

ENSURING INFORMATION SECURITY FOR FACULTY, STAFF, AND STUDENTS IN UNIVERSITIES

ĐẢM BẢO AN TOÀN THÔNG TIN CHO CÁN BỘ, GIẢNG VIÊN, SINH VIÊN TRONG TRƯỜNG ĐẠI HỌC

Đậu Mạnh Hoàn

Trường Đại học Quảng Bình

ABSTRACT: The digital transformation is rapidly advancing in the field of education, particularly in higher education. Universities are progressively developing their digital learning environments to meet the demands of education and training in the new era. Alongside this transformation, enhancing digital competencies among faculty members, staff, and students plays a crucial role in determining the success of digital education. This study explores key issues related to information security in digital higher education environments. Based on this analysis, the study proposes solutions to strengthen information security capabilities within the digital transformation process, ensuring the effective use of digital services and improving digital competencies for all stakeholders involved in higher education.

Key words: Information security, digital skills, information security capacity.

TÓM TẮT: Công cuộc chuyển đổi số đang diễn ra một cách mạnh mẽ trong hoạt động giáo dục, đặc biệt là giáo dục đại học. Các trường đại học đang dần hoàn thiện môi trường giáo dục số của mình để đáp ứng hoạt động giáo dục đào tạo trong thời kỳ mới. Đi cùng với công cuộc chuyển đổi số đó thì vấn đề nâng cao năng lực số cho cán bộ, giảng viên, sinh viên trong trường đại học đóng vai trò quan trọng và quyết định đến kết quả của giáo dục số. Trong bài viết này, tác giả đề cập đến các vấn đề đảm bảo an toàn thông tin trong môi trường giáo dục đại học số, từ đó đề xuất giải pháp nâng cao năng lực an toàn thông tin trong quy trình chuyển đổi số, khai thác, sử dụng các dịch vụ số nhằm nâng cao năng lực số cho các đối tượng tham gia vào hoạt động giáo dục đại học số hiện nay.

Từ khóa: An toàn thông tin, chuyển đổi số trong giáo dục, năng lực an toàn thông tin.

1. ĐẶT VẤN ĐỀ

Trong thời gian qua việc ứng dụng các thành tựu của công nghệ thông tin vào giáo dục bước đầu đã có những thành tựu đáng kể, đồng thời đã tác động đến các tổ chức giáo dục làm chuyển biến, thay đổi trong hình thức, phương pháp giảng dạy, học tập cũng như quản lý. Việc ứng dụng công nghệ và các thiết bị hiện đại đã giúp cho việc giảng dạy, học tập, nghiên cứu khoa học hiệu quả hơn. Hiện nay, công cuộc chuyển đổi số đã trở thành nhu cầu không thể thiếu

của các trường học, chuyển đổi số trở thành xu thế tất yếu, là cơ hội và cũng là thách thức cho giáo dục nói chung và giáo dục đại học nói riêng.

Chuyển đổi số sẽ tạo nên hệ sinh thái giáo dục đại học số với những nền tảng số sẽ được ứng dụng rộng rãi trong trường đại học, điều này đặt ra yêu cầu đối với những người thực hiện chuyển đổi số cũng như những người khai thác sử dụng trong môi trường số đó. Các đối tượng này phải có các năng lực số để có thể xây dựng, khai thác

trong dạy học cũng như làm việc trong môi trường giáo dục số hiện nay. Đây là cơ hội thay đổi và cũng là thách thức cho các nhà quản lý giáo dục trong việc hỗ trợ và trang bị các kỹ năng, hình thành năng lực số cho nguồn nhân lực để từ đó cải thiện kết quả làm việc và học tập, nâng cao hiệu quả giáo dục cho xã hội.

Năng lực số là một trong những yếu tố quan trọng hàng đầu đối với mỗi người khi làm việc trên môi trường số. Việc nắm vững các kỹ năng số sẽ giúp cán bộ, giảng viên, sinh viên tham gia hoạt động số đạt được kết quả cao trong công việc của mình. Có thể nói trong các kỹ năng số để hình thành năng lực số của mỗi người thì kỹ năng an toàn thông tin đóng vai trò vô cùng quan trọng và ảnh hưởng đến các kỹ năng khác và quyết định kết quả của các công việc trên môi trường số.

Trong bối cảnh chuyển đổi số giáo dục đại học hiện nay, với sự phát triển mạnh mẽ của công nghệ và Internet, an toàn thông tin đóng vai trò then chốt, quyết định sự thành công của quá trình chuyển đổi. Bởi vì dữ liệu và thông tin là tài nguyên vô giá, trong khi đó khi tham gia trên môi trường số thì toàn bộ dữ liệu của các tổ chức, cá nhân sẽ luôn được cập nhật trên môi trường mạng internet. Các nguy cơ gây mất an toàn thông tin cho cá nhân cũng như các tổ chức có thể xảy ra bất cứ khi nào, điều này đã đặt ra các câu hỏi cho nhà quản lý cần phải giải quyết trong quá trình chuyển đổi số hiện nay.

Ở nước ta, để đảm bảo an toàn thông tin trên không gian mạng, ngày 12/6/2018, Chính phủ đã ban hành Luật An ninh mạng, trong đó xác định hệ thống thông tin quan trọng về an ninh quốc gia bao gồm tám nội dung cốt lõi nhằm đảm bảo an toàn thông tin cho quốc gia. Vấn đề an toàn thông tin

cũng được Ban chấp hành Trung ương Đảng chỉ ra trong Nghị quyết số 52-NQ/TW của Trung ương Đảng với mục tiêu xác định rõ việc đảm bảo an toàn không gian mạng là một trong các yêu cầu trọng tâm trong chuyển đổi số.

Trong bài báo này, tác giả trình bày tầm quan trọng của vấn đề an toàn thông tin, kỹ năng an toàn thông tin trên môi trường số và đề xuất một số giải pháp nhằm đảm bảo an toàn thông tin cho các đối tượng tham gia vào quá trình xây dựng, phát triển, khai thác, sử dụng trên môi trường số.

2. AN TOÀN THÔNG TIN

2.1. An toàn thông tin là gì?

An toàn thông tin có thể được hiểu là cách thức, phương pháp để phòng ngừa, ngăn cản sự truy cập, tiết lộ, chia sẻ, phát tán, ghi lại, sử dụng hoặc phá hủy những thông tin khi chưa có được sự cho phép của cá nhân hay một tổ chức nào đó.

Theo Michael E. và các cộng sự: An toàn thông tin là việc bảo vệ các thuộc tính bí mật (confidentiality), tính toàn vẹn (integrity) và tính sẵn dùng (availability) của các tài sản thông tin trong quá trình chúng được lưu trữ, xử lý hoặc truyền tải [10].

An toàn thông tin có thể được chia thành ba thành phần chính đó là an toàn máy tính và dữ liệu (Computer & data security), an ninh mạng (Network security) và quản lý an toàn thông tin (Management of information security). Ba thành phần này có quan hệ mật thiết và giao thoa với nhau, trong đó phần chung của cả ba thành phần trên đó là chính sách an toàn thông tin. Trong đó, an toàn máy tính và dữ liệu bao gồm các nội dung đảm bảo an toàn cho hệ điều hành, ứng dụng, dịch vụ của máy tính; vấn đề điều khiển truy nhập trên hệ thống

máy tính; vấn đề mã hóa và bảo mật dữ liệu liên quan đến máy tính; vấn đề phòng chống phần mềm độc hại; việc sao lưu tạo dự phòng dữ liệu, đảm bảo dữ liệu lưu trong máy tính không bị mất mát khi xảy ra sự cố. An ninh mạng là việc đảm bảo an toàn cho hệ thống mạng và các thiết bị liên quan khi thông tin được truyền tải trên mạng, nhằm chống lại các tấn công, xâm nhập trái phép từ bên ngoài hệ thống. Quản lý an toàn thông tin là việc quản lý và giám sát việc thực thi các biện pháp nhằm đảm bảo an toàn thông tin cho hệ thống.

2.2. Tầm quan trọng của việc đảm bảo an toàn thông tin

Từ khi công nghệ thông tin ra đời thì việc chia sẻ thông tin lên hệ thống máy tính trở thành một thói quen thường xuyên của người dùng và nó gắn với quá trình sử dụng máy tính. Ngày nay, khoa học kỹ thuật và công nghệ bùng nổ và phát triển một cách nhanh chóng, đặc biệt là sự ra đời và phát triển của các thiết bị cầm tay, công nghệ internet kết nối vạn vật và đặc biệt là công cuộc chuyển đổi số đang diễn ra mạnh mẽ thì số lượng người dùng mạng Internet và số lượng thiết bị kết nối vào mạng Internet, số lượng dữ liệu và thông tin chia sẻ lên mạng đã tăng lên rất nhiều.

Theo Statista nghiên cứu cho thấy số lượng các thiết bị có kết nối Internet là khoảng 15 tỷ và trong những năm gần đây đã tăng mạnh lên hơn 28 tỷ thiết bị, có khoảng 15,14 tỷ thiết bị IoT được kết nối tính đến năm 2023, tương đương với gần gấp đôi tổng số người trên toàn thế giới. Finance Online nghiên cứu và cho biết khối lượng trong số này dự kiến sẽ tăng lên theo thời gian và lên hơn 25 tỷ trong vòng 7 năm tới [12].

Theo số liệu nghiên cứu của các tổ

chức quản lý [12] thì số lượng vi phạm an toàn thông tin tăng lên theo thời gian và năm sau luôn cao hơn năm trước, số lượng sự cố và thiệt hại do mất an toàn thông tin gây ra làm ảnh hưởng đến đời sống cá nhân cũng như hoạt động của các tổ chức là rất lớn. Số lượng thiết bị kết nối tăng trưởng nhanh chóng sẽ kéo theo số lượng thông tin chia sẻ lên mạng càng nhiều và nguy cơ bị xâm hại thông tin, không đảm bảo an toàn thông tin cũng tăng theo. Vì vậy, nếu người sử dụng không được trang bị kỹ năng, không được bồi dưỡng năng lực số để khai thác sử dụng thì sẽ dẫn đến nguy cơ mất an toàn thông tin và gây thiệt hại cho cá nhân, cơ quan, tổ chức và nhà nước. Việc trang bị nguồn lực, kỹ thuật và nâng cao kỹ năng số cho con người để đảm bảo an toàn thông tin và sẵn sàng ứng phó với sự cố an toàn thông tin là hết sức cần thiết. Chính vì vậy, việc nâng cao kỹ năng và năng lực an toàn thông tin cho người sử dụng nhằm đảm bảo an toàn thông tin trong các hoạt động cá nhân cũng như của các tổ chức trong của đời sống xã hội trở thành nhiệm vụ quan trọng hiện nay.

2.3. Năng lực số

Năng lực số là khái niệm dùng để đánh giá về khả năng của một người trong việc khai thác sử dụng, quản lý máy tính, khai thác công nghệ thông tin, khai thác mạng internet để thực hiện một hay nhiều công việc trên môi trường số. Có rất nhiều nghiên cứu định nghĩa về năng lực số, dưới đây là một số định nghĩa.

Theo Law, N. và các cộng sự thì năng lực số là năng lực tổng hợp của một người về khả năng sử dụng máy tính, sử dụng công nghệ thông tin, năng lực thông tin và năng lực truyền thông [9].

Theo Tấn, Đ. N và các cộng sự thì năng lực số là khả năng của một người có thể sử

dụng các công cụ của công nghệ để phục vụ công việc, giải trí và các hoạt động khác mang lại hiệu quả cao và an toàn trong công việc. Trong đó đánh giá khả năng làm chủ các phương tiện công nghệ để tìm kiếm, sử dụng, lưu trữ, trao đổi thông tin và khai thác thông tin qua Internet là yếu tố cốt lõi [7].

Trên cơ sở định nghĩa năng lực số, năm 2018, UNESCO dựa vào khung năng lực số của châu Âu và kết quả khảo sát khung năng lực số tại 47 quốc gia đã đề xuất khung năng lực số toàn cầu (Digital Literacy Global Framework - DLGF) bao gồm bảy năng lực như sau [11]:

- Năng lực vận hành các thiết bị và phần mềm;

- Năng lực về thông tin và dữ liệu;

- Giao tiếp và cộng tác;

- Sáng tạo nội dung số;

- Năng lực về an toàn;

- Năng lực giải quyết vấn đề;

- Năng lực liên quan đến nghề nghiệp;

Như vậy, năng lực an toàn thông tin là một trong bảy năng lực số quan trọng mà mỗi cá nhân đều cần phải có để có thể thực hiện tốt các hoạt động của mình trên môi trường số, từ đó mang lại hiệu quả công việc tốt hơn. Năng lực an toàn thông tin có mối liên hệ chặt chẽ với các năng lực khác và có ảnh hưởng đến các năng lực đó.

3. GIẢI PHÁP ĐẢM BẢO AN TOÀN THÔNG TIN CHO NGƯỜI DÙNG TRONG CÁC TRƯỜNG ĐẠI HỌC

3.1. Thực trạng chuyển đổi số trong các trường đại học

Cuộc cách mạng kỹ thuật số đã tác động toàn diện đến thế giới và chuyển đổi số đã trở thành xu hướng phát triển của mỗi quốc gia trên mọi lĩnh vực. Thời gian qua, chuyển đổi số trong nước đã có nhiều hoạt động diễn ra với các đặc điểm và điều kiện

triển khai khác nhau. Để đáp ứng nhu cầu và theo kịp sự phát triển của thế giới Thủ tướng Chính phủ đã ban hành Quyết định số 749/QĐ-TTg ngày 03/6/2020 phê duyệt “Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030” với đầy đủ các nội dung nhằm thực hiện Chương trình chuyển đổi số quốc gia. Trong đó, có nội dung chuyển đổi số trong giáo dục và đề ra mục tiêu cũng như đánh giá vai trò quan trọng kỹ năng sử dụng công nghệ thông tin, an toàn thông tin ở các cấp học trong đó có bậc đại học. Từ quyết định đó, Bộ GD&ĐT đã xây dựng và ban hành nhiều văn bản nhằm chỉ đạo thực hiện và triển khai các hoạt động chuyển đổi số trong đào tạo đại học ở Việt Nam. Vì vậy, hiện nay hệ thống các trường đại học trên cả nước đang tiến hành thực hiện chuyển đổi số một cách mạnh mẽ, ngay trong thời kỳ ảnh hưởng của đại dịch COVID-19. Các trường đã dần hình thành hệ sinh thái đại học số và hiện nay đang từng bước chuyển đổi số với các lĩnh vực như đào tạo, quản lý, tài nguyên, nhân lực.

Nhiều trường đại học đã từng bước triển khai hoạt động chuyển đổi số của mình, điển hình như Trường Đại học Bách Khoa Hà Nội đã triển khai hệ thống đào tạo trực tuyến trong thời kỳ COVID-19 thông qua việc mua các phần mềm của Microsoft để việc giảng dạy online có thể được triển khai một cách tốt nhất, đồng thời đề xuất từng bước số hoá để triển khai hệ thống học liệu số và lớp học số [6].

Trường Đại học Sư phạm Kỹ thuật thành phố Hồ Chí Minh đã xây dựng được nền tảng dạy học số với trung tâm dạy học ảo để tổ chức các khóa học trực tuyến hoàn toàn trên môi trường mạng Internet, theo đó tất cả tài nguyên học tập, hoạt động dạy học

đã được lưu trữ trên nền tảng số. Lãnh đạo trường đã có kế hoạch cụ thể vì vậy hầu hết các hoạt động trong nhà trường đã được triển khai từ rất sớm và bước đầu mang lại những kết quả khả quan [3].

Trường Đại học Công nghệ Thông tin và Truyền thông - Đại học Thái Nguyên đã xây dựng kiến trúc đại học số tổng thể đồng thời xây dựng lộ trình thực trên các nội dung chuyển đổi số trong đào tạo bằng cách dùng các phần mềm đào tạo trực tuyến, các kênh để truyền thông tuyển sinh. Xây dựng học liệu số với số lượng đầu sách, tạp chí, ebook, cơ sở dữ liệu trong thư viện của nhà trường hiện nay đạt 18.540 cuốn. Chuyển đổi số trong quản lý thông qua hệ thống quản lý học tập LMS triển khai áp dụng cho tất cả các loại hình đào tạo. Chuyển đổi số trong nghiên cứu khoa học, Nhà trường đặc biệt quan tâm đến việc đầu tư các phần mềm phục vụ quản lý, giảng dạy như các phần mềm Gerber, Lectra, Autocad, các phần mềm mô hình ảo [4].

Trường Đại học sư phạm Kỹ thuật Vinh đã triển khai chuyển đổi số bằng cách tăng cường ứng dụng công nghệ thông tin trong hoạt động đào tạo và nghiên cứu khoa học, trong chuyển đổi số học liệu phục vụ đào tạo, tuy nhiên qua nghiên cứu cho thấy hạ tầng công nghệ thông tin cơ bản còn thiếu cho việc triển khai học tập, giảng dạy và nghiên cứu khoa học của Nhà trường. Quá trình số hóa và xây dựng học liệu số đang còn manh mún, nhỏ lẻ, chưa có hệ thống và khó kiểm soát chất lượng, đây cũng là một trong các tình trạng chung của các trường đại học có quy mô nhỏ, đại học địa phương [1].

Ngoài ra, một số trường cũng đã triển khai theo đặc thù của mình, Trường Đại học Kinh tế Quốc dân tiến hành cung cấp toàn

bộ bài giảng, giáo trình của trường dưới dạng học liệu số để triển khai đào tạo trực tuyến. Nhà trường đã có chủ trương chính sách về chuyển đổi số, cơ sở hạ tầng và hệ thống phần mềm về cơ bản đáp ứng được cho quá trình chuyển đổi số, về đội ngũ con người được trang bị kiến thức cơ bản về chuyển đổi số. Trường Đại học Ngân hàng thành phố Hồ Chí Minh đã triển khai chuyển đổi số với hoạt động số hóa tài nguyên phục vụ đào tạo và triển khai hệ thống dạy học E-Learning có sự hỗ trợ của các công cụ để tổ chức, quản lý quá trình đào tạo trên nền tảng số. Trường Đại học Công nghiệp Hà Nội đã xây dựng quy trình chuyển đổi số, trường đã chuyển đổi số trong các hoạt động quản lý, đào tạo, tuyển sinh, đánh giá kết quả học tập. Trường Đại học Ngoại ngữ - Đại học Đà Nẵng đã xây dựng mục tiêu cụ thể cho hoạt động chuyển đổi số trong đào tạo là ứng dụng công nghệ thông tin vào dạy học và các bước để tiến hành chuyển đổi số cho các hoạt động trong Nhà trường với các chỉ tiêu then chốt và kế hoạch nhằm từng bước hoàn thiện quá trình chuyển đổi số.

Trường Đại học Quảng Bình từng bước xây dựng các hệ thống quản lý học liệu số, xây dựng bộ sưu tập số mở và nội sinh, triển khai hệ thống đào tạo trực tuyến, xây dựng các cơ sở dữ liệu số phục vụ kiểm định chất lượng giáo dục, vv.

Để nắm bắt tổng quan về tình hình chuyển đổi số tại các cơ sở giáo dục đại học ở Việt Nam thông qua mô hình SAMR [2], tác giả Nguyễn Thị Duyên đã nghiên cứu và chỉ ra việc chuyển đổi số ở các trường đại học tập trung vào đánh giá các hoạt động lớn: trong phương pháp giảng dạy, trong quản lý và trong công nghệ. Nhìn chung, các hoạt động chuyển đổi số của các trường

đều đang diễn ra theo chiều hướng tích cực, cơ bản đáp ứng yêu cầu về ứng dụng công nghệ trong dạy học và theo kịp xu thế trên thế giới.

Trong một nghiên cứu khác của Tô Hồng Nam [5] cho thấy các trường đại học trên toàn quốc đã có nhiều thành tựu trong hoạt động chuyển đổi số của mình. “Đối với hạ tầng công nghệ thông tin cơ bản đảm bảo để thực hiện chuyển đổi số, 100% các trường có phòng máy tính, có hệ thống mạng cục bộ, internet và wifi, có trang thông tin điện tử; 90% các trường ban hành các quy chế về an toàn thông tin; trên 90% các trường sử dụng phần mềm quản lý đào tạo, phần mềm quản lý văn bản; trên 60% sử dụng phần mềm quản lý nhân sự và quản lý tài sản, thiết bị. Đối với chuyển đổi số trong đào tạo và nghiên cứu khoa học, trên 50 trường có hệ thống quản lý học tập; có khoảng 110 trường (chiếm khoảng 50% tổng số các trường) triển khai đào tạo chính quy trực tuyến; khoảng 60% các trường triển khai học liệu số và hệ thống thi trắc nghiệm; trên 70% trường đã triển khai hệ thống thư viện điện tử”.

Như vậy, các hoạt động chuyển đổi số của các trường đại học trong cả nước đã được chú trọng và bước đầu đã có những kết quả nhất định. Điều này một lần nữa được Bộ Giáo dục & Đào tạo khẳng định trong báo cáo tính đến tháng 7 năm 2024, theo đó đã xây dựng được cơ sở dữ liệu về giáo dục đại học với 470 cơ sở đào tạo đại học tham gia, trong đó có hơn 25.000 chương trình đào tạo được chuyển đổi số, có hơn 100.000 hồ sơ cán bộ, giảng viên được số hoá và gần 3 triệu hồ sơ người học được số hoá, đồng bộ dữ liệu về sinh viên đã ra trường đã kết nối và đồng bộ chia sẻ dữ liệu việc làm của trên 97.000 sinh viên đã

tốt nghiệp. Đã đưa vào sử dụng dịch vụ công trực tuyến phục vụ gần 700.000 thí sinh đăng ký các nguyện vọng tuyển sinh vào đại học, thanh toán lệ phí xét tuyển trực tuyến và thí sinh xác nhận nhập học trực tuyến [8].

Song song với việc chú trọng hoạt động chuyển đổi số, nhiều trường đại học đã có chiến lược đào tạo ngành công nghệ thông tin và thành lập các trung tâm nghiên cứu và ứng dụng công nghệ, trang cấp thiết bị, nâng cấp hạ tầng cơ sở vật chất công nghệ thông tin để đẩy mạnh và hỗ trợ hoạt động chuyển đổi số, trong đó chú trọng đến vấn đề bảo mật và an toàn thông tin, các thiết bị, công nghệ hỗ trợ vấn đề an toàn thông tin như hệ thống máy chủ, hệ thống các thiết bị an toàn thông tin, hệ thống các phần mềm kiểm soát an toàn thông tin cho thiết bị và người sử dụng đã được nâng cấp và mua mới.

Bên cạnh những thuận lợi và kết quả đạt được thì việc chuyển đổi số trong các trường đại học cũng gặp nhiều khó khăn như hệ thống văn bản chưa hoàn thiện, các hoạt động chuyển đổi số mang tính độc lập chưa đồng bộ, kinh phí hạn hẹp, chưa thống nhất quy trình, thiếu sự gắn kết chia sẻ giữa các trường.

Nhiều chính sách liên quan đến học liệu, sở hữu trí tuệ, bản quyền tác giả còn chưa đầy đủ để hỗ trợ việc chuyển đổi số. Việc nhận thức, thói quen, tư duy về chuyển đổi số chưa được lan tỏa đến toàn thể người học, cán bộ quản lý, giảng viên; chưa sẵn sàng thay đổi và tiếp cận với môi trường số để có thể học mọi lúc, mọi nơi nhằm tiếp thu kiến thức dễ dàng thuận tiện hơn. Nhiều đơn vị còn bị động trong việc thực hiện chuyển đổi số, khả năng số hóa và thích ứng với dạy học trực tuyến của hệ thống giáo

dục số còn thấp. Một số trường hạ tầng công nghệ thông tin vẫn chưa đáp ứng yêu cầu học tập và tương tác số mọi lúc mọi nơi. Nguồn tài nguyên số chưa nhiều và chưa đồng bộ, mang tính nhỏ lẻ, nội sinh, hệ sinh thái giáo dục số chưa hoàn thiện và phát triển. Vấn đề quản trị số và đặc biệt là an toàn thông tin trong môi trường số chưa được chú trọng. Hệ thống bảo mật chưa cao, việc giáo dục, ý thức đảm bảo an toàn thông tin trong trường học chưa được chú trọng, các công nghệ, giải pháp và phần mềm ứng dụng trong công tác đảm bảo an toàn thông tin chưa có.

Như vậy, các hoạt động chuyển đổi số của các trường đại học chủ yếu tập trung vào các nội dung sau:

- Chuyển đổi số hạ tầng công nghệ thông tin, đường truyền, dịch vụ Internet và các trang thiết bị liên quan.

- Chuyển đổi số liên quan đến đào tạo như hoàn thiện quy định chương trình học trực tuyến, triển khai đào tạo trực tuyến.

- Chuyển đổi số trong quản lý giáo dục thông qua việc xây dựng các mô hình quản lý, các quy định quản lý trong hoạt động số.

- Chuyển đổi số trong các hoạt động dạy, học như xây dựng bài giảng, giáo trình số, chương trình số.

- Chuyển đổi số trong kiểm tra, đánh giá kết quả học tập.

- Chuyển đổi số trong tài nguyên và học liệu, số hóa, xây dựng, cập nhật học liệu số, chia sẻ học liệu số.

- Chuyển đổi số trong công tác tuyển sinh, đăng ký các nguyện vọng tuyển sinh vào đại học, thanh toán lệ phí xét tuyển, xác nhận nhập học trực tuyến.

- Chuyển đổi số trong nghiên cứu khoa học và đào tạo nhân lực chuyển đổi số.

- Chuyển đổi số trong quản lý hồ sơ

cán bộ, giảng viên, sinh viên.

- Chuyển đổi số trong các dịch vụ giáo dục như đóng học phí, bảo hiểm, cung cấp thông tin người học sau khi tốt nghiệp.

- Chuyển đổi số trong việc đảm bảo an ninh mạng và các hoạt động chuyển đổi số khác.

3.2. Giải pháp đảm bảo an toàn thông tin

Đảm bảo an toàn thông tin cho mỗi trường đại học và mỗi người khi tham gia vào hoạt động giáo dục là yêu cầu cơ bản nhưng lại quyết định đến hiệu quả trong suốt quá trình diễn ra của hoạt động giáo dục. Đảm bảo an toàn thông tin có thể được xem là một trong các yếu tố vô cùng quan trọng trong khi triển khai các hoạt động số trong môi trường giáo dục hiện nay. Đảm bảo an toàn thông tin là nghĩa vụ và trách nhiệm của các tổ chức giáo dục và mỗi công dân khi tham gia vào hoạt động giáo dục đó. Vì vậy, mỗi trường đại học và cá nhân tham gia hoạt động giáo dục cần thực hiện các giải pháp tăng cường nhằm bảo đảm an toàn thông tin, đảm bảo bảo mật thông tin, đảm bảo tính toàn vẹn thông tin và sẵn sàng đáp ứng thông tin cho các hệ thống thông tin quan trọng phục vụ mọi hoạt động giáo dục và đào tạo cũng như các hoạt động trong đời sống xã hội. Việc đảm bảo an toàn thông tin này liên quan đến các tổ chức giáo dục mà cụ thể là các trường đại học và người tham gia vào hoạt động giáo dục đó là cán bộ, giảng viên và sinh viên trong các trường đại học. Trên cơ sở nghiên cứu thực trạng và rút ra được 11 nội dung chuyển đổi số trong các trường đại học trong mục 3.1, chúng tôi đề xuất hai nhóm giải pháp liên quan đến hai đối tượng trên 11 nội dung đó như sau.

a. Đối với các trường đại học

Là các tổ chức giáo dục quản lý và đào tạo người học, có vai trò định hướng chủ

trương, chính sách, chiến lược phát triển chuyển đổi số của nhà trường, vì vậy việc đảm bảo năng lực an toàn thông tin cho các hoạt động giáo dục của các trường đại học là vô cùng quan trọng, chính vì vậy các trường đại học cần phải:

- Ban hành chủ trương, chính sách về chuyển đổi số của mình một cách vĩ mô, dài hạn nhưng mang tính cụ thể với từng nội dung liên quan đến hoạt động chuyển đổi số của Nhà trường.

- Quản lý chặt chẽ toàn bộ thông tin của đơn vị và các cá nhân trên môi trường mạng trên cơ sở pháp luật và công ước quốc tế. Xây dựng, triển khai các quy định nội bộ có tính pháp lý để đảm bảo an toàn thông tin và dữ liệu trong nhà trường.

- Trong quá trình thực hiện chuyển đổi số nói chung và trang cấp các hệ thống phần mềm cần phải đảm bảo an toàn thông tin ngay từ khâu thiết kế, đảm bảo an toàn thông tin theo mô hình 4 lớp đã được Bộ Thông tin và Truyền thông quy định. Các hệ thống thông tin trong nhà trường cần phải được kiểm tra và xây dựng với cấp độ an toàn thông tin phù hợp trong từng công việc.

- Phổ biến Luật An ninh mạng, quy định về hoạt động bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn, xã hội trên không gian mạng. Phổ biến các quy định pháp lý của Nhà nước liên quan đến an toàn thông tin đến từng đối tượng để nắm bắt và vận dụng hợp lý trong công việc của mình.

- Triển khai các hoạt động theo Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh công tác ứng cứu sự cố an toàn thông tin mạng.

- Tăng cường thông tin và tuyên truyền về an toàn thông tin đến cán bộ, giảng viên và sinh viên nhằm nâng cao nhận thức của các đối tượng về an toàn thông tin và những

mối đe dọa tiềm ẩn liên quan đến an ninh mạng trong quá trình thực hiện các hoạt động của mình.

- Đẩy mạnh các giải pháp bảo mật thông tin, tăng cường giám sát và bảo vệ dữ liệu đào tạo, kho tài nguyên số, tài sản sở hữu trí tuệ, các công trình nghiên cứu khoa học, sách và các loại tài nguyên số khác nhằm bảo đảm an toàn cho các ứng dụng, dịch vụ trên nền tảng số, đặc biệt là các hệ thống quản lý tài nguyên thông tin của giảng viên và sinh viên, đảm bảo tính bảo mật và riêng tư cho dữ liệu cá nhân.

- Nâng cao năng lực và kiến thức an toàn thông tin cho cán bộ, giảng viên và sinh viên trong hoạt động chuyển đổi số và các công việc trên môi trường số thông qua các khóa đào tạo, tập huấn, bồi dưỡng về an toàn thông tin, về phòng chống các cuộc tấn công mạng và xử lý sự cố an ninh mạng.

- Xây dựng và triển khai các chính sách, quy trình, quy định về an toàn thông tin, an toàn dữ liệu trong nhà trường, đặc biệt là các dữ liệu nhạy cảm để mỗi cán bộ, giảng viên và sinh viên đảm bảo có sự hiểu biết và tuân thủ quy tắc an toàn thông tin một cách toàn diện và nhất quán.

- Thành lập đội xử lý sự cố về an toàn thông tin mạng trong nhà trường đồng thời tham gia vào mạng lưới ứng cứu sự cố an toàn thông tin của Bộ Giáo dục và Đào tạo, Bộ Thông tin và Truyền thông và mạng lưới quốc gia để nhận được sự tư vấn, hỗ trợ xử lý kịp thời các sự cố gây mất an toàn thông tin trong quá trình thực hiện các hoạt động của mình.

- Tiếp tục hoàn thiện và đồng bộ cơ sở hạ tầng, thiết bị công nghệ thông tin để phục vụ mọi hoạt động số. Nâng cao các giải pháp bảo mật cơ sở dữ liệu trong giáo dục. Tăng cường áp dụng các công nghệ cao

trong bảo mật và an toàn thông tin, có các giải pháp sao lưu dự phòng và nâng cao chất lượng quản lý an toàn thông tin để thúc đẩy và phát triển các hoạt động số trong môi trường giáo dục.

- Xây dựng các chiến lược an toàn thông tin thông qua các giải pháp mã hoá thông tin dữ liệu của Nhà trường, triển khai chữ ký số và các kỹ thuật đảm bảo an toàn thông tin như điều khiển truy nhập; tường lửa; các hệ thống phát hiện và ngăn chặn xâm nhập; các công cụ rà quét phần mềm độc hại.

- Thường xuyên thực hiện kiểm tra, đánh giá và cải tiến hệ thống an toàn thông tin cho máy chủ, máy tính trạm, các hệ thống đào tạo, hệ thống quản lý, hệ thống dạy học trực tuyến, hợp tác với các cơ quan chức năng chuyên về an toàn thông tin để giao lưu, học hỏi, chia sẻ thông tin, kinh nghiệm trong công tác chuyển đổi số, công tác an toàn thông tin, bảo mật dữ liệu và thông tin cá nhân.

- Nhận diện các nguy cơ gây mất an toàn thông tin để thường xuyên tuyên truyền và phổ biến các dạng tấn công thường gặp làm mất an toàn thông tin như tấn công vào mật khẩu; tấn công bằng mã độc; tấn công từ chối dịch vụ; tấn công giả mạo địa chỉ; tấn công nghe lén; tấn công bằng bom thư và các kiểu tấn công khác cho người dùng. Công khai các dạng phần mềm độc hại để mọi người cũng tránh và đề phòng như phần mềm Logic bomb; Trojan Horse; Back door; các loại virus; Worm; Zombie; Rootkit; Adware và các loại phần mềm khác.

- Thiết lập chế độ phân quyền, khai thác tài nguyên trong các hệ thống dùng chung như thư viện số, các phần mềm quản lý sinh viên, quản lý đào tạo hay các hệ

thống phần mềm khác.

- Tiến hành kiểm tra, xử lý và có chế tài khi các cá nhân hay đơn vị vi phạm an toàn thông tin để nâng cao hiệu quả việc bảo vệ thông tin trên mạng.

b. Đối với cán bộ, giảng viên và sinh viên

Là những người trực tiếp thực hiện các hoạt động trên môi trường số một cách thường xuyên, là đối tượng tương tác và tiếp cận cũng như thực hiện các quy trình, nội dung, thao tác trong môi trường số. Vì vậy, mỗi đối tượng cần phải:

- Thực hiện nghĩa vụ công dân về việc đảm bảo an toàn thông tin trong luật an ninh mạng và các quy định khác của Nhà nước và Pháp luật khi tham gia các hoạt động giáo dục trên môi trường số, tham gia chuyển đổi số.

- Không ngừng nâng cao năng lực và kiến thức an toàn thông tin của cá nhân, tham gia đầy đủ các khóa đào tạo, tập huấn, bồi dưỡng về an toàn thông tin, về phòng chống các cuộc tấn công mạng và xử lý sự cố an ninh mạng nói chung và dành cho giáo dục nói riêng mà nhà trường và các đơn vị tổ chức.

- Có nhận thức đầy đủ, đúng đắn về tầm quan trọng của việc đảm bảo an toàn thông tin trong môi trường giáo dục số để tránh những nguy cơ gây mất an toàn thông tin cho cá nhân và Nhà trường khi thực hiện các hoạt động giáo dục.

- Khi sử dụng mạng xã hội và các hoạt động trên môi trường số cần phải kiểm tra tính xác thực của thông tin trước khi thực hiện các hoạt động của mình, luôn luôn có ý thức đề phòng và thực hiện bảo vệ an toàn cá nhân cũng như của tổ chức trước các thông tin không lành mạnh trên môi trường mạng.

- Tăng cường sử dụng các giải pháp bảo mật và an toàn thông tin trên thiết bị cá nhân, thường xuyên cập nhật các phiên bản phần mềm bảo mật để bảo vệ máy tính và thiết bị số khác khỏi các nguy cơ mất an toàn thông tin và dữ liệu cá nhân. Tránh sử dụng các thiết bị cũng như hệ thống mạng không an toàn để thực hiện các hoạt động giáo dục.

- Đẩy mạnh quá trình bảo vệ an toàn thông tin cá nhân trong mọi tình huống, mọi lúc, mọi nơi để thông tin cá nhân không bị tiết lộ, dẫn đến tình trạng đánh cắp thông tin phục vụ truy cập bất hợp pháp, lừa đảo, giả mạo và chiếm đoạt thông tin, tài sản cá nhân cũng như của các tổ chức xã hội. Có trách nhiệm cao khi cung cấp những thông tin lên môi trường mạng, thận trọng khi chia sẻ và tương tác thông tin lên mạng Internet.

- Nâng cao ý thức toàn dân bảo vệ an toàn thông tin của mình và tuyên truyền rộng rãi trong nhân dân. Khi có sự cố nhanh chóng báo cáo cho Nhà trường và cơ quan chức năng để được hỗ trợ, xử lý các vấn đề liên quan đến an toàn thông tin của cá nhân và đơn vị.

- Biết nhận diện các nguy cơ gây mất an toàn thông tin thông qua các phương thức tấn công và phần mềm độc hại như tấn công vào mật khẩu; tấn công bằng mã độc; tấn công từ chối dịch vụ; tấn công giả mạo địa chỉ; tấn công nghe lén; tấn công bằng bom thư; phần mềm độc hại Logic bomb; Trojan Horse; Back door; các loại virus; Worm; Zombie; Rootkit; Adware và các loại phần mềm khác.

- Nâng cao năng lực quản lý an toàn thông tin cá nhân, xây dựng và hoàn thiện đạo đức an toàn thông tin của mỗi cá nhân để ngày một hoàn thiện năng lực an toàn thông tin của mình, từ đó phát huy hiệu quả công

việc và mọi hoạt động trên môi trường số.

- Không cung cấp hay để lộ các loại tài khoản, định danh số của cá nhân như thông tin về thẻ cán bộ, giảng viên, sinh viên cho người khác trên môi trường mạng.

- Không cung cấp các tài khoản sử dụng thư viện số, các hệ thống phần mềm quản lý đào tạo, học trực tuyến, các hệ thống phần mềm khác cho người lạ. Khi sử dụng cần tuân thủ các quy định của Nhà trường, nhất là bảo quản tài khoản và định danh và thông tin dữ liệu liên quan.

- Khi sử dụng các nền tảng, công cụ để thực hiện chuyển đổi số hay tham gia các hoạt động dạy học, nghiên cứu trên môi trường số cần lựa chọn, sử dụng các công cụ, hệ thống có tính chính quy, có nguồn gốc xuất xứ rõ ràng để tránh bị rò rỉ hay bị đánh cắp thông tin khi sử dụng.

- Khi tham gia các hội nhóm trên mạng xã hội cần tìm hiểu và nắm bắt các tổ chức thông tin có tính pháp lý để tránh bị lừa hoặc lôi kéo vào các hoạt động chống phá nhà nước và phá hoại thông tin quốc gia.

- Khi thực hiện các giao dịch cá nhân cần sử dụng các yếu tố xác thực hai lớp hay bảo mật cá nhân để đảm bảo an toàn dữ liệu.

4. KẾT LUẬN

Cuộc cách mạng công nghiệp lần thứ 4 ra đời và phát triển cùng với công cuộc chuyển đổi số đang diễn ra một cách mạnh mẽ đã và đang mang đến cho ngành giáo dục nói chung các trường đại học nói riêng nhiều cơ hội phát triển nhưng cũng kèm theo những thách thức trong đó có vấn đề an toàn thông tin và dữ liệu. Do đó, các trường đại học cần tiến hành xây dựng các kế hoạch có tầm chiến lược về an toàn thông tin và dữ liệu, có các phương án nhận diện các nguy cơ, gây mất an toàn thông tin từ đó nâng cao trách nhiệm, nghĩa vụ của mỗi cá nhân trong

việc đảm bảo an toàn thông tin và dữ liệu để có thể tham gia vào hệ thống giáo dục đại học một cách an toàn và đáp ứng tốt mọi công việc trong thời kỳ chuyển đổi số. Các trường đại học tiếp tục tiến hành xây dựng, hoàn thiện hệ thống quy định về bảo đảm an toàn thông tin, tạo cơ sở pháp lý vững chắc bảo đảm sự an toàn, tin cậy trong quá trình chuyển đổi số, quản lý hoạt động của cá nhân và các đơn vị trong nhà trường để đảm bảo an toàn thông tin một cách tốt nhất.

Với đặc điểm quá trình chuyển đổi số, thực trạng, điều kiện, môi trường và cả nhân tố con người khi tham gia vào hoạt động chuyển đổi số của các trường khác nhau là khác nhau. Do đó, trong nghiên cứu này, chúng tôi chưa chỉ ra một cách chi tiết cho từng trường khi thực hiện các giải pháp, đó cũng chính là hạn chế mà chúng tôi sẽ tiếp tục nghiên cứu trong tương lai để hoàn thiện hơn hệ thống giải pháp đảm bảo an toàn thông tin của mình.

TÀI LIỆU THAM KHẢO

- [1] Nguyễn Viết Cường, Phan Việt Đức (2023), Thực trạng và giải pháp chuyển đổi số trong giáo dục ở Trường Đại học Sư phạm Kỹ thuật Vinh. *Equipment with new general education program*, Volume 1, Issue 294. ISSN 1859 - 0810. 2023, trang 30-32. Journal homepage: www.tapchithietbigiaoduc.vn.
- [2] Nguyễn Thị Duyên (2023), Đánh giá tình hình chuyển đổi số tại các cơ sở giáo dục đại học ở Việt Nam thông qua mô hình SAMR. *Tạp chí nghiên cứu Tài chính kế toán*. 2023, trang 43-47.
- [3] Đỗ Văn Dũng, Bùi Hồng Minh (2024), Trường Đại học Sư phạm Kỹ thuật TP Hồ Chí Minh, Chuyển đổi số cho giáo dục đại học và kết quả tại trường Đại học Sư phạm Kỹ thuật TP Hồ Chí Minh. Trang 294-303. <https://tailieu.vn/doc/chuyen-doi-so-cho-giao-duc-dai-hoc-va-ket-qua-tai-truong-dai-hoc-su-pham-ky-thuat-thanh-pho-ho-chi-m-2534937.html>. Truy cập ngày 20/5/2024.
- [4] Bùi Thị Thu Hương (2022), Chuyển đổi số trong giáo dục đại học tại Trường Đại học Công nghệ Thông tin và Truyền thông - Đại học Thái Nguyên. *International Conference on Smart Schools 2022*, PP 228-232.
- [5] Tô Hồng Nam (2022), Chuyển đổi số giáo dục đại học: Xây dựng mô hình giáo dục đại học số tại Việt Nam. Số 5, 5/2022, *Tạp Chí Thông tin & Truyền thông*.
- [6] Nguyễn Đăng Tuệ (2024), Viện Kinh tế và Quản lý - Trường Đại học Bách Khoa Hà Nội. Thách thức chuyển đổi số đối với cơ sở giáo dục đại học - Trường hợp Trường Đại học Bách Khoa Hà Nội. Trang: 124-132. <https://tailieu.vn/doc/thach-thuc-chuyen-doi-so-doi-voi-co-so-giao-duc-dai-hoc-truong-hop-truong-dai-hoc-bach-khoa-ha-noi-2534920.html>. Truy cập ngày 20/5/2024.
- [7] Tấn, Đ. N., & Marquet, P. (2018), Năng lực công nghệ số đáp ứng nhu cầu xã hội: Các mô hình quốc tế và hướng tiếp cận tại Việt Nam. *Tạp Chí Khoa Học Xã Hội TP. HCM*, 244(12), 23–39.
- [8] Bộ GDĐT sơ kết công tác chuyển đổi số, cải cách hành chính. <https://moet.gov.vn/tintuc/Pages/tin-tong-hop.aspx?ItemID=9559>. Truy cập 30/7/2024.
- [9] Law, N., Woo, D., & Wong, G. (2018). A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2 (p. 146). UNESCO.

- [10] Michael E. Whitman, Herbert J. Mattord, Principles of information security, 4th edition, Course Technology, Cengage Learning, 2012.
- [11] UNESCO. (2018). A Global Framework of Reference on Digital Literacy. In UNESCO Institute for Statistics.
- [12] <https://techinformed.com/iot-in-2023-and-beyond/>

Liên hệ:

TS. Đậu Mạnh Hoàn

Khoa Công nghệ thông tin, Trường Đại học Quảng Bình

Địa chỉ: 18 Nguyễn Văn Linh, Đồng Hới, Quảng Bình

Email: daumanhhoan@yahoo.com

Ngày nhận bài: 04/12/2024

Ngày gửi phản biện: 04/12/2024

Ngày duyệt đăng: 26/02/2025