

NÂNG CAO CÔNG TÁC BẢO MẬT THÔNG TIN CỦA KHÁCH HÀNG CỦA DỊCH VỤ NGÂN HÀNG SỐ TẠI THỊ TRƯỜNG VIỆT NAM

Trần Văn Hải¹, Nguyễn Bá Tùng^{1}*

**Tác giả liên hệ, Email: nbtung@hou.edu.vn*

Ngày tòa soạn nhận được bài báo: 19/05/2025

Ngày phản biện đánh giá: 21/07/2025

Ngày bài báo được duyệt đăng: 29/08/2025

DOI: 10.59266/houjs.2025.686

Tóm tắt: Cuộc cách mạng công nghiệp lần thứ tư đã mang lại những thay đổi sâu sắc trong nhiều lĩnh vực như: giáo dục, y tế, văn hóa, xã hội, kinh tế bao gồm cả lĩnh vực tài chính ngân hàng. Nhờ những thành tựu của khoa học công nghệ, các sản phẩm, dịch vụ của ngân hàng ngày càng đa dạng, đáp ứng nhu cầu ngày càng cao của khách hàng. Bên cạnh ngân hàng truyền thống, dịch vụ ngân hàng số ra đời như một điều tất yếu góp phần nâng cao chất lượng sản phẩm, tăng cường năng lực cạnh tranh và tối đa hóa lợi nhuận. Tuy nhiên, vấn đề chiếm đoạt thông tin, tài sản của khách hàng trong dịch vụ ngân hàng số hiện nay diễn ra với tần suất đáng báo động. Tội phạm công nghệ cao đang lợi dụng các lỗ hổng trong công tác quản lý và sự hạn chế của hạ tầng kỹ thuật nhằm tiến hành các hoạt động bất hợp pháp. Bài viết sẽ tập trung làm rõ những thành tựu, thách thức cần giải quyết, từ đó đề xuất các biện pháp giúp cải thiện năng lực bảo mật thông tin của khách hàng trong dịch vụ ngân hàng số. Bài viết sử dụng phương pháp nghiên cứu định tính thông qua các nguồn dữ liệu thứ cấp trong giai đoạn 5 năm trở lại đây. Những vấn đề liên quan đến khung pháp lý, cơ sở hạ tầng và đội ngũ nhân lực sẽ được phân tích và làm rõ qua bài viết.

Từ khóa: Ngân hàng số, bảo mật thông tin, khách hàng, khung pháp lý, cơ sở hạ tầng, đội ngũ nhân lực

I. Đặt vấn đề

Hiện nay có khá nhiều khái niệm, định nghĩa về bảo mật thông tin. Theo khái niệm về bảo mật thông tin của Tập đoàn IBM, bảo mật thông tin (Information Security) là việc bảo vệ thông tin quan trọng khỏi việc bị truy cập, tiết lộ, sử

dụng, thay đổi hoặc phá hoại trái phép. Bảo mật thông tin giúp đảm bảo thông tin của tổ chức, cá nhân được bảo mật và duy trì sự toàn vẹn. Theo như khái niệm, ta có thể hiểu rằng thông tin ở đây có thể bao gồm dữ liệu về tài chính, những bí mật của cá nhân hoặc doanh nghiệp. Những thông tin này được coi là tài sản của cá nhân hay

¹ Khoa Tài chính - Ngân hàng, Trường Đại học Mở Hà Nội

doanh nghiệp có thể ở dạng tệp hoặc dữ liệu kỹ thuật số, tài liệu giấy, phương tiện vật lý hay thậm chí có thể là lời nói của con người. Những dữ liệu, tài sản này cần được bảo đảm an toàn trong suốt vòng đời tồn tại của nó thông qua các hoạt động như lưu trữ, kiểm toán, thử nghiệm...

Hiện nay, khoảng 60% dân số toàn cầu đang sử dụng mạng internet. Những người sử dụng này thường xuyên phải đối mặt với các vấn đề liên quan tới bảo mật thông tin. Các đối tượng đang lợi dụng những lỗ hổng trong hệ thống thông tin, viễn thông nhằm tiến hành các hành vi bất hợp pháp. Theo báo cáo Global Risk của Diễn đàn Kinh tế Thế giới, thiệt hại do tội phạm mạng gây ra cho nền kinh tế toàn cầu là hơn 445 tỷ USD/năm. Đối với thị trường Việt Nam theo BKAV, thiệt hại do loại tội phạm này gây là 8.700 tỷ đồng, trong đó thiệt hại trong lĩnh vực tài chính ngân hàng chiếm tỷ trọng lớn (TS. Trần Thị Thu Hà, TS. Nguyễn Thị Thu Thoa, 2024).

Tội phạm công nghệ cao trong môi trường ngân hàng số ngày càng tinh vi với nhiều thủ đoạn và rủi ro khác nhau. Người sử dụng có thể gặp rủi ro khi lộ tin nhắn, mã OTP, rủi ro từ người thân, từ tài khoản giả mạo, rò rỉ các thông tin trên căn cước công dân. Khi quá trình lừa đảo diễn ra, chúng đánh cắp tài sản của chủ sở hữu rất nhanh, đặc biệt là tiền và chuyển qua các tài khoản giả mạo khác. Nhiều đối tượng có thể chiếm đoạt quyền kiểm soát tài khoản thư điện tử, hay tài khoản mạng xã hội sau đó chúng gửi những tin nhắn với nội dung lừa đảo, tiếp cận và lừa khách hàng chuyển tiền, hoặc gửi đường link vay tín dụng đen lãi suất cao. Chúng giả mạo nhân viên ngân hàng liên lạc, nhằm chiếm đoạt thông tin, giao dịch, lừa chuyển tiền hay hướng dẫn cài mã độc. Đặc biệt, nhiều đối tượng giả danh cơ quan chức năng đã chiếm đoạt hàng tỷ đồng.... Tội phạm

công nghệ cao trong lĩnh vực ngân hàng có thể tiến hành hành vi phạm tội mọi lúc, mọi nơi với nhiều hình thức đa dạng như: gây gián đoạn giao dịch, chiếm quyền sử dụng tài khoản, chiếm đoạt tiền, tài liệu và thông tin cá nhân.

Theo Bộ Công an Việt Nam, từ năm 2019 - 2020 có 1.300 GB dữ liệu cá nhân của Việt Nam bị mua bán trái phép. Nhiều vụ án đánh cắp thông tin khách hàng đã diễn ra, có thể kể tới vụ hơn 163 triệu tài khoản khách hàng của Công ty Công nghệ và Internet hàng đầu Việt Nam (VNG) bị tiết lộ; hơn 5 triệu email và hàng chục nghìn thông tin thẻ thanh toán của Công ty Thế giới Di động và Điện máy xanh bị rò rỉ; Việt Nam Airline để lộ 411 nghìn tài khoản thành viên Bông Sen Vàng.... (Nguyễn Thanh Nguyên, 2024). Đứng trước những khó khăn trên, các ngân hàng đang không ngừng nâng cao năng lực thông qua nhiều giải pháp giúp cho việc triển khai các dịch vụ ngân hàng số một cách thuận tiện, nhanh chóng, và đảm bảo an toàn cho người dùng. Tuy nhiên điều này cũng đặt ra bài toán an toàn thông tin mà các ngân hàng cần phải xử lý, đặc biệt đối với dịch vụ ngân hàng số đang ngày càng trở nên phổ biến hơn.

II. Cơ sở lý thuyết

Hiện nay, có nhiều khái niệm về Ngân hàng số - Digital Banking. Theo Ngân hàng United Overseas Bank Singapore: “Ngân hàng số là kinh doanh ngân hàng trong thời đại số, tức là kinh doanh ngân hàng trong điều kiện khách hàng sử dụng nhiều thiết bị công nghệ hơn, kết nối internet nhiều hơn, có nhu cầu kết nối qua công nghệ số, các phân đoạn khách hàng khác nhau có thể chọn các kênh kết nối với ngân hàng khác nhau”. Hãng Temenos đưa ra mô hình ngân hàng số được mô phỏng ngân hàng số bằng

phương trình: $A+B+C = D$, trong đó:

- Anytime, anyplace, any channel: phục vụ khách hàng mọi lúc, mọi nơi, bất cứ khi nào;

- Better banking: dịch vụ tốt hơn ngân hàng truyền thống;

- C-Contextual: các sản phẩm, dịch vụ đáp ứng nhu cầu của mọi khách hàng;

- Digital banking: là tổng hợp của các yếu tố nêu trên trở thành ngân hàng số.

Theo Ngân hàng Nhà nước Việt Nam, ngân hàng số hoạt động dựa trên nền tảng công nghệ nhằm cung cấp toàn bộ các dịch vụ cho khách hàng. Các dịch vụ của ngân hàng sẽ được tiến hành thông qua các thiết bị số trong môi trường mạng và phần lớn được số hóa để triển khai. Các kênh phân phối, ứng dụng sản phẩm, phân tích dữ liệu lớn, sẽ được tự động hóa (PGS.TS. Lê Hoàng Nga, 2022).

Đảm bảo tính bảo mật thông tin của khách hàng hay an ninh thông tin chính là đảm bảo tính bảo mật sẵn có của thông tin đó (ISO/IEC, 2700). Điều này bao gồm bảo vệ cả dữ liệu vật lý và dữ liệu số khỏi các hoạt động trái pháp luật (Ogbanufe, 2021). Tuy nhiên khi xem xét các vấn đề về an ninh hay bảo mật thông tin hiện nay thì thuật ngữ này chưa thực sự phù hợp (Lundgren & Moller, 2017) vì xét trong bối cảnh hiện nay công tác bảo mật không chỉ dừng lại ở các biện pháp kỹ thuật nhằm đảm bảo bảo mật thông tin mà còn phản ánh sự tương tác giữa các chủ thể với nhau. Von Solms & Van Nickerk (2013) cho rằng việc giữ bí mật thông tin giống như bảo vệ tài sản khỏi bất kỳ hiểm họa nào. Trong môi trường số, khi các cá nhân tương tác với nhau thì bảo mật thông tin sẽ diễn ra ở phạm trù rộng hơn về phạm vi và đối tượng. Chính vì vậy đảm bảo an ninh về thông tin tài chính sẽ liên quan tới các bí mật thông tin tài chính của khách hàng.

Nếu đối tượng khách hàng là doanh nghiệp, thì thông tin tài chính đến từ các hoạt động giao dịch được ghi nhận trên báo cáo tài chính. Đây là các thông tin quan trọng phục vụ cho quá trình ra quyết định của nhà đầu tư (Honggowati, 2015) cũng như nhà quản lý (Gibson, 1992). Thông tin tài chính của khách hàng sẽ bao gồm thông tin của cá nhân và doanh nghiệp. Khi khách hàng sử dụng dịch vụ của ngân hàng họ đã đặt niềm tin trong việc sử dụng vì vậy việc vi phạm dữ liệu khách hàng sẽ ảnh hưởng tiêu cực tới niềm tin của khách hàng dẫn tới quyết định thay đổi nhà cung cấp dịch vụ tài chính của khách hàng (Kang, 2018). Do vậy, đảm bảo an toàn thông tin của khách hàng giúp doanh nghiệp nâng cao năng lực cạnh tranh, phòng ngừa rủi ro và tối đa hóa lợi nhuận (Reid & Van Niekerk, 2014).

Như vậy, đảm bảo an toàn các thông tin tài chính khách hàng trong môi trường số nhằm ngăn ngừa những rủi ro cho doanh nghiệp, tổ chức, cá nhân trong không gian mạng. Điều này giúp mang lại lợi ích cao nhất cho khách hàng khi sử dụng các sản phẩm, dịch vụ tài chính. Để làm được điều đó, các ngân hàng cần đảm bảo quy trình hoạt động, nguồn nhân lực cao kết hợp với những yếu tố bên ngoài như: môi trường kinh doanh lành mạnh, cùng với một khung pháp lý, chính sách nhà nước rõ ràng, vững chắc giúp phòng ngừa rủi ro, tăng cường chất lượng cũng như nâng cao lợi nhuận cho doanh nghiệp.

III. Phương pháp nghiên cứu

Để phân tích làm rõ các nội dung về việc đảm bảo an toàn thông tin trong ngân hàng số tại Việt Nam qua đó đánh giá thực trạng và đề xuất giải pháp nhằm nâng cao chất lượng và năng lực bảo mật thông tin. Nhóm tác giả đã sử dụng phương pháp phân tích định tính thông qua các nguồn dữ liệu thứ cấp từ các báo cáo, bài báo, tạp

chí, số liệu từ báo cáo tình hình thực hiện hoạt động cung cấp và triển khai các sản phẩm, dịch vụ số của các ngân hàng tại Việt Nam.

IV. Kết quả và thảo luận

4.1. Tính cấp thiết

Ngân hàng số nhằm đáp ứng xu thế công nghệ của hoạt động của ngân hàng, chủ yếu dựa vào các nền tảng dữ liệu điện tử và công nghệ số. Nhắc tới ngân hàng số, ta cần nhắc tới các dịch vụ ngân hàng số phổ biến hiện nay như: Home Banking, Internet Banking, Mobile Banking, thẻ ngân hàng Visa, debit hay mc2, ví điện tử... Trong đó, dịch vụ Internet Banking có thể coi là phổ biến hơn cả, với nhiều tính năng, tiện ích như chuyển tiền 24/7, thanh toán trực tuyến... Trong những năm gần đây, sự phát triển vượt bậc của ngân hàng số đã đem lại lợi nhuận không nhỏ cho các ngân hàng cũng như tiện ích cho khách hàng.

Nhờ sự phát triển của công nghệ, ngân hàng số hiện nay có thể phục vụ các dịch vụ mọi lúc mọi nơi. Các dịch vụ ngân hàng số ngày nay có thể tiếp cận được khách hàng ở vùng sâu, vùng xa, giúp giảm chi phí, nhân công, kho bãi và nâng cao lợi thế cạnh tranh. Dịch vụ số giúp ngân hàng nhanh chóng tiếp cận khách hàng, kịp thời bắt kịp những thay đổi của thị trường cũng như nhu cầu khách hàng. Cung cấp các sản phẩm và dịch vụ tài chính qua nền tảng số giúp ngân hàng đa dạng hóa sản phẩm của mình giúp tăng doanh thu và lợi nhuận chung. Các sản phẩm và dịch vụ tài chính của ngân hàng số rất đa dạng, phù hợp với nhu cầu đa dạng của khách hàng kết hợp với thủ tục đơn giản, linh hoạt về không gian và thời gian thực hiện thông qua các thiết bị kết nối internet là xu hướng hiện đại hóa hiện nay.

Đối với khách hàng, việc thực hiện

các giao dịch qua ngân hàng số giúp họ có thể nhanh chóng hoàn tất các giao dịch một cách thuận lợi, giúp giảm chi phí và tiết kiệm thời gian điều mà với ngân hàng truyền thống họ cần phải di chuyển ra các chi nhánh để thanh toán, chuyển khoản, thay đổi thông tin cá nhân..... Sau khi hoàn thành các giao dịch trên ngân hàng số khách hàng có thể dễ dàng kiểm tra giao dịch và lưu trữ trong phần lịch sử giao dịch một cách dễ dàng phục vụ cho việc tra cứu và tìm kiếm sau này. Điều này giúp cho các giao dịch được nhanh chóng, tiết kiệm thời gian và công sức.

Bên cạnh những lợi thế, các ngân hàng đang phải đối mặt với nhiều thách thức trong việc bảo mật thông tin của khách hàng trong không gian mạng hiện nay. Mặc dù, việc tiến hành các giao dịch được triển khai bảo mật ba lớp bao gồm: sử dụng tên đăng nhập, nhập mật khẩu và sử dụng mã OTP để thực hiện giao dịch nhằm giúp bảo mật thông tin của khách hàng. Tuy nhiên, các lỗ hổng trong công tác bảo mật vẫn tồn tại như bị đánh cắp mật khẩu hay bị đánh cắp mã OTP và không ít trường hợp kẻ gian lợi dụng các lỗ hổng này để đánh cắp, rao bán thông tin khách hàng, thậm chí trong nhiều trường hợp tiền trong tài khoản của khách hàng đã bị đánh cắp. Khả năng bảo mật thông tin đối với các giao dịch ngân hàng số luôn được các ngân hàng quan tâm đầu tư nhưng vẫn chưa tạo được sự yên tâm hoàn toàn cho khách hàng.

4.2. Thực trạng an toàn thông tin tại Việt Nam

Trong thời gian qua, hoạt động đánh cắp thông tin tài chính của khách hàng tại Việt Nam đang ngày càng trở nên bất cập điều này ảnh hưởng lớn cho hệ thống tài chính quốc gia và cá nhân khách hàng. Theo công bố của hãng bảo

mật Kaspersky ngày 19/12/2024, hai quốc gia đứng đầu về các mối đe dọa lây nhiễm trên thiết bị nội bộ trong khu vực trong 6 tháng đầu năm 2024 là Việt Nam và Indonesia. Việt Nam ghi nhận đến hơn 10,5 triệu mối đe dọa. Indonesia xếp thứ hai với hơn 7,95 triệu mối đe dọa. Xếp thứ ba và thứ tư là Thái Lan và Malaysia lần lượt là 2,65 triệu và hơn 1,96 triệu mối đe dọa. Singapore ghi nhận con số thấp nhất với chỉ hơn 500.000 sự cố. Philippines phải đối mặt với gần 700.000 sự cố (Đức Thiện, 2024). Theo Viettel Security (2024), số vụ tấn công liên quan đến lĩnh vực tài chính ngân hàng chiếm 71% trong năm 2024, với 4.000 tên miền lừa đảo trong năm 2024, giảm khoảng 30% so với 2023 tuy nhiên số lượng trang giả mạo, sử dụng thương hiệu trái phép tăng gấp 3 lần so với năm 2023 ở mức 1.200 trang. Công nghệ AI đã được các đối tượng sử dụng trong việc tạo ra các email, website giả nhằm lừa đảo chiếm đoạt tài sản của khách hàng. Gần 40.000 lỗ hổng bảo mật được phát hiện, tăng 46% so với năm 2023, trong đó 47% là các lỗ hổng cao và nghiêm trọng tập trung vào các sản phẩm và dịch vụ phổ biến như hệ thống VPN, máy chủ web và phần mềm quản trị (Viettel Security 2024).

Theo Kaspersky, 6 tháng đầu năm 2024, Việt Nam có 40.102 vụ đánh cắp thông tin đứng thứ ba trong khu vực Đông Nam Á. Các đối tượng thường giả mạo các thương hiệu lớn, ngân hàng để đánh cắp thông tin, số tiền trong tài khoản của khách hàng hàng sau khi đã chiếm quyền truy cập và kiểm soát tài khoản. Nhiều trường hợp các đối tượng sử dụng các công cụ thông minh, trí tuệ nhân tạo, để thực hiện các hành vi phạm pháp (Nguyễn Quỳnh, 2024). Theo CDNetworks, các ngân hàng hiện nay thường đối mặt với hình thức tấn công vào Layer 3/4, Layer

7 DDoS và các ứng dụng web thông qua nhiều phương thức tấn công, hơn 87% các cuộc tấn công có sự kết hợp từ 2 phương thức (Hiếu Phương 2023). Các trải nghiệm của khách hàng cũng bị ảnh hưởng do khả năng kết nối chậm đối với các ứng dụng toàn cầu. Đặc biệt mối đe dọa lớn nhất đến virus như virus Trojan. Khi chúng xâm nhập vào thiết bị của nạn nhân, chúng sẽ chuyển quyền điều khiển về cho tội phạm. Bên cạnh đó, các ứng dụng không mong muốn, có thể vô tình cài đặt trên máy tính hay thiết bị cá nhân dễ dàng mang lại những rủi ro cho khách hàng (Phạm Thị Vân Anh, Trần Thanh Thu, Bạch Đức Khôi Nguyên, 2024).

4.3. Thực trạng bảo mật thông tin trong dịch vụ ngân hàng số tại Việt Nam

4.3.1. Về khung pháp lý

Sự phát triển nhanh của khoa học công nghệ, đặc biệt là ứng dụng vào các dịch vụ của ngân hàng số, đã gây ra cho khách hàng nhiều khó khăn trong việc làm quen với nhưng thay đổi này. Người tiêu dùng dễ dàng bị các vấn đề về chi phí, sự phức tạp của công nghệ cũng như các vấn đề về pháp lý gây khó khăn (World Bank, 2017). Chính vì vậy nguy cơ bị đánh cắp thông tin luôn luôn rình rập. Mặc dù hiện nay có khá nhiều văn bản pháp luật quy định để bảo vệ quyền lợi của khách hàng, người tiêu dùng như: Luật các Tổ chức tín dụng 2010 sửa đổi bổ sung 2017, Nghị định số 117/2018/NĐ-CP, ngày 11/9/2018, Quyết định số 201/QĐ-BTC của Bộ trưởng Bộ Tài chính, Thông tư số 09/2020/TT-NHNN hay Quyết định 2354/QĐ-NHNN của Ngân hàng nhà nước về việc triển khai các giải pháp an toàn, bảo mật trong thanh toán trực tuyến và thanh toán thẻ ngân hàng. Tuy nhiên các quy định của nhà nước hiện nay còn phân tán và gây ra sự chồng chéo, khó tiếp cận, tra cứu khi khách hàng

hay người tiêu dùng các sản phẩm dịch vụ của ngân hàng số có nhu cầu. Bên cạnh đó, những hướng dẫn nhằm giảm thiểu rủi ro của phương thức định danh khách hàng điện tử như: nhận dạng sinh trắc học, chữ ký số hay thực hiện cuộc gọi trực tuyến trong thời gian thực... còn thiếu, đã gây nên những khó khăn cho khách hàng trong việc sử dụng dịch vụ ngân hàng số.

4.3.2. Về hạ tầng cơ sở

Theo thống kê từ Ngân hàng nhà nước tính đến năm 2018, dịch vụ ngân hàng trực tuyến đã được hầu hết các ngân hàng triển khai như Timo Bank của VPBank, Digial Lab của Vietcombank, LiveBank của TPBank, hay Thẻ phi vật lý Ví Việt của LienVietPosstBank.... Hiện hơn 20 ví điện tử đã được ngân hàng nhà nước cấp phép nhằm cung ứng các dịch vụ trung gian thanh toán tại Việt Nam như MoMo, Bankplus, WePay.... Ngoài ra trí tuệ nhân tạo AI đã được nhiều ngân hàng triển khai với giải pháp cơ bản như Chatbot. Theo khảo sát Ngân hàng nhà nước 2025, hiện chỉ có 15% các ngân hàng thương mại ứng dụng AI đạt mức độ trung bình trở lên, điều này còn khá khiêm tốn nếu so sánh với các quốc gia như Hoa Kỳ, Singapore, Trung Quốc hay Thái Lan.

Công nghệ tại hệ thống ngân hàng Việt Nam hiện nay còn thiếu tính đồng bộ. Công nghệ cũ vẫn còn tồn tại ở nhiều ngân hàng. Theo khảo sát từ Ngân hàng nhà nước, các hệ thống thông tin không đồng bộ và lỗi thời vẫn còn tồn tại ở gần 60% các ngân hàng (Trịnh Tường Khiêm, 2024). Để nâng cấp hệ thống công nghệ để đảm bảo bảo mật thông tin cần phải có sự đầu tư lớn, điều này sẽ gây khó khăn cho các ngân hàng nhỏ và vừa với năng lực tài chính hạn chế. Với việc không đáp ứng được các tiêu chuẩn và quy định về bảo mật thông tin của hệ thống ngân hàng đã tạo ra rủi ro về an

ninh, an toàn thông tin khách hàng, an toàn dữ liệu tài chính.

4.3.3. Về nguồn nhân lực.

Nhu cầu về nguồn nhân lực nhằm bảo mật thông tin trong ngành tài chính ngân hàng tại Việt Nam đang gia tăng, đặc biệt trong giai đoạn chuyển đổi số như hiện nay. Bên cạnh nhu cầu tuyển lực nhân lực cho lĩnh vực ngân hàng truyền thống, nhân sự cho mảng ngân hàng số đang được các ngân hàng săn đón, đặc biệt là các vị trí như: kỹ sư trí tuệ nhân tạo (AI), lập trình viên... Theo bà Đặng Trịnh Nhã Hương, Giám đốc khu vực miền Nam, công ty Navigos Search, nhu cầu về nhân sự cho quá trình chuyển đổi số trong lĩnh vực tài chính, ngân hàng Việt Nam hiện đang rất lớn. Các nhà tuyển dụng đang ưu tiên tìm kiếm những nhân lực có trình độ công nghệ nhằm triển khai quá trình chuyển đổi số toàn diện, đặc biệt là những nhân sự có thể mạnh về công nghệ lõi như: AI, Big Data, Blockchain....

Tuy nhiên hiện nay, số lượng nhân lực trong nước có thể đáp ứng được nhu cầu của chuyển đổi số còn hạn chế, nhiều trường hợp các ngân hàng phải tiến hành tìm kiếm nguồn nhân lực từ các nước trong khu vực và trên thế giới. Lực lượng nhân lực về công nghệ thông tin và an ninh mạng còn mỏng là một thách thức lớn với ngành tài chính ngân hàng, ảnh hưởng không nhỏ tới chất lượng, dịch vụ của ngân hàng số. Hiện nay, Bộ Tài chính và Ngân hàng Nhà nước đã có kế hoạch phát triển đội ngũ nhân lực công nghệ thông tin đáp ứng nhu cầu của chuyển đổi số trong lĩnh vực tài chính ngân hàng. Tuy nhiên, đây là quá trình cần tiến hành trong dài hạn với sự vào cuộc của các cấp, các ngành có liên quan.

4.4. Giải pháp nâng cao chất lượng bảo mật thông tin khách hàng cho ngân

hàng số

Trước những thách thức hiện nay trong công tác bảo mật thông tin khách hàng khi sử dụng ngân hàng số ở Việt Nam, cần triển khai đồng bộ một số giải pháp như sau:

4.4.1. Hoàn thiện khung pháp lý

Hệ thống pháp lý cần tiếp tục được hoàn thiện, những quy định trong việc đảm bảo bảo mật thông tin khách hàng cần được cụ thể và mang tính thực tế cao hơn. Căn cứ vào Luật An toàn thông tin mạng số 86/2015/QH13 và Luật An ninh mạng số 24/2018/QH14, từng ngành, từng lĩnh vực, các cơ quan cần xây dựng những văn bản ban hành, hướng dẫn thông tin phù hợp. Ngoài ra Chính phủ cần phối hợp cùng với các bộ, ban ngành xây dựng những văn bản quy định liên bộ, liên ngành về những quy tắc, hướng dẫn chung nhằm tăng cường tính phối hợp và hiệu quả trong việc triển khai đảm bảo an ninh thông tin tài chính.

4.4.2. Phát triển cơ sở hạ tầng

Nhà nước cần có những chính sách hỗ trợ các ngân hàng trong việc đầu tư phát triển cơ sở hạ tầng của ngân hàng số. Nếu máy chủ của ngân hàng bị tấn công hoặc bị sập cần có những phương án xử lý hiệu quả và kịp thời. Bên cạnh đó, hệ thống phòng chống từ xa, đặc biệt là việc chống xâm phạm các vùng thông tin, cần được xây dựng nhằm kịp thời phát hiện và khắc phục các lỗ hổng của hệ thống. Hiện nay, các dữ liệu, thông tin chủ yếu được lưu trữ trên nền tảng đám mây, nếu dữ liệu đám mây bị tấn công thì sẽ dẫn đến rủi ro bị đánh cắp thông tin khách hàng, chính vì vậy giải pháp sử dụng mạng riêng ảo giúp các ngân hàng tạo kết nối an toàn khi tham gia vào mạng chung hoặc mạng riêng do một đơn vị khác sở hữu. Đồng thời, hệ thống mạng này giúp bảo vệ dữ

liệu, thông tin khách hàng cũng như giấu địa chỉ IP thật.

4.4.3. Xây dựng và nâng cao chất lượng nguồn nhân lực

Tập trung xây dựng và nâng cao chất lượng nguồn nhân lực có trình độ, nhằm xử lý các vấn đề về an ninh thông tin. Đây được coi là nhiệm vụ cần phải ưu tiên hàng đầu. Sự thiếu hụt về đội ngũ nhân lực cũng như yếu kém về trình độ trong công tác quản lý thông tin, xử lý tình huống khi những rủi ro về bảo mật thông tin khách hàng xảy ra sẽ dẫn tới những hậu quả nặng nề. Một trong những giải pháp là thuê chuyên gia của bên thứ ba để hỗ trợ nhưng điều này đòi hỏi chi phí sẽ cao, ngoài ra mức độ đáp ứng của đội ngũ chuyên gia này khi sự cố xảy ra có thể chưa cao vì thiếu sự hiểu biết toàn diện về hoạt động của tổ chức, hơn nữa đạo đức nghề nghiệp cũng là một vấn đề mà doanh nghiệp cần lưu tâm. Do đó, xây dựng lực lượng nhân sự của chính ngân hàng với đầy đủ năng lực, chuyên môn là nhiệm vụ cấp thiết và cần phải thực hiện một cách thường xuyên, liên tục.

V. Kết luận

Bảo mật thông tin khách hàng đang trở thành một nhiệm vụ chính yếu không chỉ của ngành ngân hàng mà còn của quốc gia. Nhiệm vụ này cần có những chiến lược cụ thể với sự phối hợp, vào cuộc của các bên có liên quan. Bài viết đã làm rõ một số vấn đề của công tác đảm bảo an ninh thông tin mà ngành ngân hàng hiện nay đang gặp phải trong môi trường số. Bài viết cũng đề xuất một số giải pháp nhằm giảm thiểu rủi ro trong công tác bảo mật thông tin khách hàng. Bên cạnh một khung pháp lý rõ ràng, tránh chồng chéo cùng với những văn bản hướng dẫn cụ thể, cần kết hợp với công tác nâng cao cơ sở hạ tầng kỹ thuật và phát triển chất lượng đội

nguồn nhân lực là những giải pháp cần tập trung xử lý và triển khai một cách có hệ thống và đồng bộ hiện nay.

Tài liệu tham khảo:

- [1]. Đại Hùng. (2025). AI Agent: Xu hướng công nghệ mới, thực tiễn quốc tế và giải pháp áp dụng trong lĩnh vực ngân hàng tại Việt Nam. *Tạp chí Ngân hàng*. <https://tapchinganhang.gov.vn/ai-agent-xu-huong-cong-nghe-moi-thuc-tien-quoc-te-va-giai-phap-ap-dung-trong-linh-vuc-ngan-hang-tai-viet-nam-15825.html>
- [2]. Đức Thiện. (2024). Việt Nam đứng đầu Đông Nam Á về mã độc lây nhiễm qua thiết bị lưu trữ. *Tuổi Trẻ Online*. <https://tuoitre.vn/viet-nam-dung-dau-dong-nam-a-ve-ma-doc-lay-nhiem-qua-thiet-bi-luu-tru-20241219175037822.htm>
- [3]. Gibson, B. (1992). Financial Information for Decision Making: An Alternative Small Firm Perspective. *Journal of Small Business Finance*, 1(3), 221-232. <https://doi.org/10.57229/2373-1761.1123>
- [4]. Hiếu Phương. (2023). CDN networks giới thiệu giải pháp, công nghệ an ninh đa lớp cho ngành ngân hàng, tài chính. *Tạp chí Kinh tế và Dự báo*. <https://kinhtevadubao.vn/cdn-networks-gioi-thieu-giai-phap-cong-nghe-an-ninh-da-lop-cho-nganh-ngan-hang-tai-chinh-27275.html>
- [5]. Honggowati, S., Aryani, Y. A., & Rahmawati, R. (2015). Value Relevance of Financial and Non-Financial Information to Investor decision. *Global Business and Finance Review*, 20(2), 95-104. <https://doi.org/10.17549/gbfr.2015.20.2.95>
- [6]. Kang, J. (2018). Mobile payment in Fintech environment: trends, security challenges, and services. *Human-centric Computing and Information Sciences*, 8(32), 1-16. <https://doi.org/10.1186/s13673-018-0155-4>
- [7]. Linh Anh. (2024). Ngân hàng nâng cấp công nghệ bảo mật, kịp thời ngăn chặn tội phạm công nghệ và lừa đảo. *Tạp chí Ngân hàng*. <https://tapchinganhang.gov.vn/ngan-hang-nang-cap-cong-nghe-bao-mat-kip-thoi-ngan-chan-toi-pham-cong-nghe-va-lua-dao-9257.html>
- [8]. Lundgren, B., & Moller, N. (2017). Defining information security. *Science and Engineering Ethics*, 25(2), 419-441. <https://doi.org/10.1007/s11948-017-9992-1>
- [9]. Nguyễn Thanh Nguyên. (2024). An toàn dữ liệu cá nhân trong hệ thống ngân hàng thương mại Việt Nam. *Tạp chí Tài chính*. <https://tapchitaichinh.vn/an-toan-du-lieu-ca-nhan-trong-he-thong-ngan-hang-thuong-mai-viet-nam.html>
- [10]. Ogbanufe, O. (2021). Enhancing end-user roles in information security: Exploring the setting, situation, and identity. *Computer & Security*, 108, 102340. <https://doi.org/10.1016/j.cose.2021.102340>
- [11]. Phạm Thị Vân Anh, Trần Thanh Thu, & Bạch Đức Khôi Nguyên. (2024). Tăng cường an ninh thông tin tài chính trong môi trường số - Thực trạng và hàm ý chính sách cho Việt Nam. Học viện Tài chính, Việt Nam.
- [12]. PGS. TS. Lê Hoàng Nga. (2022). *Phát triển dịch vụ ngân hàng số trong các ngân hàng thương mại Việt Nam*. Đại học Thành Đông.
- [13]. Reid, R., & Van Niekerk, J. (2014). From information security to cyber security cultures. *Proceeding of Information Security for South Africa*, Johannesburg, South Africa, 1-7. <https://doi.org/10.1109/ISSA.2014.6950492>
- [14]. ThS. Lương Thanh Bình. (2024, tháng 7). Hoàn thiện khung pháp luật về ngân hàng số tại Việt Nam. *Tạp chí Kinh tế và Dự báo*, (14). <https://kinhtevadubao.vn/hoan-thien-khung-phap-luat-ve-ngan-hang-so-tai-viet-nam-29794.html>
- [15]. ThS. Phạm Thị Hồng Tâm, ThS. Trần Linh Huân, & Đặng Thị Ngọc H. (2023). Bảo mật thông tin khách hàng khi sử dụng dịch vụ ngân hàng số - Thực trạng và một số kiến nghị. *Tạp chí Ngân*

- hàng. <https://tapchinganhang.gov.vn/bao-mat-thong-tin-khach-hang-khi-su-dung-dich-vu-ngan-hang-so-thuc-trang-va-mot-so-kien-nghi-9421.html>
- [16]. TS. Trần Thị Thu Hà & TS. Nguyễn Thị Thu Thoa. (2024). Phòng, chống tội phạm công nghệ cao ở các ngân hàng thương mại. *Trường Đại học Công Thương TP. Hồ Chí Minh*. <https://www.quanlynhanuoc.vn/2024/09/12>
- [17]. Viettel. (2024). *Viettel công bố Báo cáo An ninh mạng 6 tháng đầu năm*. <https://viettel.com.vn/vi/tin-tuc-va-su-kien/tin-tuc/viettel-cong-bo-bao-cao-tinh-hinh-an-ninh-mang-tai-viet-nam-nam-2024/>
- [18]. Viettel. (2025). *Viettel công bố Báo cáo tình hình An ninh mạng tại Việt Nam năm 2024*. <https://viettel.com.vn/vi/tin-tuc-va-su-kien/tin-tuc/viettel-cong-bo-bao-cao-tinh-hinh-an-ninh-mang-tai-viet-nam-nam-2024/>
- [19]. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102. <https://doi.org/10.1016/j.cose.2013.04.004>

DEVELOPMENT IN SECURING CUSTOMER INFORMATION OF DIGITAL BANKING SERVICES IN VIETNAM

Tran Van Hai², Nguyen Ba Tung²

Abstract: *The fourth industrial revolution has brought about profound changes in many areas such as education, health, culture, society, economy, including the banking and finance sector. Thanks to the development of science and technology, banking products and services are increasingly diverse, meeting the needs of customers. Besides traditional banking, digital banking services were born as an inevitable thing to improve product quality as well as maximize profits. However, the problem of customers' security information in digital banking services is currently occurring at an alarming frequency. High-tech criminals are taking advantage of loopholes in management and limitations of technical infrastructure to conduct fraudulent activities and appropriate customers' assets. The article will focus on clarifying the achievements and challenges that need to be resolved, thereby proposing solutions to contribute to improving customer information security in digital banking services. The article is conducted based on qualitative research methods through secondary data sources in the past 5 years. Issues relating to legal framework, information infrastructure and human resources will be analyzed and clarified through the article.*

Keywords: *Digital banking, security, information, customers, legal framework, information infrastructure, human resources*

² Faculty of Finance and Banking, Hanoi Open University