AN TOÀN, BẢO MẬT TRONG GIAO DỊCH NGÂN HÀNG TRỰC TUYẾN TẠI LIÊN BANG NGA

*TS. Nguyễn Đình Trung**

Bài viết bàn về một số khía cạnh trong xây dựng và triển khai chiến lược số hóa nhằm mở rộng và nâng cao chất lượng dịch vụ ngân hàng, đảm bảo khả năng tiếp cận và bảo mật của ngân hàng trực tuyến (Internet Banking), một trong những phương thức phục vụ khách hàng từ xa phổ biến nhất tại Liên bang Nga. Mô hình quan hệ kinh tế mới cho thấy sự cần thiết phải hình thành một mô hình kinh doanh điện tử độc lập, trong đó, các sản phẩm chủ yếu của ngân hàng được cung cấp qua Internet và mạng vật lý đóng vai trò là người chuyển phát nhanh.

Trong bối cảnh phát triển nhanh chóng của các công nghệ ngân hàng mới, chìa khóa để duy trì vị thế hàng đầu của ngân hàng trong môi trường cạnh tranh là nâng cao chất lượng dịch vụ ngân hàng từ xa (Remote/ Distance Banking Services, RBS), đảm bảo khả năng tiếp cận và mở rộng các dịch vụ ngân hàng trực tuyến, thực hiện một loạt các biện pháp để đảm bảo an toàn, bảo mật của dịch vụ cung cấp, một trong những thành phần quan trọng của chiến lược số hóa.

Dịch vụ ngân hàng từ xa (RBS) là tên gọi chung của phương thức cung cấp dịch vụ ngân hàng cho khách hàng (cả pháp nhân và cá nhân) sử dụng phương tiện viễn thông (thường là điện thoại, Internet) mà không cần trực tiếp đến ngân hàng.

Ngày nay, chỉ với một trang web, khả năng kết nối với ngân hàng trực tuyến và cung cấp dịch vụ thông qua các thiết bị đầu cuối là không đủ để cạnh tranh thành công trên thị trường sản phẩm và dịch vụ tài chính đang phát triển nhanh chóng.

Các ngân hàng hiểu rằng khách hàng, trước hết, quan tâm đến các dịch vụ Internet chất lượng cao. Các tổ chức tín dụng không lớn đang tích cực triển khai các giải pháp nền tảng, còn các tổ chức tín dụng lớn thì tập hợp các nhóm chuyên gia của họ để "chạy đua vũ trang" trong lĩnh vực chức năng, năng lực và tiện ích sử dụng.

Việc công bố các nghiên cứu và đánh giá RBS tạo động lực thúc đẩy các thành viên tham gia thị trường. Vị trí trong bảng xếp hạng trở thành một trong những chỉ số hiệu quả chủ chốt cho các bộ phận cung cấp RBS, là thông số rõ ràng nhất phản ánh hoạt động nhóm dự án. Để đánh giá hiệu quả dịch vụ, các chỉ tiêu sau đây có thể được sử dụng:

- Số lượng khách hàng đang hoạt động (định nghĩa được hầu hết các ngân hàng chấp nhận: khách hàng sử dụng dịch vụ ít nhất một lần một quý, thực hiện giao dịch);

- Tỉ trọng khách hàng sử dụng RBS (so với tổng số khách hàng của ngân hàng);

- Thu nhập từ RBS [1].

Mô hình của ngân hàng số cũng đã thay đổi rõ rệt. Nếu một vài năm trước đây, các thành phần kỹ thuật và hoạt động được đề cập nhiều hơn - chuyển đổi các nghiệp vụ truyền thống, tăng cường các tính năng của dịch vụ, phát triển ứng dụng di động,... giờ đây, hoạt động marketing (tiếp thị) được đưa lên hàng đầu - thu hút khách hàng qua mạng, bán chéo sản phẩm qua Internet Banking và các ứng dụng di động, cũng như tương tác với khách hàng thông qua e-mail, SMS, mạng xã hội.

Mô hình mới cho thấy sự cần thiết phải tạo ra một ngân hàng điện tử (trực tuyến) độc lập, trong đó, các sản phẩm chính của ngân hàng - các khoản cho vay và tiền gửi - được cung cấp qua Internet và mạng vật lý đóng vai trò là người chuyển phát nhanh, cung cấp các hợp đồng và thẻ.

Nhu cầu ngày càng tăng của người tiêu dùng đối với các dịch vụ thông qua Internet Banking được minh chứng bằng số liệu thống kê trong bảng 1.

Bảng 1 cho thấy, xu hướng thanh toán điện tử qua Internet ngày càng trở nên phổ biến và gia tăng cả về giá trị lẫn số lượng giao dịch: giao dịch thanh toán bằng phương tiện điện tử thông qua Internet chiếm một tỉ trọng đáng kể (quý I năm 2020 - chiếm 48.6 %, với 454 triệu giao dịch); trong giai đoạn 2017 - 2020, những con số này đang tăng trưởng đều đặn, tuy nhiên, về giá trị, các chỉ tiêu này còn cao hơn nhiều, theo đó, giá trị giao dịch thanh toán điện tử qua Internet chiếm hơn 86% doanh số thanh toán điện tử, với trên 128 nghìn tỷ RUB, tăng 42.7% so với cùng kì năm 2017.

Mặc dù có những lợi thế rõ ràng của RBS (tiện lợi, dễ tiếp cận, kịp thời, hiệu quả, lợi nhuận,...), song, không thể không tính đến một số

* Đại học Đại Nam

Bảng 1: Dữ liệu thanh toán điện tử của khách hàng các tổ chức tín dụng

	Số giao dịch thanh toán điện tử					Giá trị giao dịch thanh toán điện tử				
	Tổng số, triệu đơn vị	Tăng trưởng, %	Trong đó, thông qua Internet, triệu đơn vị	Tỉ trọng thanh toán qua Internet	Tăng trưởng, %	Tổng số, tỉ RUB	Tăng trưởng, %	Trong đó, thông qua Internet, tỉ RUB	Tỉ trọng thanh toán qua Internet, %	Tăng trưởng, %
QI 2020	933	23	454	48.6	31	148287	9.7	128237	86.4	14
QI 2019	757	14	347	46	9.8	135118	10.2	112564	83	14
QI 2018	664	13.5	315.7	47.5	17	122568	11	103427	84	15
QI 2017	585	-8.1	269.6	46	14	110470	1.6	89850	81	2

Nguồn: Ngân hàng Nga

nhược điểm sau đây [2;3;4;5]:

Một là, vấn đề xuyên suốt những năm gần đây là mức độ an toàn và bảo mật thông tin không đầy đủ: còn yếu trong khâu tổ chức bảo mật các khoản thanh toán và tài sản của khách hàng trong các tài khoản. Các chuyên gia cho rằng, vấn đề liên quan đến trộm cắp dữ liệu cá nhân và tội phạm mạng sẽ còn kéo dài trong một thời gian dài.

Gần đây, thủ đoạn đánh cắp tiền phổ biến nhất là gửi tin nhắn SMS hoặc gửi thư cho khách hàng nhân danh ngân hàng.

Hiện nay, chưa thể loại trừ các thủ đoạn lừa đảo như lập các trang web lừa đảo, giống hệt hệ thống Internet Banking, và làm giả chữ ký số của khách hàng thông qua các phương tiện khác nhau...

Tất nhiên, để hạn chế rủi ro lừa đảo này, các ngân hàng tích cực tìm kiếm những biện pháp loại bỏ chúng thông qua sử dụng các giải pháp bảo mật mới nhất trong lĩnh vực đảm bảo an toàn và bảo mật thanh toán qua Internet; các cơ quan quản lý vĩ mô ban hành các quy định, tạo hành lang pháp lý để điều chỉnh, quản lý và giám sát dịch vụ thanh toán điện tử qua Internet.

Hai là, một nguyên nhân quan trọng của hạn chế nêu trên là do thiếu một hành lang pháp lý thống nhất về sử dụng Internet Banking. Mặc dù kênh phân phối RBS đã phát triển mạnh và sự quan tâm với kênh phân phối này từ ngân hàng và khách hàng cũng ngày càng tăng, những khoảng trống pháp lý và thiếu định nghĩa chính thức vẫn là một thiếu sót nghiêm trọng.

Trong Công văn số 36-T, ngày 31 tháng 3 năm 2008 của Ngân hàng Nga "Về những khuyến nghị tổ chức quản trị rủi ro phát sinh từ việc thực hiện các nghiệp vụ có sử dụng hệ thống tại tổ chức tín dụng" có đưa ra định nghĩa về Internet Banking, tuy nhiên, chỉ mang tính khuyến nghị.

Trong Luật liên bang số 395-1 "Về Ngân hàng và hoạt động ngân hàng" ngày 02/02/1990, chưa đề cập đến thuật ngữ dịch vụ ngân hàng từ xa và Internet Banking.

Vì vậy, tại thời điểm này, những vấn đề bảo mật quan trọng đối với Internet Banking chỉ được phản ánh trong một số quy định mang tính chất khuyến nghị. Đây là điều không thể chấp nhận được trong điều kiện ứng dụng rộng rãi công nghệ dữ liệu và rất nhiều rủi ro phát sinh đi kèm.

Rõ ràng, trước hết, các nguyên tắc cơ bản trong cung cấp RBS nói chung, Internet Banking nói riêng và các tính năng của chúng cần được quy định trong Luật liên bang "Về Ngân hàng và hoạt động ngân hàng".

Ba là, lỗi kỹ thuật là một vấn đề phụ thuộc rất nhiều vào số lượng người dùng và tải hệ thống. Tuy nhiên, trong một số trường hợp, vấn đề này có liên quan đến dịch vụ, mà một sản phẩm cụ thể sẽ được cung ứng và sự cần thiết phải thực hiện các nghiệp vụ kỹ thuật, ứng dụng các tính năng bổ sung và phát triển phần mềm.

Do lỗi kỹ thuật, khách hàng không thể thực hiện các giao dịch (hoặc phải lặp lại nhiều lần), hoặc không sử dụng được khả năng tiếp cận từ xa để quản lý tài khoản. Những vấn đề này có thể ảnh hưởng xấu đến hình ảnh của ngân hàng [6].

Ngoài sự cố kỹ thuật trong cung cấp dịch vụ ngân hàng, cũng có thể xảy ra những sự cố tại các trung gian mà khách hàng có thể sử dụng dịch vụ của họ khi sử dụng dịch vụ ngân

hàng. Những trung gian đó có thể là nhà cung cấp dịch vụ Internet hoặc nhà cung cấp dịch vụ di động. Chất lượng dịch vụ mà khách hàng nhận được phụ thuộc vào chất lượng dịch vụ của các trung gian.

Ví dụ, khách hàng của ngân hàng không nhận SMS để xác nhận đăng nhập ngân hàng trực tuyến hoặc tiến hành các giao dịch gây ra những khó khăn nhất định; đường truyền chậm không cho phép tải trang web hoặc tăng thời gian thực hiện giao dịch gây ra một ấn tượng tiêu cực về dịch vụ được cung cấp [7].

Bốn là, sự phức tạp của giao diện được thiết kế cho Internet Banking. Cần lưu ý rằng, thông thường, các ngân hàng mua phần mềm có sẵn và không tập trung vào những chuyện như sự đơn giản và dễ hiểu khi thực hiện thanh toán qua ngân hàng, trong khi đó, khách hàng đối mặt với một vấn đề như sự phức tạp trong thực hiện các khoản thanh toán qua ngân hàng đơn giản nhất.

Trong một số trường hợp, độ phức tạp của sản phẩm phần mềm buộc khách hàng phải đi sâu vào hướng dẫn sử dụng và các khuyến nghị của nhà cung cấp phần mềm. Thế là, Internet Banking bắt đầu được nhìn nhận một cách tiêu cực, và ngân hàng không được coi là một doanh nghiệp mang lại lợi nhuận, mà như một phương thức cung cấp dịch vụ [8].

Năm là, khách hàng thiếu thông tin về công nghệ mới và phương pháp bảo vệ mình trước các hoạt động lừa đảo. Nhược điểm này chủ yếu liên quan đến thái độ của chính tổ chức tín dụng đối với ngân hàng trực tuyến như một dịch vụ đi kèm. Mô hình kinh doanh chi nhánh dẫn đến thực tế, do thiếu thông tin, khách hàng hoặc đơn giản là không sử dụng dịch vụ, hoặc rơi vào tay những kẻ lừa đảo sau khi trải nghiệm bài học tiêu cực và từ chối sử dụng dịch vụ sau này.

Sáu là, khả năng kỹ thuật hạn chế của các dịch vụ điện tử vẫn còn "nóng" cho đến ngày hôm nay. Sự phát triển hệ thống viễn thông trong nước không đồng đều khiến người sử dụng thiếu các kênh truyền dữ liệu giá rẻ, có thể đảm bảo hiệu suất hoạt động bình thường của công nghệ ngân hàng trực tuyến. Do đó, khách hàng buộc phải sử dụng các kênh điện thoại di động để truy cập tài khoản cá nhân, từ đó, tốc độ thực hiện giao dịch và một phần tính năng hệ thống bị giảm đi.

Giải pháp các vấn đề nêu trên đòi hỏi ngân hàng phải thực hiện các khoản đầu tư tài chính nghiêm túc nhằm: (i) cải tiến công nghệ truyền dữ liệu, nghiên cứu sở thích của người tiêu dùng, thay đổi chức năng và giao diện; (ii) phát triển và thực hiện các chiến dịch quảng cáo và truyền thông tốn kém, mà trong điều kiện khủng hoảng, vượt quá khả năng chịu đựng đối với nhiều tổ chức tín dụng, nếu xét trên các tiêu chí về tính kinh tế.

Liên quan đến vấn đề bảo đảm an toàn và bảo mật thông tin, hậu quả của những vấn đề chưa được giải quyết không chỉ có tác động tiêu cực cho hình ảnh của ngân hàng, mà còn tác động xấu đến các chỉ tiêu tài chính của ngân hàng.

Theo báo cáo của Tập đoàn an ninh mạng đa quốc gia Group-IB, hằng năm, quy mô các cuộc tấn công theo mục tiêu (targeted attacks) đối với các ngân hàng càng gia tăng (tấn công DDoS, spam,...).

Cài đặt các hệ thống bảo mật đáng tin cậy hơn sẽ tốn kém nhiều hơn, nhưng rõ ràng, không còn cách nào khác, các ngân hàng cần phải đi theo hướng này.

Ngày nay, xác thực một yếu tố sẽ rất dễ dàng bị vượt qua bởi những kẻ xâm nhập: mọi thứ cần cho vấn đề này là - một chương trình "keylogger" đơn giản để ghi lại và kiểm soát các thông tin đưa vào từ bàn phím.

Một mặt, sự gia tăng số lượng ngân hàng sử dụng hệ thống xác thực hai yếu tố sẽ làm tăng số lượng phần mềm độc hại có thể vượt qua phương pháp bảo vệ như vậy. Điều này có nghĩa là, ứng dụng rộng rãi xác thực hai yếu tố sẽ không mang lại hiệu quả lâu dài, mà chỉ tạo dư địa cho những người tạo ra phần mềm tài chính độc hại.

Mặt khác, cần lưu ý rằng hầu hết các ngân hàng hiện đang sử dụng hệ thống xác thực hai yếu tố đã không thiết lập nó ở mức độ bảo vệ tối đa. Ngoài ra, công nghệ này có nhược điểm nghiêm trọng: mặc dù khu vực Internet Banking được bảo vệ, nhưng lại khó có thể kiểm soát kịp thời được những gì xảy ra trong khu vực này. Để tăng cường bảo mật, đòi hỏi các phương pháp kiểm soát bổ sung như sử dụng thiết bị mã hóa xác thực (mã thông báo, token) hoặc tin nhắn SMS. Thông qua những phương thức xác thực này, có thể thiết lập giới hạn thời hạn hiệu lực của mã xác thực, số tài khoản có thể được truy cập để giao dịch, số tiền giao dịch tối đa được phép. Trong những năm gần đây, công nghệ sinh trắc học - công nghệ sử dụng những thuộc tính vật lý, những đặc điểm sinh học của cá nhân như vân tay, khuôn mặt, mống mắt, tĩnh mạch… để nhận diện, xác thực đã có những bước tiến đáng kể, góp phần tăng cường bảo mật và có thể trở thành xu hướng phát triển tất yếu trong thời gian tới.

Công ty nghiên cứu quốc tế Aite Group đã tiến hành phân tích an toàn và bảo mật thông tin của các ngân

hàng cũng như giám sát các mối đe dọa hiện có. Kết quả cho thấy hiện nay, hằng ngày, có đến 10.000 mối đe dọa mới. Các nhà nghiên cứu nhấn mạnh, 50% các loại phần mềm độc hại mới đang được phát triển để thực hiện các hoạt động gian lận trong lĩnh vực ngân hàng điện tử.

Theo D. Katkov, người đứng đầu Văn phòng đấu tranh chống tội phạm trong lĩnh vực tài chính - tín dụng của Bộ Nội vụ Nga, năm 2015, tỉ trọng các sự cố máy tính với tổn thất tài chính dưới 100 nghìn RUB, chiếm 90%. Những sự cố tương tự với tổn thất tài chính lớn (vài chục triệu RUB) xảy ra không nhiều, tuy nhiên, chúng chiếm 90% giá trị tổn thất.

Trong lĩnh vực tài chính - tín dụng, năm 2015, đã phát hiện 342 tội phạm theo Điều 159.3 Bộ luật Hình sự của Liên bang Nga "Thực hiện gian lận trong thanh toán Thẻ", đã thực hiện điều tra sơ bộ 239 trường hợp. Và 1.030 tội phạm theo quy định bởi Điều 159.6 của Bộ luật Hình sự Liên bang Nga "Gian lận trong lĩnh vực thông tin máy tính" đã được tin báo, trong đó, đã điều tra sơ bộ 151 trường hợp. Nghĩa là, tỷ lệ xử lý tội phạm máy tính còn thấp.

Điều đáng chú ý là các số liệu thống kê chưa phản ánh tình hình thực tế vì mức độ án của các tội phạm này khá cao. Thực tiễn cho thấy rằng, các thông báo về hành vi trộm cắp tiền trên các tài khoản không tiền mặt chủ yếu xuất phát từ các tổ chức tín dụng lớn có uy tín lâu dài. Phần còn lại không muốn thu hút sự chú ý đến các đặc thù công việc của họ, thông thường - do có những hành vi vi phạm pháp luật, trong đó, có việc sử dụng tài khoản thẻ và ATM để thực hiện các giao dịch tài chính bất hợp pháp.

Theo báo cáo thường niên của Group-IB, năm 2015, số vụ tấn công vào ATM cũng tăng lên, cũng như các "Mobile Trojans" nhằm mục đích lây nhiễm các thiết bị cá nhân. Trong báo cáo của mình, Group-IB cho thấy hành vi trộm cắp từ điện thoại thông minh của khách hàng tăng 35 lần so với các thủ đoạn lừa đảo truyền thống (bảng 2).

Theo Ngân hàng Nga, năm 2019, khách hàng của các ngân hàng Nga đã bị đánh cắp 6.4 tỉ RUB (hơn 100 triệu USD theo tỉ giá cuối năm 2019); các ứng dụng ngân hàng trực tuyến và điện thoại di động bị tin tặc tấn công 160.8 nghìn lần với tổng thiệt hại 2.27 tỉ RUB (khoảng 372 nghìn USD).

Thông thường, các tổ chức tín dụng cố gắng thiết lập hệ thống bảo mật thông tin trong phạm vi giới hạn các mối đe dọa có thể xảy ra. Mục tiêu chính là bảo vệ những thông tin tiềm năng có giá trị của ngân hàng từ các đối thủ cạnh tranh. Một số nghiên cứu cho thấy, để giữ chân khách hàng và thu hút khách hàng mới khi xây dựng hệ thống bảo mật thông tin, ngân hàng cần tính đến một số đặc điểm đòi hỏi những yêu cầu bảo mật cao hơn trong tổ chức bảo mật các khoản thanh toán trực tuyến.

(1) Thông tin được ngân hàng xử lý và lưu trữ, có nội dung tài chính, do đó, nhận được sự quan tâm nhiều hơn của những kẻ lừa đảo. Vì vậy, cần phải sẵn sàng đối phó thường xuyên với các thủ đoạn đánh cắp dữ liệu.

(2) Các thông tin được lưu trữ và xử lý trong ngân hàng là vô cùng lớn, do đó, bảo mật không đầy đủ khiến tổ chức tín dụng có nguy cơ mất hình ảnh và uy tín trước khách hàng.

(3) Việc truy cập 24/24 của khách

Bảng 2: Đánh giá tội phạm công nghệ cao trên phân đoạn thị trường Nga

Phân đoạn thị trường Nga	Số nhóm tội phạm	Số lần tấn công thành công/ ngày	Số tiền bị lấy cắp bình quân/ lần (nghìn RUB)	Số tiền bị lấy cắp/ ngày (nghìn RUB)	Số tiền bị lấy cắp từ quý I 2014 - quý 1 2015 (nghìn RUB)
Lấy cắp từ tài khoản tổ chức qua Internet Banking	8	16	480	7680	1912320
Lấy cắp từ tài khoản cá nhân qua Internet Banking	2	2	76.5	153	38097
Lấy cắp từ tài khoản cá nhân bằng Adroid Trojans	14	70	3.5	245	61005
Tấn công theo mục tiêu vào ngân hàng	3	-	90000	-	638000

Nguồn: Group - IB

hàng vào tài khoản ngân hàng làm tăng xác suất thâm nhập vào hệ thống ngân hàng của những kẻ xấu.

(4) Số lượng người dùng lớn làm tăng số lượng các tình huống khẩn cấp, do đó, hệ thống an toàn, bảo mật cần sẵn sàng để xử lý chúng.

Bốn đặc điểm nêu trên cho phép xác định hai cấp độ nhiệm vụ đối với hệ thống bảo mật thông tin của Internet Banking.

Thứ nhất, các nhiệm vụ phân tích liên quan đến lập kế hoạch, tiến hành các nghiên cứu khác nhau về tài khoản,... Nội dung này không mang tính tức thời và không yêu cầu các quyết định chớp nhoáng, nhưng kết quả có ảnh hưởng ngay đến việc xây dựng hoặc cập nhật chính sách bảo mật ngân hàng đối với một mối đe dọa hoặc lỗ hổng cụ thể.

Thứ hai, các nhiệm vụ hiện tại phát sinh trong hoạt động hàng ngày của ngân hàng, ví dụ, tổ chức thanh toán hoặc các nghiệp vụ liên quan đến điều chỉnh tài khoản. Giá trị của thông tin này có tính thời điểm và theo thời gian, sẽ mất đi tính cấp thiết. Do đó, các tổ chức tín dụng cần cố gắng bằng mọi cách đảm bảo an toàn, bảo mật quá trình thông tin tại thời điểm thực hiện các giao dịch tài chính một cách liên tục.

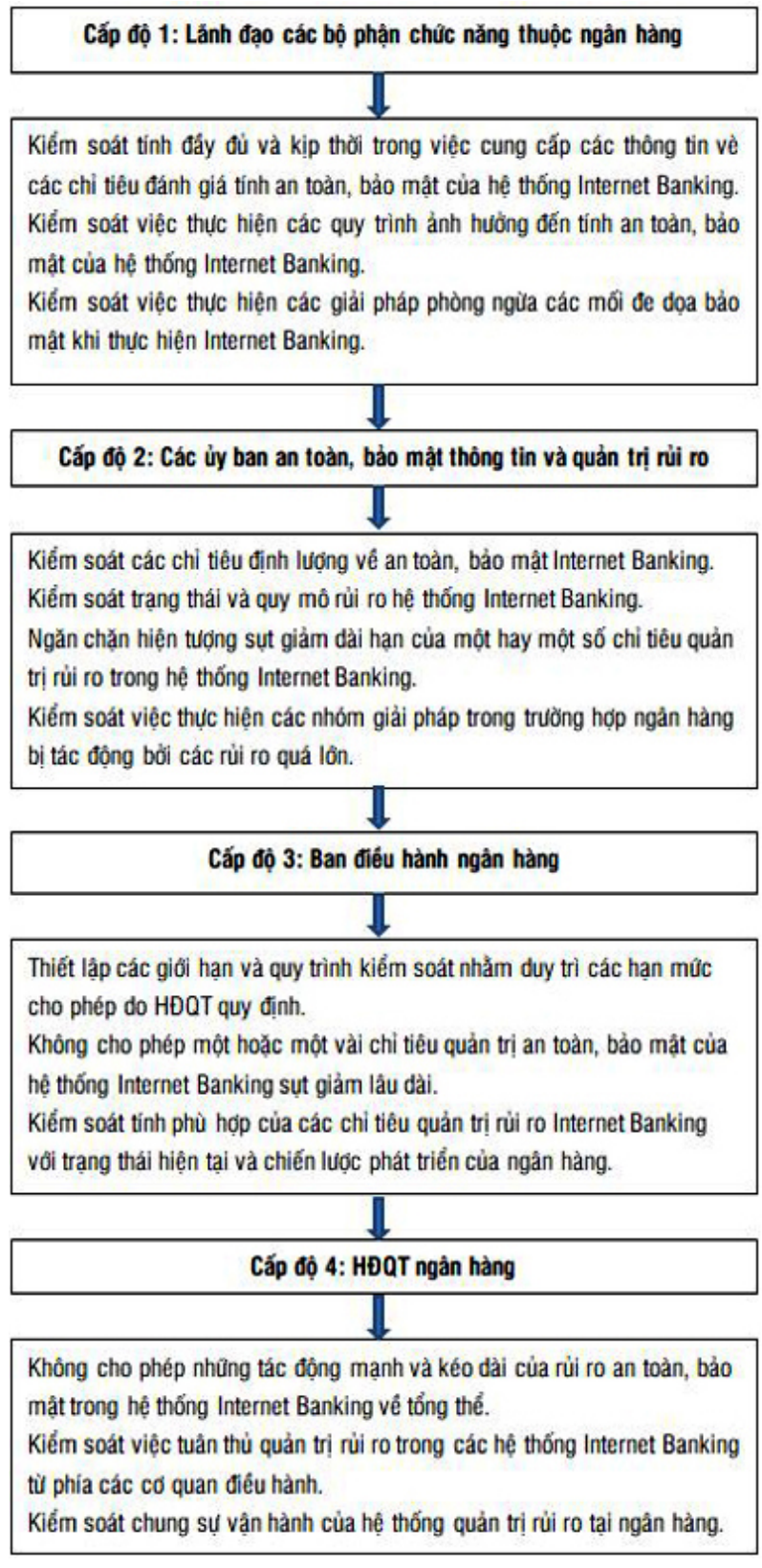
Giải pháp cho các nhiệm vụ này chỉ khả thi khi trách nhiệm của các bộ phận ngân hàng trong lĩnh vực đảm bảo an toàn và kiểm soát an ninh các công nghệ Internet được quy định chặt chẽ.

Do đó, một thành phần không thể thiếu trong chính sách bảo mật hiệu quả đối với lĩnh vực Internet Banking là phân định trách nhiệm và quyền hạn tương ứng giữa các bộ phận và con người một cách rõ ràng, hợp lý [7].

Trên cơ sở hệ thống hóa thực tiễn hoạt động ngân hàng trong lĩnh vực giám sát rủi ro Internet Banking, một hệ thống hiệu quả và phổ biến nhất được đề xuất trong hình 1.

Mức độ phối hợp cao giữa các bộ phận chịu trách nhiệm bảo mật hệ thống Internet Banking là chìa khóa đảm bảo cho một chính sách bảo mật hiệu quả đối với các khoản thanh toán trực tuyến. Trước hết, tính hiệu quả có được là nhờ quá trình cập nhật liên tục các thủ đoạn gian lận và các mối đe dọa mới, đi kèm với đó là sự đa dạng các tình huống khẩn cấp, đòi hỏi có những quyết định ngay lập tức.

Hình 1: Các cấp độ kiểm soát rủi ro trong lĩnh vực bảo mật Internet Banking



Mặc dù hiện có nhiều phương pháp để đảm bảo an toàn, bảo mật thông tin cho Internet Banking, nhưng vẫn còn nhiều vấn đề liên quan đến rủi ro khi thực hiện các giao dịch thanh toán qua Internet. Dưới đây là một số vấn đề chủ yếu:

Thứ nhất, vấn đề cơ bản trong tổ chức bảo mật thông tin của ngân hàng là khả năng đối phó kịp thời với những nguy cơ nhiễm mã độc của hệ thống và khả năng phục hồi hệ thống Internet Banking sau sự cố tấn công.

Những mối đe dọa này có thể được vô hiệu hóa thông qua các giải pháp phần mềm, thành lập các trung tâm dự phòng của hệ thống với khả năng phục hồi tự động, cũng như thông qua các phương tiện kỹ thuật, sử dụng các nguồn cung cấp năng lượng liên tục. Tuy nhiên, trong điều kiện khủng hoảng kinh tế, các tổ chức tín dụng tìm cách giảm chi phí với thời gian hoàn vốn dài, do vậy, vấn đề bảo mật không được đưa lên hàng đầu.

Thứ hai, một vấn đề quan trọng không kém khác là phân định quyền truy cập của khách hàng đối với thông tin được lưu trữ và xử lý trong hệ thống ngân hàng. Để kiểm soát truy cập ngân hàng, thường sử dụng các ứng dụng phần mềm; đôi khi, có thể được thay thế bởi các phần mềm chống virus và tường lửa bảo vệ. Các ngân hàng lớn có xu hướng sử dụng các giải pháp phần mềm do họ tự phát triển, nhưng các ngân hàng nhỏ hơn thường sử dụng các phần mềm của bên thứ ba. Tuy nhiên, trên thị trường, thị phần phần mềm quản lý truy cập có chứng chỉ đáp ứng các yêu cầu của các cơ quan có thẩm quyền chiếm tỉ lệ rất nhỏ (ở Nga, khoảng 5%); vì vậy, độ tin cậy của chúng là vấn đề còn bỏ ngỏ. Một tỉ lệ thấp như vậy có lý do là để thiết kế, phát triển và nhận được giấy chứng nhận tương thích, đáp ứng các yêu cầu của cơ quan có thẩm quyền, các nhà phát triển phải đầu tư rất nhiều vốn tài chính và thời gian.

Thứ ba, khi nhận và truyền dữ liệu, chỉ có tầm 60 - 80% ngân hàng sử dụng các thuật toán mã hóa khác nhau. Nguyên nhân chủ yếu của việc ít sử dụng rộng rãi các phương tiện tương tự là do tính phức tạp của việc khởi tạo và phân phối các mã khóa; yêu cầu nghiêm ngặt của khách hàng đối với tốc độ xử lý nhanh của hệ thống ngân hàng.

Thứ tư, các vấn đề cốt yếu, trong đó, các tổ chức tín dụng đánh giá thấp các mối đe dọa và lỗ hổng hệ thống, có thể bao gồm: tính bảo mật các đường truyền thoại (tin nhắn) qua liên lạc bằng điện thoại không đầy đủ, cũng như sử dụng các phần mềm và máy tính cá nhân bất hợp pháp.

Giải pháp cho vấn đề này là tuân thủ nghiêm ngặt các tiêu chuẩn khuyến nghị về bảo mật thông tin được Ngân hàng Nga và Cơ quan an ninh liên bang (FSB) phát triển.

Sau khi xem xét các vấn đề liên quan đến bảo mật thông tin của tổ chức tín dụng, có thể kết luận: Mức độ bảo mật các giao dịch Internet phụ thuộc rất nhiều vào mong muốn và năng lực của chính các định chế tài chính.

Bảo mật Internet Banking - một vấn đề tương đối mới, mà giải pháp xử lý nó có tính phức tạp hơn bởi sự cần thiết phải đảm bảo phát hiện, cập nhật liên tục các mối đe dọa thông tin và ngăn chặn chúng.

Vai trò không kém phần quan trọng là nâng cao trình độ hiểu biết của người dùng Internet Banking, bởi vì chính khách hàng là người ra quyết định, theo đường link hay chạy ứng dụng, có cần cài đặt tất cả các cập nhật cần thiết,... Như kinh nghiệm đã cho thấy, chừng nào việc đào tạo người dùng không đủ hiệu quả thì các biện pháp an ninh của các ngân hàng sẽ thiếu tính hệ thống.■

TÀI LIỆU THAM KHẢO:

1. Новиков А. Трансформация digital-стратегии// Банковское обозрение. 2016. № 5.

2. Конявский В.А. Минимизация рисков участников дистанционного банковского обслуживания// Вопросы защиты информации. 2014. № 4.

3. Медведева М.Б., Маврусова В.А. Улучшение качества дистанционного бслуживания в России:мобильный эквайринг и мини-терминалы // Финансы, деньги, инвестиции. 2015. № 1-2.

4. Поздеева И.А. Актуальные вопросы дистанционного банковского обслуживания с использованием интернет-технологий// Проблемы современной экономики. 2013. № 2.

5. Самчетова Н.В. Инновационный формат банковского обслуживания: планшет в руках клиента //Банковские услуги. 2015. № 3.

6. Юсупова О.А. Инновационные технологии в подготовке бакалавров финансового профиля // Инновации в образовании. 2015. № 7.

7. Доронкин М., Ионова А. Онлайн-возможности: на этапе насыщения // БДМ. Банки и деловой мир. 2015. № 6.

8. Шустов А.А. Инновационная деятельность в банковской сфере. Электронные инновации // Молодой ученый. 2013. № 9.

9. Козлов С.В. Некоторые аспекты правового регулирования дистанционного банковского обслуживания // Банковское право. 2014. № 3.

10. Савельев Д.Б. Гражданско-правовые аспекты распределения рисков в интернет-банкинге// Банковское право. 2016. № 3.