infomaton security policy): *là những chỉ thị và hướng dẫn về an toàn thông tin.* Hay *Chính sách an toàn thông tin là tập hợp các luật, quy tắc và các thủ tục nhằm điều chỉnh cách một tổ chức quản lý, bảo vệ và phân phối tài nguyên một cách hợp lý, để đạt được các mục tiêu an toàn thông tin cụ thể. Các luật, quy tắc và các thủ tục này phải được gắn với trách nhiệm của từng cá nhân, và có thể xác định cụ thể các điều kiện mà trong đó các cá nhân được phép thực thi quyền hạn của mình.*

Hay *chính sách an toàn bảo mật thông tin là tài liệu hướng dẫn về an toàn thông tin trong một tổ chức. Tài liệu này đề cập đến sự hỗ trợ của cấp quản lý, cam kết và định hướng trong việc đạt được các mục tiêu về an toàn thông tin. Chính sách an toàn bảo mật thông tin là một văn bản mang tính khái niệm, không cụ thể về phương thức thi hành, bao gồm các tiêu chí an toàn thông tin của một tổ chức.*

Theo "Sách da cam" (1983), *Chính sách an toàn bảo mật thông tin là tập hợp các điều luật, các qui định và các giải pháp thực tế để giám sát sự điều khiển, sự bảo vệ và việc phân phối các thông tin nhạy cảm trong hệ thống.*

Tóm lại, chính sách ATTT thể hiện những quy định chung nhất của các cấp lãnh đạo đối với việc bảo vệ hệ thống thông tin, bao gồm đầy đủ các yếu tố: thông tin (Information), hạ tầng thông tin (phần cứng, phần mềm, mạng và các hệ thống khác,…) và các ứng dụng (CSDL, Web, ứng dụng nghiệp vụ,…).

Chính sách ATTT là cốt lõi, là trung tâm để có thể bắt đầu xây dựng các giải pháp ATTT. Từ chính sách ATTT, ngoài việc sẽ đưa ra được giải pháp an ninh toàn diện còn gắn với ý thức, trách nhiệm của từng nhân viên trong thư viện về ATTT. Từ lâu, hậu quả của việc không xây dựng chính sách ATTT mà chỉ có giải pháp an ninh đã khiến cho giải pháp trở nên không toàn diện và hiệu quả.

Hiện tại, các cơ quan TT-TV chỉ mới đưa ra các giải pháp công nghệ là chính mà chưa xây dựng cùng với chính sách ATTT, hay nói cách khác là xây dựng theo mô hình "bottom-up". Tức là xây dựng hạ tầng thông tin, giải pháp bảo mật trước rồi sau đó mới xây dựng chính sách ATTT và thậm chí là chưa xây dựng. Chính vì vậy, các giải pháp công nghệ xây dựng đều không toàn diện, thiếu đâu vá đấy, không mang tính tổng thể đồng bộ, chi phí cao. Ví dụ: Đề xuất xây dựng hệ thống bảo mật mạng với firewall, IPS nhưng sau đó do hệ thống máy tính bị virus, lại đề xuất giải pháp diệt virus. Khi thấy hệ thống không kiểm soát được việc truy cập mạng, lại đề xuất giải pháp kiểm soát truy cập mạng NAC,... Điều này thể hiện sự thiếu toàn diện, đồng bộ, chiến lược.

Theo khuyến cáo của các tổ chức trên thế giới, để xây dựng hệ thống an toàn thì nên xây dựng theo mô hình "top-down" tức là phải xây dựng chính sách ATTT trước. Tổ chức thực thi theo chính sách ATTT bao gồm con người, quy trình, giải pháp công nghệ, vật lý. Phương pháp này đạt được tính toàn diện, đồng bộ và lâu dài. Và cũng trong các tài liệu chuẩn về ATTT như ISO 17799, ISO 27001 hay COBIT, nhiệm vụ xây dựng chính sách bảo mật đều được đặt lên đầu tiên trong lộ trình xây dựng hệ thống ATTT.

3. CÁC TIÊU CHUẨN AN TOÀN THÔNG TIN (ISO/IEC 17799 VÀ ISO 27001)- CƠ SỞ ĐỂ XÂY DỰNG CHÍNH SÁCH AN TOÀN THÔNG TIN CHO CÁC CƠ QUAN THÔNG TIN - THƯ VIỆN

Tuân thủ tiêu chuẩn ATTT là yếu tố quan trọng đảm bảo cho sự hoạt động ổn định và tin cậy của hạ tầng kỹ thuật, sự an toàn của hệ thống thông tin và dữ liệu của các cơ quan TT-TV.

Hiện nay, trên thế giới đã hình thành một hệ thống tiêu chuẩn ATTT tương đối đầy đủ, bao quát được hầu hết các khía cạnh của lĩnh vực ATTT và đáp ứng mọi đối tượng cần tiêu chuẩn hóa (sản phẩm, dịch vụ, quy trình). Hệ thống tiêu chuẩn này có thể phân thành ba loại gồm: tiêu chuẩn đánh giá, tiêu chuẩn đặc tả và tiêu chuẩn về quản lý.

Có nhiều quan điểm và cách thức để thiết lập một chính sách ATTT. Tuy nhiên, thông thường người ta dựa vào các tiêu chuẩn về quản lý ATTT, trong số đó hai tiêu chuẩn ISO 27001 và ISO/IEC 17799 thường được nhắc đến và sử dụng nhiều nhất, bởi tính hệ thống, tính thông dụng và tính quốc tế của chúng. Khi xây dựng một hệ thống ATTT, người ta thường tham khảo cả hai như một cặp không thể tách rời. Khi áp dụng, tiêu chuẩn ISO 27001 đưa ra các yêu cầu cho việc xây dựng, áp dụng, điều hành, kiểm tra, giám sát và phát triển hệ thống an ninh thông tin một cách toàn diện và khoa học, ISO 27001 được xây dựng hòa hợp, tương thích với các hệ thống quản lý khác như: ISO 9001:2000 và ISO 14001:2004,... Trong khi đó, ISO/IEC 17799 cung cấp các kinh nghiệm để có thể thiết kế một hệ thống cụ thể, mang tính tham khảo, với những điều chỉnh có thể được thực hiện để phù hợp với nhu cầu của tổ chức áp dụng và nó cũng là cơ sở để xem xét đánh giá cấp chứng chỉ của tổ chức bên thứ ba.

3.1. ISO/IEC 17799

ISO/IEC 17799 do Tổ chức Tiêu chuẩn hóa quốc tế (ISO) và Ủy ban Kỹ thuật điện quốc tế (IEC) soạn thảo. ISO 17799 là tài liệu chính thức phản ánh toàn bộ các vấn đề liên quan tới ATTT.

ISO/IEC 17799 cung cấp cho các chuyên gia về ATTT một bức tranh tổng thể, chính xác và logic về những bước cần thiết để xây dựng một hệ thống thông tin an toàn, hệ thống chất lượng ATTT ISO 17799 đã đề cập đến toàn bộ các chính sách về ATTT từ tổ chức, con người, môi trường làm việc đến các giải pháp cụ thể để thiết lập hệ thống ATTT.

Hệ thống tiêu chuẩn ISO 17799 tác động tới 10 lĩnh vực gồm 127 giải pháp. ISO 17799 có thể chia thành 3 phần chính:

1. Những vấn đề chính về ISO 17799.

2. Chính sách về ATTT và những tài liệu về ATTT.

3. Các giải pháp, phương tiện và các thành phần ATTT.

ISO 17799 cũng chỉ ra rằng không có một tập hợp các kiểm soát nào đạt được an toàn bảo mật hoàn thiện. Do đó, ISO khuyến khích các can thiệp thêm từ lãnh đạo để theo dõi, đánh giá và cải tiến hiệu lực của các kiểm soát an toàn bảo mật hỗ trợ cho các mục tiêu ATTT của tổ chức.

Nội dung tiêu chuẩn ISO 17799:

Chuẩn ISO 17799 thiết lập các hướng dẫn và nguyên tắc chung nhằm thi hành, duy trì và tăng cường quản lý ATTT trong tổ chức. Hiện nay, bản cập nhật mới nhất của tiêu chuẩn ISO 17799-2005 bao gồm 11 phần sau:

1. Chính sách an ninh chung (Security Policy)

2. Tổ chức ATTT (Organizing Information Security)

3. Quản lý sự cố ATTT (Information Security Incident Management)

4. Xác định, phân cấp và quản lý tài nguyên (Asset Management)

5. An ninh nhân sự (Human Resources Security)

6. An ninh vật lý và môi trường (Physical and Environmental Security)

7. Quản trị CNTT và mạng (Communication and Operations Management)

8. Quản lý truy cập (Access Control)

9. Phát triển và duy trì hệ thống (Informations System Acquisition, Development and Maintenance).

10. Quản lý tính liên tục kinh doanh (Business Continuity Management)

11. Yếu tố tuân thủ luật pháp (Compliance).

3.2. ISO 27001

Sự ra đời Tiêu chuẩn ISO/IEC 27001:2005 của Hệ thống quản lý ATTT (Information security management system -ISMS) đánh dấu một bước phát triển trong lĩnh vực bảo mật thông tin trên thế giới. Áp dụng ISMS giúp cho các cơ quan TT - TV kiến trúc một mô hình quản lý hệ thống tiên tiến với những giải pháp ATTT tổng thể hiệu quả, chi phí hợp lý nhằm bảo vệ hoạt động của mình.

Từ năm 2005 đến nay, bộ tiêu chuẩn ISO/IEC 27000 liên tục được hoàn thiện để cung cấp những công cụ quản lý mang tính quốc tế, đảm bảo cho quá trình thiết lập, vận hành, giám sát, xem xét, duy trì và cải tiến hệ thống quản lý ATTT. Bộ tiêu chuẩn ISO/IEC 27000 gồm các tiêu chuẩn sau:

- ISO/IEC 27000 : 2009 Các nguyên tắc và từ vựng
- ISO/IEC 27001: 2005 Các yêu cầu Hệ thống quản lý ATTT
- ISO/IEC 27002: 2005 Mã thực hành Hệ thống quản lý ATTT
- ISO/IEC 27003: 2010 Hướng dẫn áp dụng Hệ thống quản lý ATTT
- ISO/IEC 27004: 2007 Đo lường Hệ thống quản lý ATTT
- ISO/IEC 27005: 2007 Quản lý rủi ro Hệ thống quản lý ATTT
- ISO/IEC 27006: 2007 Dành cho các tổ chức đánh giá và chứng nhận ISMS.

Trong các tiêu chuẩn trên, ISO/IEC 27001:2005 chính là những yêu cầu bắt buộc đối với tổ chức khi xây dựng, vận hành, duy trì và cũng là cơ sở để các tổ chức tư vấn, đánh giá quản lý chất lượng thực hiện công việc chuyên môn của mình. Các tiêu chuẩn khác trong bộ ISO/IEC 27000 được coi như những công cụ hỗ trợ phục vụ cho tiêu chuẩn ISO/IEC 27001:20005.

Việc áp dụng một hệ thống quản lý ATTT sẽ giúp các cơ quan TT-TV ngăn ngừa, hạn chế các tổn thất trong hoạt động nghề nghiệp của mình, như: hư hỏng, mất mát các thông tin, dữ liệu quan trọng.

Trên thế giới việc xây dựng các chính sách ATTT gần như một yêu cầu hiển nhiên, có thể tham khảo các chính sách ATTT như của trường: The London school of economics and Political science (LSE) tại địa chỉ: https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/infSecPol.pdf hoặc của Trường Đại học London (University of London) tại địa chỉ: https://london.ac.uk/sites/default/files/governance/ISP-001-information-security-policy.pdf

KẾT LUẬN

Không có chính sách ATTT thì mọi cố gắng xây dựng giải pháp ATTT sẽ không có một định hướng và cơ sở pháp lý để thực hiện, đồng thời các giải pháp kỹ thuật cao cấp và đắt tiền nhất cũng sẽ không hiệu quả do thiếu những quy định đối với thành phần nhân lực trong hệ thống. Thêm vào đó, không có bộ chính sách về ATTT thì sẽ không có được sự phối hợp của các bộ phận khác nhau có liên quan đến chương trình ATTT. Vì vậy, việc xây dựng một chính sách ATTT trong các cơ quan TT-TV là một việc làm thực sự cần thiết. Nó vừa là tiền đề để xây dựng các giải pháp bảo mật toàn diện, hiệu quả, vừa mang tới tính đồng bộ và tiết kiệm chi phí cho các cơ quan TT-TV.

TÀI LIỆU THAM KHẢO

1. Banerjee, K. (2003). How much security does your library need? Computers in Libraries, 23(5), 12-15. Truy cập ngày 28/01/2022, từ cơ sở dữ liệu ProQuest.
2. Chính phủ (2007). Nghị định số 64/2007/NĐ-CP ngày 10 tháng 04 năm 2007 về ứng dụng công nghệ thông tin trong hoạt động các cơ quan nhà nước.
3. Karin Hone and J.H.P.Eloff (2002). Information security policy, What do international information security standards Say? Computers & Security, Volume 21, Issue 5, 1 October 2002, Pages 402-409, https://doi.org/10.1016/S0167-4048(02)00504-7 truy cập ngày 25/01/2022.
4. ISO/IEC 17799:2005: Information technology-Security techniques-Code of practice for information security management.
5. Olson, Ingrid M and Abrams, Marshall D (2003). Information Security Policy, https://www.yumpu.com/en/document/read/7936824/essay-7-information-security-policy-acsac (Truy cập ngày 20/01/2022).
6. Sách da cam (1983). Department of defense trusted computer system evaluation criteria (1983).

(Ngày Tòa soạn nhận được bài: 6-12-2021; Ngày phản biện đánh giá: 8-2-2022; Ngày chấp nhận đăng: 15-5-2022).