# TRƯỜNG ĐẠI HỌC SƯ PHẠM TP.HCM

**Khoa Công Nghệ Thông Tin**

**BÁO CÁO ĐỒ ÁN CHỦ ĐỀ 5: THẾ NÀO LÀ VĂN HÓA VÀ ĐẠO ĐỨC TRONG NGHIÊN CỨU KHOA HỌC?**

Thành phố Hồ Chí Minh – 2018

## 

## TRƯỜNG ĐẠI HỌC SƯ PHẠM TP.HCM

**Khoa Công Nghệ Thông Tin**

Môn: Phương pháp nghiên cứu khoa học

# ĐỀ TÀI: THẾ NÀO VĂN HÓA VÀ ĐẠO ĐỨC TRONG NGHIÊN CỨU KHOA HỌC?

**GVHD: TS. Lê Đức Long**

**Sinh viên thực hiện:NHÓM 111**

**1.Phan Thị Nam Anh – 43.01.103.002**

**2. Mai Thị Xuân Chung – 43.01.103.006**

**Lớp: Sư phạm Tin A K43**

Thành Phố Hồ Chí Minh – Năm 2018

**I.NỘI DUNG TỰ NGHIÊN CỨU**

**Câu 1: Đọc tài liệu “Kĩ năng mềm” cho nhà khoa học của GS. Nguyễn Văn Tuấn. Cho biết những “Kĩ năng mềm” là gì?**

Theo GS. Nguyễn Văn Tuấn thì có hai kĩ năng mềm mà các nhà khoa học Việt Nam cần phải cải tiến và học hỏi, đó là: Kĩ năng thông tin ngoại giao. Kĩ năng thông tin ở đây là khả năng truyền đạt thông tin khoa học đến đồng nghiệp trong và ngoài nước qua viết và nói chuyện. Viết trên các tập san khoa học quốc tế đòi hỏi những kĩ năng về Tiếng Anh (vì phần lớn tập san khoa học ngày nay sử dụng Tiếng Anh) và cách biện luận, mà các đồng nghiệp trong nước đều rất nhiều. Điều này thì có thể hiểu được vì Tiếng Anh không phải là tiếng mẹ đẻ, ngay cả những ngay cả những người từng đi du học ở các nước nói tiếng anh cũng chưa thể viết hoàn chỉnh một bài báo cáo khoa học vì làm được việc này đòi hỏi thời gian cọ sát khá lâu mới trở thành chuyên nghiệp được. Ngay cả những nghiên cứu sinh mà tiếng anh là tiếng mẹ đẻ cũng khó có thể viết một bài báo cáo một cách chỉnh chu.

Nói chuyện trong các hội nghị khoa học đòi hỏi những kĩ năng chẳng những về ngôn ngữ mà còn nghệ thuật.

Và ông đưa ra một số nguyên tắc như sau:

\*Một số nguyên tắc khi đặt tựa đề cho bài báo khoa học

1.Nên cố gắng đặt tự đề với một thông điệp mới. Làm được như thế rất dễ gây sự chú ý của người đọc.

2.Không nên viết tựa đề theo kiểu phát biểu.

3.Không bao giờ sử dụng viết tắt trong tựa đề bài báo. Mỗi công trình nghiên cứu thường tập trung vào một vấn đề chuyên sâu nào đó, và nếu chúng ta sử dụng viết tắt thì chỉ những người trong ngành mới hiểu, còn những người ngoài ngành không hiểu và đó là một thiệt thòi cho nghiên cứu của mình.

4.Không nên viết tựa đề theo kiểu nghịch lí. Những tựa đề kiểu này có thể làm cho người đọc khó chịu, và có khi làm lần lộn vấn đề nghiên cứu.

5.Tựa đề không nên quá dài hay nhiều chữ. Tựa đề có nhiều chữ làm khó đọc và làm cho người đọc dễ quên. Thông thường, tác giả nên cố gắng đặt tựa đề dưới 20 chữ

\*Một số nguyên tắc khi trình bày Power Point báo cáo khoa học:

1.Nên dùng font chữ không có chân và Sán Serif như Arial hay Tahoma để khan giả dễ đọc. Những font chữ có chân như Times New Roman hay Courier làm cho khan giả tốn nhiều thời gian hơn để theo dõi.

2.Nên dùng cỡ chữ từ 18 trở lên, vì chữ nhỏ hơn làm người có tuổi khó đọc, còn chữ quá lớn thì tốn nhiều không gian.

3.Tránh viết toàn bộ bằng chữ in hoa vì rất khó đọc, và gây ấn tượng là diễn giả đang la hét!

4.Nên chọn chữ tối trên nền sáng cho giảng dạy hay nói chuyện trong giảng đường nhỏ.

5.Nên chọn chứ sáng trên nền tối cho các bài báo cáo khoa học và trong các giảng đường rộng. Tránh chữ màu xanh lá cây trên nền màu đỏ vì dễ gây “ngộ độc màu” cho người theo dõi.

6.Không nên cho âm thanh chạy theo chữ. Không nên sử dụng hoạt hình quá nhiều, vì nó gây ấn tượng diễn giải là trẻ con.

7.Không nên nhồi nhét quá nhiều thông tin và hình ảnh trong một slide, vì nó giảm sự chú ý và gây lẫn lộn cho diễn giả.

8.Không nên đọc side! Đọc side gây ấn tượng “trả bài” và làm cho người nghe không có hứng thú theo dõi.

**Câu 2. Đánh giá chất lượng của một bài báo khoa học đã công bố như thế nào? Làm thế nào để biết một hội nghị/hội thảo khoa học hay tạp chí khoa học có uy tín và chất lượng?**

* Đánh giá chất lượng của một bài báo khoa học đã công bố như thế nào?

Trên bình diện quốc gia, công bố báo cáo khoa học trên các diễn đàn khoa học quốc tế là một cách không chỉ nâng cao sự hiện diện, mà còn nâng cao năng suất khoa học, của nước nhà. Ở phương Tây người ta thường đếm số lượng bài báo khoa học mà các nhà khoa học công bố trên các tập chí khoa học để đo lường và so sánh hiệu suất khoa học giữa các quốc gia. Hiện nay, trong bất cứ lĩnh vực nào, phải nhìn nhận một thực tế là hiệu suất khoa của nước ta chưa cao. Phần lớn các công trình nghiên cứu tại nước ta chỉ được kết thúc bằng những buổi nghiệm thu hay luận án. Đối với hoạt động khoa học, cho dù công trình đã được nghiệm thu hay đưa vào luận án tiến sĩ hay thạc sĩ , nếu chưa được công bố trên các diễn đàn khoa học quốc tế thì công trình đó coi như chưa hoàn tất, bởi vì nó chưa qua “thử lửa” với môi trường rộng lớn hơn.

* Làm thế nào để biết một hội nghị/hội thảo khoa học hay tạp chí khoa học có uy tín và chất lượng?

Trong nghiên cứu hàn lâm, lựa chọn tạp chí là một việc quan trọng. Thứ nhất, chúng ta cần lựa chọn tạp chí có chất lượng cao, hay ít nhất là tạp chí có chất lượng phù hợp để công bố bài báo của mình, tránh đăng trên tạp chí giả khoa học, tạp chí chất lượng thấp, nhà xuất bản nặng về thương mại. Thứ hai, khi trích dẫn, khi làm tổng quan lý thuyết chúng ta cũng cần chọn bài trên các tạp chí uy tín để đảm bảo chất lượng bài báo của mình. Trích dẫn báo ngày hay tạp chí giả khoa học sẽ là cách “tốt nhất” làm cho bài báo của chúng ta bị từ chối. Bài viết ngắn này trình bày một cách tóm tắt cách thức tìm kiếm các nguồn tài liệu có độ tin cậy cao, hữu ích cho những người làm nghiên cứu trích dẫn cũng như giới thiệu một số danh mục tạp chí có độ tin cậy để các nhà nghiên cứu xuất bản, đồng thời tránh các nhà xuất bản, tạp chí nên tránh.

Với các tác giả có dự định gửi bài tới các tạp chí quốc tế uy tín thì việc kiểm tra chất lượng, tính xác thực và xếp hạng của tạp chí mà mình gửi bài là việc rất quan trọng. Trên thế giới có nhiều hệ thống xếp hạng các tạp chí, trong đó hiện nay có hai hệ thống được coi là phổ biến, uy tín và tin cậy nhất đó là ISI và SCOPUS.

**II. BÀI TẬP TÌNH HUỐNG VÀ THỰC HÀNH**

**Câu 1: Tìm kiếm một số hội thảo quốc tế về lĩnh vực quan tâm? Xem đánh giá (ranking) về các hội thảo thuộc về lĩnh vực quan tâm.**

\*Một số hội thảo liên quan đến lĩnh vực an toàn và bảo mật thông tin năm 2016:

* Hội thảo quốc tế về đa dạng hóa dịch vụ 4G:  “**HOÀN THIỆN HẠ TẦNG KỸ THUẬT VÀ BẢO MẬT THÔNG TIN CHO MẠNG 4G LTE”**

# Hội thảo quốc tế về an toàn - an ninh thông tin và hệ thống VNSECON’07

# Hội thảo quốc tế về “Ứng dụng CNTT và Quản lý” tại Đà Nẵng: Hướng đến kỳ họp chung về chủ đề “Tương lai Châu Á”:bảo mật thông tin

# Hội thảo bảo mật quốc tế SyScan 2010

\*Đánh giá về các cuộc hội thảo:

* Hội thảo quốc tế về đa dạng hóa dịch vụ 4G:  “**HOÀN THIỆN HẠ TẦNG KỸ THUẬT VÀ BẢO MẬT THÔNG TIN CHO MẠNG 4G LTE”**

# Hội thảo quốc tế về an toàn - an ninh thông tin và hệ thống VNSECON’07

# Các nội dung kỹ thuật trình bày tại hội thảo cung cấp những thông tin thực sự hữu ích cho các nhà chuyên môn hoạt động trong lĩnh vực bảo mật, an toàn thông tin và đã thu hút được khoảng 300 khách tham dự.

# Hội thảo quốc tế về “Ứng dụng CNTT và Quản lý” tại Đà Nẵng: Hướng đến kỳ họp chung về chủ đề “Tương lai Châu Á”:bảo mật thông tin

# Hội thảo là diễn đàn thường niên của những người công tác nghiên cứu, ứng dụng, giảng dạy và quản lý trong lĩnh vực công nghệ thông tin và quản trị trao đổi học thuật, chia sẻ kinh nghiệm ứng dụng và tìm kiếm sự hợp tác, phát triển đa phương. Qua đó sẵn sàng xúc tiến hợp tác nhiều mặt dựa trên thế mạnh của từng thành viên trong đào tạo, nghiên cứu khoa học, đặc biệt là chia sẻ sáng kiến và chuyển giao công nghệ mang tính ứng dụng cao thuộc các lĩnh vực công nghệ thông tin và quản lý.

# Hội thảo bảo mật quốc tế SyScan 2010:

# Chương trình được SyScan, công ty IET và nhóm nghiên cứu bảo mật hàng đầu Việt Nam VNSECURITY phối hợp tổ chức. Khác với các hội thảo về bảo mật khác, SyScan không nói về sản phẩm hay giải pháp thương mại mà là nơi các chuyên gia chia sẻ nghiên cứu, kinh nghiệm với giới bảo mật trong khu vực. Nội dung của 2 ngày thảo luận xoay quanh các vấn đề bảo mật đang nóng bỏng hiện nay như phát hiện các tệp tin nhiễm độc, bảo mật hệ điều hành, lỗ hổng phần mềm, kiểm tra an ninh ứng dụng web…

# Kết quả: thành công và tốt đẹp

**Câu 2:Tìm kiếm một số tạp chí có uy tín trong và ngoài nước về lĩnh vực quan tâm? Trích dẫn 2 bài báo trong số các tạp chí đã nêu.**

\*Tạp chí có uy tín về lĩnh vực an toàn và bảo mật thông tin là: Tạp chí an toàn thông tin

\*Trích dẫn 2 bài báo trong số các tạp chí đã nêu:

Bài báo thứ nhất: Một số kỹ thuật kiểm tra điểm yếu về An toàn thông tin

Bài báo giới thiệu một số kĩ thuật kiểm tra, đánh giá các lỗ hổng về an toàn thông tin trong các hệ thống CNTT của tổ chức. Đây là những công đoạn cần thiết để có thể phát hiện những điểm yếu và điều chỉnh các biện pháp khắc phục kịp thời để đảm bảo hệ thống họt động an toàn.

**1.Quét mạng:**

Phương pháp quét mạng liên quan đến việc quét các cổng (port) trên hệ thống mạng để xác định các thiết bị có lỗ hổng, dễ bị tin tặc lợi dụng tấn công vào hệ thống mạng hoặc các dịch vụ chạy trên thiết bị đó. Ví dụ như: dịch vụ truyền file (FTP), dịch vụ truyền siêu văn bản (HTTP) và đặc biệt là các ứng dụng chạy một dịch vụ xác định như WU-FTPD, Internet Information Server (IIS), Apache chạy dịch vụ HTTP,.… Kết quả của phương pháp quét này là một danh sách toàn diện các máy tính đang hoạt động, các dịch vụ và các thiết bị khác trong hệ thống.  
Phương pháp quét các cổng (ví dụ công cụ nmap) sẽ xác định các máy tính đang hoạt động trên vùng địa chỉ quét. Sau đó, trên mỗi một máy tính, chương trình sẽ kiểm tra các cổng mở thuộc các giao thức TCP hoặc UDP để xác định các dịch vụ chạy trên thiết bị.  
Nội dung cơ bản của phương pháp quét là xác định các máy tính hoạt động và các cổng mở của nó. Để thực hiện tốt mục tiêu của phương pháp này, nên quét mạng theo các tiêu chí sau: Kiểm tra quyền kết nối của các máy tính trong mạng; Xác định các lỗ hổng của dịch vụ; Kiểm tra sự sai lệch của tất cả các dịch vụ so với chính sách bảo mật; Chuẩn bị cho việc kiểm tra sự xâm nhập mạng; Hỗ trợ cấu hình cho hệ thống phát hiện xâm nhập; Thu thập bằng chứng về các sự xâm nhập....  
Kết quả của quá trình quét mạng phải được lưu giữ lại để làm căn cứ khắc phục sự cố. Sau khi quét mạng cần làm một số việc: Ngắt và điều tra các kết nối không được phép; Vô hiệu hóa hoặc gỡ bỏ các dịch vụ không cần thiết hoặc có nhiều lỗ hổng bảo mật; Hạn chế quyền truy cập vào các dịch vụ có nhiều điểm yếu; Cấu hình firewall để hạn chế quyền truy cập từ bên ngoài các dịch vụ có lỗ hổng.

**2. Quét lỗ hổng bảo mật**  
Phương pháp quét lỗ hổng bảo mật thực chất là việc quét các cổng ở mức độ cao hơn. Ngoài việc xác định các máy tính hoạt động và các cổng mở, nó còn cung cấp thêm các thông tin về lỗ hổng của các máy tính đó. Phương pháp này cung cấp cho hệ thống và người quản trị mạng một công cụ để phát hiện các lỗ hổng trước khi kẻ tấn công có thể tiếp cận đến nó, bao gồm các khả năng sau: Xác định các máy tính hoạt động trên mạng; Xác định các dịch vụ (cổng) đang hoạt động trên mạng và các điểm yếu của chúng nếu có; Xác định các ứng dụng và đọc “biểu ngữ” được trả lời từ các ứng dụng; Xác định hệ điều hành; Xác định các lỗ hổng thông qua việc tìm hiểu hệ điều hành và các ứng dụng chạy trên nó; Xác định các thiết lập cấu hình sai; Kiểm tra việc tuân thủ sử dụng ứng dụng hoặc chính sách bảo mật; Thiết lập nền tảng cho việc kiểm tra sự xâm nhập.  
Kết quả của quá trình quét lỗ hổng bảo mật phải được lưu giữ lại và làm căn cứ để tiến hành khắc phục các lỗ hổng nếu có. Một số biện pháp cần phải làm ngay sau khi quét lỗ hổng là: Nâng cấp hoặc vá lỗi hệ thống để giảm thiểu các nguy cơ từ lỗ hổng; Triển khai các biện pháp giảm nhẹ nguy cơ nếu như hệ thống chưa được vá lỗi; Cấu hình và nâng cấp thường xuyên chương trình quản lý; Giám sát và cảnh báo về lỗ hổng, thay đổi cấu hình hệ thống để giảm thiểu nguy cơ; Thay đổi các chính sách bảo mật, kiến trúc hệ thống hoặc các tài liệu khác để đảm bảo hoạt động ổn định cho hệ thống.

**3. Phá mật khẩu**  
Chương trình phá mật khẩu được sử dụng để xác định các mật khẩu yếu. Mật khẩu được lưu trữ và truyền đi dưới dạng mã hóa “băm”. Khi người dùng đăng nhập vào hệ thống, hệ thống sẽ tạo ra dãy mã hóa băm từ mật khẩu đăng nhập và so sánh với dãy mã hóa băm đã được lưu. Nếu chúng trùng nhau tức là người dùng đã được xác thực.  
Trong suốt quá trình thâm nhập hoặc tấn công, việc phá mật khẩu đòi hỏi phải lấy được dãy mã hóa băm của mật khẩu. Việc chặn bắt này xảy ra khi dãy mã hóa của mật khẩu truyền đi trên mạng hoặc được lấy từ hệ thống mục tiêu. Khi đã lấy được dãy băm của mật khẩu, chương trình sẽ nhanh chóng tạo ra các dãy băm cho đến khi trùng với dãy băm của mật khẩu đã nhận được. Phương pháp nhanh nhất của cách này là sử dụng bộ từ điển tấn công gồm rất nhiều từ phổ biến trên thế giới.  
Phương pháp mạnh nhất để phá mật khẩu là chương trình “tấn công tổng lực”, tức là chương trình sẽ tấn công tất cả các mật khẩu có thể có.  
Sau đây là một số phương pháp có thể sử dụng để giảm thiểu khả năng phá mật khẩu của kẻ tấn công:  
- Thay đổi chính sách để giảm tỉ lệ mật khẩu bị phá hoặc thay thế phương pháp xác thực (ví dụ sử dụng token key).  
- Phổ biến với người sử dụng về những tác hại của mật khẩu yếu. Nếu người dùng vẫn sử dụng mật khẩu yếu thì người quản trị nên áp dụng các biện pháp bổ sung để đảm bảo.

**4. Kiểm tra file log**  
Các file log trên hệ thống bao gồm firewall log, IDS log, server log hoặc bất kỳ một file nào ghi lại quá trình kiểm tra dữ liệu trên hệ thống. Việc kiểm tra các file log và phân tích chúng sẽ cho biết các hoạt động đang diễn ra trên hệ thống, để có thể so sánh với mục đích và nội dung của chính sách bảo mật. Vì thế, việc kiểm tra này sẽ xác định hệ thống có vận hành theo đúng chính sách bảo mật hay không.  
Ví dụ, khi ta đặt một hệ thống phát hiện xâm nhập (IDS) đằng sau tường lửa thì file log của nó sẽ được sử dụng để kiểm tra các yêu cầu dịch vụ và các giao dịch được tường lửa cấp phép. Nếu như trên file log của IDS này ghi lại các hoạt động không được phép, điều đó chứng tỏ tường lửa đã bị vượt qua và hệ thống mạng đã mất an toàn.  
Nên định kỳ cho việc kiểm tra file log, trừ những trường hợp yêu cầu kiểm tra do việc nâng cấp hệ thống. Nếu hệ thống không được cấu hình theo đúng chính sách bảo mật thì có thể thực hiện những việc sau: Gỡ bỏ các dịch vụ có lỗ hổng nếu chúng không cần thiết; Cấu hình lại hệ thống; Thay đổi chính sách bảo mật của tường lửa để hạn chế quyền truy cập vào các hệ thống hoặc dịch vụ có lỗ hổng.

**5. Kiểm tra sự toàn vẹn**  
Kiểm tra sự toàn vẹn của một file là tạo và lưu trữ một biến phát hiện lỗi checksum cho mọi file được bảo vệ và thiết lập một cơ sở dữ liệu của biến checksum đó. Phương pháp này cung cấp một công cụ cho quản trị hệ thống nhận ra sự thay đổi của các file, đặc biệt là sự thay đổi trái phép. Các biến checksum lưu trữ nên được tính toán lại thường xuyên để so sánh với giá trị hiện tại được lưu trữ, sau đó xác định có sự thay đổi file hay không. Chức năng kiểm tra sự toàn vẹn của file thường được tích hợp vào trong hệ thống phát hiện xâm nhập trên máy chủ thương mại.  
Phương pháp kiểm tra sự toàn vẹn là một công cụ hữu ích mà không đòi hỏi sự can thiệp của con người ở mức độ cao, nhưng nó cần phải thực hiện một cách thận trọng để đảm bảo tính hiệu quả.  
Một số công cụ kiểm tra sự toàn vẹn của dữ liệu như Aide, LANGuard, Tripwire,....

**6. Phát hiện virus**  
Mọi hệ thống mạng đều có nguy cơ nhiễm virus, trojan, sâu nếu như chúng kết nối với mạng Internet hoặc sử dụng USB, phần mềm miễn phí.  
Có hai dạng chương trình diệt virus chính là chương trình được cài đặt trên hạ tầng mạng và chương trình cài đặt trên máy người sử dụng. Mỗi loại có những ưu điểm và nhược điểm riêng, nhưng với những hệ thống yêu cầu bảo mật cao thì nên sử dụng cả hai loại chương trình diệt virus đó.

**7. Kiểm tra mạng không dây**  
Giao thức mạng không dây phổ biến nhất là 802.11b có nhiều lỗi nghiêm trọng khi sử dụng công cụ mã hóa WEP, bởi vì ở chế độ mặc định nó được cấu hình không an toàn.  
Mỗi một hệ thống mạng không dây nên được kiểm tra định kỳ để tìm ra các kết nối trái phép hoặc các cấu hình yếu, đồng thời cũng phải kiểm tra các tín hiệu của mạng không dây lân cận. Một số phần mềm kiểm tra sự an toàn của hệ thống mạng không dây như Aerosol, AirSnort, Kismet, Sniffer Wireless,....  
**8. Thâm nhập thử nghiệm**  
Đây là việc kiểm tra an toàn của hệ thống bằng cách phá vỡ các tính năng an toàn của chúng dựa trên các hiểu biết về thiết kế và hoạt động của hệ thống. Mục đích là để xác định các phương pháp tiếp cận hệ thống thông qua các công cụ và kỹ thuật cơ bản của kẻ tấn công. Việc thâm nhập phải được tiến hành sau khi khảo sát hệ thống một cách cẩn thận, thông báo cho toàn hệ thống và lập kế hoạch thâm nhập đầy đủ.  
Việc thử nghiệm thâm nhập chính là tạo ra một mô phỏng cuộc tấn công vào hệ thống, nên có thể bị pháp luật hoặc chính sách bảo mật ngăn cấm. Do đó, trước khi thực hiện phải được sự cho phép và chỉ nên thực hiện như sau: Thực hiện trên một địa chỉ hoặc một dải địa chỉ cụ thể; Không thực hiện trên một số máy tính bị ngăn cấm; Dùng một số các kỹ thuật thâm nhập cho phép; Xác định rõ thời gian thực hiện việc thâm nhập; Xác định khoảng thời gian hữu hạn cho việc thâm nhập; Xác định rõ địa chỉ IP từ máy sẽ thực hiện thâm nhập để người quản trị có thể phân biệt cuộc tấn công thử nghiệm với các cuộc tấn công thực sự khác; Xử lý các thông tin được thu thập bởi đội thử nghiệm thâm nhập.

**Kết luận**  
Như vậy, việc kiểm tra an toàn của hệ thống thông tin chính là hoạt động tìm kiếm các lỗ hổng bảo mật sau đó khắc phục các điểm yếu đó. Thông thường, nhiều phương pháp kiểm tra sẽ được kết hợp cùng lúc để đánh giá một cách toàn diện về tình trạng bảo đảm an toàn của mạng. Ví dụ, để kiểm tra sự thâm nhập mạng thì kết hợp việc quét mạng và quét lỗ hổng để xác định các máy tính dễ bị tấn công và các dịch vụ có thể là mục tiêu của sự tấn công sau này. Một số phương pháp quét lỗ hổng bảo mật lại cần đi kèm với phương pháp phá mật khẩu và không một phương pháp nào có thể cung cấp một bức tranh toàn diện về mạng và tình trạng bảo mật của chúng.

**KS. Phạm Thành Công (Biên dịch) Theo “Computer Security - Guideline on Network Security Testing” của John Wack, Miles Tracy**

Bài báo thứ hai: Xây dựng hệ thống bảo vệ thông tin

**An toàn thông tin (ATTT) là điều kiện tiên quyết để các hệ thống thông tin vận hành tin cậy và hiệu quả. ATTT được đảm bảo bởi việc triển khai đồng bộ các giải pháp tổ chức, quản lý và kỹ thuật, liên kết với nhau thành một hệ thống thống nhất nhằm đáp ứng các yêu cầu nhất định về bảo vệ thông tin - hệ thống đó được gọi là hệ thống đảm bảo ATTT hay hệ thống bảo vệ thông tin (BVTT).**

Kỹ thuật bảo vệ thông tin luôn luôn thay đổi theo trình độ phát triển của kỹ thuật thông tin. Ngày nay, sự phát triển nhanh chóng của công nghệ, kéo theo sự đa dạng và khó dự đoán của các mối nguy cơ an toàn làm cho bài toán xây dựng hệ thống BVTT đã trở nên hết sức phức tạp. Mặc dù phần lớn các chuyên gia đều cho rằng một hệ thống BVTT an toàn tuyệt đối là không hề tồn tại, song trong lĩnh vực này người ta đã đạt được những thành tựu to lớn cả trên bình diện lý thuyết cũng như thực tiễn. Bên cạnh việc thiết kê, sản xuất các thiết bị kỹ thuật phục vụ nhu cầu đảm bảo an toàn cho các thành phần của hệ thống thông tin, các tổ chức quốc tế và của các quốc gia, các hãng sản xuất đã ban hành tài liệu hướng dẫn trong lĩnh vực xây dựng và quản lý ATTT. Nhiều tài liệu trong đó đã được nghiên cứu, đề xuất ban hành thành Tiêu chuẩn Việt Nam, giúp định hướng trong việc giải quyết nhiều vấn đề của hệ thống BVTT.  
Bài báo giới thiệu một số vấn đề cốt lõi trong xây dựng và thiết kế hệ thống BVTT, bao gồm các giai đoạn sau: Xây dựng các nguyên tắc thiết kế và các yêu cầu đối với hệ thống BVTT; Khảo sát hệ thống thông tin cần bảo vệ, từ đó xác định mục tiêu, chính sách và mô hình hệ thống BVTT; Thiết kế hệ thống BVTT theo mô hình đã chọn; Tổ chức triển khai hệ thống đảm BVTT.  
**1. Các nguyên tắc cơ bản trong xây dựng và thiết kế hệ thống BVTT**  
Trong quá trình xây dựng và thiết kế hệ thống BVTT, cần tuân thủ các nguyên tắc cơ bản sau:  
- Thường xuyên hoàn thiện và phát triển hệ thống đảm bảo ATTT. Mục tiêu của hệ thống này là chống lại các tấn công từ bên ngoài và cả bên trong hệ thống thông tin. Thực tế cho thấy cùng với sự phát triển công nghệ và đội ngũ hacker, các kiểu tấn công ngày càng tinh vi, không ít trong số đó dễ dàng lọt qua các hệ thống thông tin không được bảo vệ đầy đủ. Do đó phải thường xuyên giám sát sự vận hành của hệ thống, phát hiện các điểm yếu, các kênh rò rỉ thông tin và các kiểu xâm nhập trái phép mới, hoàn thiện các cơ chế và phương pháp bảo vệ tùy thuộc vào đặc tính của các kiểu tấn công và các mối đe dọa mới. Để đảm bảo nguyên tắc này, hệ thống BVTT phải được thiết kế mềmdẻo, có khả năng tích hợp các phương tiện mới.  
- Đảm bảo tính hệ thống và tổng thể trong việc sử dụng các phương tiện đảm bảo ATTT. Những kẻ xâm nhập bất hợp pháp vào hệ thống để khai thác và phá hoại thông tin thường sử dụng mọi phương tiện và dựa vào sơ hở của hệ thống, kể cả việc lợi dụng yếu tố con người. Vì vậy các phương tiện đảm bảo ATTT phải đồng bộ và được kết hợp lại thành một thể thống nhất. Hệ thống này là tập hợp các giải pháp về tổ chức -  quản trị và các giải pháp kỹ thuật. Trong đó, bên cạnh các giải pháp kỹ thuật, các giải pháp về tổ chức -  quản trị hệ thống có vai trò đặc biệt. Đó là quá trình đảm bảo kiểm soát an toàn sự vận hành của hệ thống, bố trí  nguồn nhân lực chuyên trách một cách phù hợp, xây dựng chính sách an toàn và các quy định về vận hành hệ thống, sử dụng hợp lý các nguồn tài nguyên thông tin, các máy chủ, máy trạm; những quy định này xác định yêu cầu cụ thể đảm bảo an toàn cho các thành  phần của hạ tầng thông tin,  mô tả các phương tiện và biện pháp thực hiện các yêu cầu được đặt ra trong chính sách ATTT và kiểm tra việc thực hiện chúng.  
- Hệ thống BVTT cần được tổ chức thành nhiều lớp. Việc bảo vệ hệ thống thông tin, nhất là những  hệ thống phức tạp, thường được so sánh như bảo vệ các mục tiêu quân sự, cần được tổ chức thành nhiều lớp, nhiều tuyến. Có ít nhất bốn lớp cần được bảo vệ là: lớp ngoài bao quát toàn bộ lãnh thổ hệ thống, trên đó bố trí các trang bị của hệ thống thông tin; lớp thứ hai gồm các phòng làm việc và các trang bị của hệ thống; lớp thứ ba là các bộ phận cấu thành của hệ thống (các phương tiện kỹ thuật, các chương trình, các hệ CSDL) và lớp thứ tư bao gồm các quá trình xử lý thông tin. Nguyên tắc nhiều lớp không chỉ dựa trên phương pháp ngăn chặn, từng bước làm suy yếu tấn công của đối phương mà còn vì sự đa dạng của các nhiệm vụ đảm bảo thông tin.  
- Đảm bảo nguyên tắc tập trung. Công tác đảm bảo ATTT là hoạt động có điều khiển, cần được quản lý thống nhất và vì vậy phải vận hành trên nguyên tắc tập trung. Nguyên tắc này cho phép bám sát được các mục tiêu chung và tập trung được nguồn lực và phương tiện kỹ thuật để thực hiện các nhiệm vụ an toàn đặt ra.  
- Đảm bảo tính trong suốt đối với hạ tầng thông tin. Nguyên tắc này trước hết đòi hỏi hệ thống BVTT phải đơn giản trong cách sử dụng. Điều này có nghĩa là việc sử dụng hệ thống BVTT không nhất thiết đòi hỏi người sử dụng phải hiểu biết nhiều và phải thực hiện nhiều động tác phức tạp. Ngoài ra, hệ thống BVTT cần được xây dựng và thiết kế sao cho không gây ra cản trở hoặc giảm hiệu quả họat động của hệ thống thông tin. Đây là một vấn đề không đơn giản. Để minh họa, chúng ta có thể xem xét bài toán bảo mật hệ quản trị CSDL. Trong một thời điểm có thể có một số lượng lớn người dùng truy cập và khai thác CSDL, do đó bài toán bảo mật CSDL phải đươc giải quyết sao cho một mặt vẫn đảm bảo cho phép một số người dùng khai thác các dữ liệu mật mà không làm ảnh hưởng đến các hoạt động của những người dùng còn lại trong cùng thời điểm. Mặt khác, việc mã hóa dữ liệu thông qua các thuật toán mật mã làm tăng đáng kể kích cỡ dữ liệu, và do CSDL chứa một khối lượng lớn dữ liệu nên việc mã hóa CSDL dẫn đến ảnh hưởng lớn lên tốc độ và hiệu quả của CSDL. Như vậy bảo mật CSDL phải đạt được một giải pháp tối ưu để không ảnh hưởng đến hoạt động của hệ thống, nói cách khác giải pháp này phải là trong suốt đối với hệ thống.  
- Nguyên tắc hiệu quả kinh tế. Theo nguyên tắc này, việc xây dựng hệ thống BVTT cần tính đến hiệu quả kinh tế, do đó cần tuân thủ nguyên tắc cân bằng giữa mức độ bảo vệ và kinh phí đầu tư. Nói chung, kinh phí đầu tư không thể vượt quá thiệt hại do các nguy cơ an toàn thông tin đưa lại.  
**2. Khảo sát hiện trạng an toàn của hệ thống thông tin**  
Hoạt động khảo sát phải được tiến hành tổng thể, toàn diện đối với tất cả các quá trình hoạt động trên hệ thống thông tin cũng như các phương tiện đảm bảo ATTT hiện có, không chỉ bao gồm các phương tiện kỹ thuật an toàn đang được áp dụng mà cả các biện pháp tổ chức -  quản trị như: tình hình xây dựng chính sách an toàn, việc thực hiện các quy định về an toàn, việc tổ chức hệ thống sao lưu dự trữ, việc phân cấp độ mật dữ liệu, sự phân quyền, phân cấp người dùng và nhiều vấn đề khác. Khảo sát sẽ cho phép đánh giá xem mức độ an toàn của các tài nguyên CNTT có phù hợp với các yêu cầu đặt ra hay không, nghĩa là có đảm bảo các yếu tố bảo mật, tính toàn vẹn và tính sẵn sàng của dữ liệu hay không. Trong quá trình khảo sát cần phân tích các mối nguy cơ đe dọa an toàn hệ thống thông tin, các điểm yếu của hệ thống và các rủi ro có thể.  
Việc khảo sát hiện trạng an toàn của hệ thống thông tin gồm ba bước:  
-  Thu thập dữ liệu và mô tả hiện trạng của hệ thống thông tin.  
- Đánh giá hiện trạng an toàn của hệ thống. Việc đánh giá phải trên cơ sở một hệ thống tiêu chí an toàn. Ở giai đoạn này nếu hệ tiêu chí như thế chưa được xây dựng thì có thể tham khảo các tiêu chuẩn quốc tế, quốc gia tiên tiến (như ISO 17799, ISO 1335, ISO 15408, NIST 800- 35) hoặc của các nhà cung cấp giải pháp uy tín trong lĩnh vực ATTT.  
- Xây dựng các khuyến cáo về việc tổ chức BVTT.  
Kết quả của quá trình khảo sát là bản báo cáo chi tiết cho các nhà lãnh đạo và quản lý của tổ chức về hiện trạng an toàn thông tin của hệ thống hiện hành, những thay đổi hoặc bổ sung hạ tầng của hệ thống thông tin và danh mục dự kiến các biện pháp về đảm bảo ATTT sẽ được tiến hành.  
**3. Thiết kế và xây dựng hệ thống BVTT**  
Thiết kế hệ thống thông tin bao gồm các nội dung sau:  
-  Xác định các mục tiêu, các yêu cầu đối với ATTT và từ đó xác định các nhiệm vụ đảm bảo ATTT; Xác định các phương pháp tiếp cận giải quyết các nhiệm vụ ATTT đặt ra.  
-  Xây dựng mô hình hệ thống ATTT bao gồm kiến trúc hệ thống, các giải pháp kỹ thuật và hệ thống tổ chức, quản lý hệ thống ATTT  
-  Lập dự án kỹ thuật xây dựng hệ thống ATTT. Ngoài việc xác định mục tiêu, các nguyên tắc, các yêu cầu đối với hệ thống ATTT, dự án cần nêu rõ các luận cứ cho các giải pháp kỹ thuật và tổ chức được lựa chọn, xác định tổ hợp các thiết bị kỹ thuật, các chương trình phần mềm.  
-  Xây dựng chính sách ATTT và kế hoạch huấn luyện khai thác sử dụng hệ thống ATTT.  
Cốt lõi của xây dựng hệ thống BVTT là kiến trúc hệ thống, bao gồm: Cấu trúc  hệ thống ATTT và Hệ thống quản lý ATTT.  
Kiến trúc hệ thống ATTT về cơ bản được xây dựng trên phương pháp phân hoạch hệ thống thành các tiểu hệ thống (hệ thống con). Việc phân hoạch phụ thuộc vào bối cảnh do mục tiêu an toàn đặt ra mà hệ thống thông tin cụ thể đòi hỏi. Ví dụ phân hoạch hệ thống BVTT thành các tiểu hệ thống như sau: Tiểu hệ thống bảo vệ chống virus; Tiểu hệ thống sao dự phòng và khôi phục dữ liệu; Tiểu hệ thống bảo vệ thư điện tử; Tiểu hệ thống phát hiện tấn công và phản ứng tự động; Tiểu hệ thống quản lý ATTT, giám sát tập trung và kiểm soát sự kiện; Tiểu hệ thống bảo vệ kênh truyền dữ liệu (VPN); Tiểu hệ thống xác thực và định danh; Tiểu hệ thống đăng ký và kiểm kê; Tiểu hệ thống đảm bảo tính toàn vẹn.  
Mỗi tiểu hệ thống có thể là một hệ thống phức tạp, thực hiện nhiều chức năng khác nhau. Việc phân hoạch hệ thống thành các tiểu hệ thống không chỉ cho phép hạ giá thành tổng thể của hệ thống, tăng cường hiệu quả đầu tư mà còn tăng cường chất lượng và hiệu quả của công tác quản lý ATTT.  
Hệ thống quản lý ATTT như một thành phần của kiến trúc hệ thống BVTT bao gồm các quá trình và các thủ tục đảm bảo ATTT. Hệ thống này cũng xác định mối tương quan giữa các quá trình và các tiểu hệ thống, xác định nguồn nhân lực và tài chính đảm bảo cho việc thực hiện các quá trình và các tiểu hệ thống đo  
Ngoài ra, hệ thống quản lý ATTT chịu trách nhiệm về lập kế hoạch, tổ chức thực hiện, kiểm soát và dịch vụ kỹ thuật cho toàn bộ hạ tầng thông tin. Hệ thống quản lý ATTT còn cho phép đưa vào hệ thống ATTT các sửa đổi và bổ sung, cho phép quản lý hiệu quả hệ thống trong những tình huống đặc biệt.  
Sau khi hoàn thành giai đoạn thiết kế, cần tiến hành thẩm định chất lượng thiết kế. Tiếp đó có thể chuyển sang việc triển khai hệ thống theo thiết kế đã lựa chọn với các nội dung: cung cấp các phương tiện phầm mềm và phần cứng; cài đặt các bộ phận chương trình; xây dựng các tiểu  hệ thống; thử nghiệm; triển khai hệ thống quản lý; huấn luyện sử dụng; xây dựng chính sách an toàn.  
Cần chú trọng đặc biệt việc xây dựng chính sách an toàn trong quá trình xây dựng hệ thống BVTT, bởi nếu thiếu yếu tố này thì không một hệ thống nào được bảo vệ hiệu quả.  
**4. Xây dựng và triển khai hệ thống BVTT**  
Hệ thống BVTT được triển khai hiệu quả trên thực tế chỉ khi chúng đáp ứng các yêu cầu sau:  
- Hệ thống được xây dựng đảm bảo chất lượng.  
-  Hệ thống sau khi triển khai được tổ chức tiếp nhận và sử dụng trên thực tế.  
Chất lượng xây dựng hệ thống BVTT không chỉ phụ thuộc vào chất lượng thiết kế mà còn phụ thuộc đáng kể vào quá trình triển khai sau đó, đặc biệt là việc cung cấp các trang thiết bị bảo vệ thông tin. Đối với những quốc gia mà hệ thống thông tin còn phụ thuộc chủ yếu vào thiết bị  nhập ngoại thì độ an toàn của hệ thống BVTT sẽ phụ thuộc rất lớn vào việc thực hiện chặt chẽ quy trình đảm  bảo an toàn trong cung cấp thiết bị. Bởi vậy, một yếu tố hết sức quan trọng là các thiết bị (phần cứng, phần mềm) nhất định phải được các đối tác tin cậy cung cấp và phải được chứng nhận về chất lượng bởi các tổ chức có uy tín trong và ngoài nước. Tại nhiều quốc gia, các thành phần của hệ thống tin trong các cơ quan nhà nước trước khi đưa vào sử dụng được kiểm tra kỹ, rà soát các loại rệp điện tử, các chương trình Trojan mà có thể được cài đặt để đánh cắp hoặc phá hoại thông tin hoặc chuẩn bị sẵn cho chiến tranh thông tin.  
Một nguyên tắc khác đảm bảo chất lượng cho quá trình thiết kế và triển khai hệ thống BVTT là chúng phải được thiết kế bởi đội ngũ chuyên gia trình độ cao trong lĩnh vực này. Rõ ràng phần lớn các tổ chức và doanh nghiệp ở Việt Nam phải cần đến tư vấn hoặc thuê thiết kế từ ngoài. Như vậy nảy sinh vấn đề lựa chọn đối tác thực hiện. Đối tác tin cậy chỉ có thể là những tổ chức đã có uy tín và nhiều kinh nghiệm trong lĩnh vực này.  
Hệ thống BVTT sau khi triển khai sẽ được tổ chức tiếp nhận và sử dụng khi chúng được thiết kế tiện dụng với quá trình vận hành hệ thống thông tin, nói cách khác là đảm bảo nguyên tắc trong suốt với người dùng. Tuy nhiên, thuật ngữ này cũng cần được hiểu một cách tương đối. Chẳng hạn, khi áp dụng các phương pháp mật mã để bảo mật các hệ CSDL thì dù kỹ thuật hoàn thiện đến đâu cũng sẽ ảnh hưởng đến tốc độ hoạt động của hệ thống và phát sinh một số thao tác mà người sử dụng bắt buộc phải thực hiện.

Và cuối cùng, muốn duy trì hoạt động hiệu quả lâu dài của hệ thống BVTT thì tổ chức sử dụng cần nhận thức rằng BVTT là một quá trình liên tục, thường xuyên. Hệ thống thông tin chỉ có thể bảo vệ hiệu quả khi sử dụng đồng bộ các phương tiện, và không một hệ thống nào có thể bảo vệ được nếu con người thiếu ý thức về bảo vệ thông tin. Đây phải là mối quan tâm hàng đầu của lãnh đạo và đội ngũ nhân viên của tổ chức

**TS. Trần Đức Lịch**

**Câu 3: Tìm và trình bày 2 tài liệu được xem là vi phạm đạo đức và văn hóa trong nghiên cứu khoa học?**

**Trích : Tác giả Nguyễn Tuấn**

**1.Woo Suk Hwang: Ngụy tạo dữliệu**

Tháng 2.2004, một nhóm nhà khoa họcHàn Quốc đã công bố một NCKH được xemlà tiên phong trong việc sử dụng tế bàomầm (stem cells) vào các mục tiêu điều trị lâm sàng. Nhóm khoa học do GS HwangWoo Suk, một nhà nghiên cứu thú y danh tiếng ở Hàn Quốc đứng đầu, tuyên bố trênTạp chí Science rằng, họ đã thành công sản sinh một số tuyến tế bào mầm(embryonic stem cell lines) bằng cách cấy các nhân (nucleus) rút ra các tế bàocủa người lớn vào trứng của một người khác. 4 tháng sau, GS Hwang tuyên bố thêm rằng nhóm của ông đã tiến hành chuyển nhân như thế cho 11 bệnh nhân khác. Thành công vượt bậc này được giới khoa học khắp thế giới ca ngợi như là một kỳ tích,là bước đầu quan trọng trong mục tiêu điều trị bệnh nhân bằng chính mô của bệnh nhân được tái sinh bằng kỹ thuật cấy tế bào mầm.

Tháng 8.2005, nhóm của GS Hwang làm thế giới ngạc nhiên nữa: Đã thành công trong việc nhân bản một con chó mà ôngđặt tên là “Snuppy” (ghép từ chữ cái củaSeoulNationalUniversityvà puppy). Công trình này được công bố trên Tạp chí Nature. Đây cũng là một thành công nổi bật, theo sau thànhcông của công trình tạo con cừu Dolly nổi tiếng vài năm trước đó ở Scotland, mộtcông trình xứng đáng là niềm tự hào của khoa học Á châu. Giới khoa học thế giới làm việc trong cùng lĩnh vực cũng nghiêng mình bái phục khả năng chuyên môn của ông, vì ông và cộng sự đã làm được một việc mà họ chưa làm được. Thế nhưng, ngaysau khi công bố trên Tạp chí Science, công trình nghiên cứu của GS Hwang đã bị nhiều nhà khoa học Hàn Quốc phê bình và chỉ trích gay gắt. Chỉ 2 tháng sau khi công trình của GS Hwang công bố, một số nhà khoa học Hàn Quốc phát biểu nặc danh trên các websites ở Hàn Quốc chỉ ra rằng, một số hình ảnh trong bài báo trênScience là ngụy tạo, chứ không phải là kết quả nghiên cứu. Họ còn suy luận rằng các ảnh này được “sản xuất” từ hai cụm tế bào mà thôi (chứ không phải 11 như bài báo viết). 3 tháng sau công bố bài báo trên Science, Tạp chí Nature chạy một bảntin ngắn cho biết hai nhà nghiên cứu và cũng là cộng sự viên của Hwang là hai trong số những người hiến trứng cho công trình nghiên cứu của GS Hwang. Họ còn nói thêm rằng, họ được trả khoảng 1.500 USD cho việc hiến trứng này. Nói cách khác, đây là một vi phạm y đức trong nghiên cứu rất nghiêm trọng, vì luật pháp không cho phép cộng sự viên hiến trứng cho nghiên cứu.

Tiếp theo đó, một thành viên trong nhóm nghiên cứu của GS Hwang, TS Kim Sun Jong (hiện đang làm việc tại Đại họcPittsburgh) cho biết, trong lúc tham gia vào công trình nghiên cứu, GS Hwang đã chỉ thị cho ông phải làm sao dùng 2 hay 3 tuyến tế bào để sản xuất cho được 11tuyến. Nói cách khác, đây là một ngụy tạo dữ kiện nghiên cứu.

**2.Gerald Schatten: Vấn đề đứng tên tácgiả**

Giữa tháng 11.2005, GS GeraldSchatten thuộc Đại học Pittsburgh (Mỹ) và cũng là một cộng tác viên với nhóm củaGS Hwang tuyên bố rằng, ông đã chấm dứt tất cả cộng tác với GS Hwang vì ông quan tâm đến vấn đề y đức trong nghiên cứu của GS Hwang.Qua tiết lộ của GS Schatten,người ta còn biết thêm một tình tiết bất bình thường khác: Đó là vấn đề tácgiả.Bài báo có 25 tác giả đứng tên, trong đó có GS Schatten thuộc Đại họcPittsburgh.GSSchatten cho biết, chẳng hiểu vì lý do gì, trước khi công bố công trình nghiêncứu, ông được GS Hwang mời cùng đứng tên đồng tác giả chính (senior co-author)của bài báo, và GS Schatten đồng ý! Nhưng đến giữa tháng 12.2005, GS Schattenyêu cầu Science bỏ tên ông ra khỏi bài báo vì hai lý do: Một, ông cảm thấy không“thoải mái” với những dữ kiện trong bài báo; và hai, ông chỉ đóng vai trò phântích số liệu và giúp đỡ trong việc soạn thảo bài báo.

Về phía GS Hwang, trước hàng loạt cáobuộc bất lợi như trên, thoạt đầu ông khẳng định rằng ông chẳng làm gì sai, và quyết tâm sẽ điều tra vấn đề cho đến nơi đến chốn. Nhưng đến cuối tháng 11, đầutháng 12.2005 (tức gần 2 năm sau khi công bố bài báo trên Science) ông thú nhậnlà một số ảnh trong bài báo là bản sao chứ không phải chụp từ thí nghiệm; là nhóm của ông quả có sử dụng trứng do cộng sự viên hiến, và một số trứng khác làdo mua từ bệnh viện; một số số liệu trong bảng thống kê trong bài báo là sai.Phát biểu trước báo chí Hàn Quốc, ông nói: “Tôi cảm thấy rất hối tiếc phải nói ra những điều xấu hổ và tồi tệ trước công chúng.Một lần nữa, tôi thành thật xin lỗi vì đã làm cho quốc gia và thế giới quan tâm”. ông từ chức GS Đại học QuốcgiaSeoul, từ chức Giám đốc Trung tâm nghiên cứu tế bào mầm. Ngày 18.12.2005, Tổng biên tập Science là Donald Kennedy nhận được thư của GS Hwang và GS Schatten đề nghị rút lại bài báo trên Science. Thế là công trình nghiên cứu đã đi đến một đoạn kết buồn, một xì-căng-đan lớn trong khoa học, một vết nhơ cho khoahọc.