

**Presentation of effective factors in e-banking security for society interests in Islamic republic of Iran**

Recently, in e-banking fields, instruments and technology issues have been more studied, while the other factors have not been taken into the account. This problem has resulted in failures in several e-banking security projects. The aim of this paper is studying of effective and important factors on e-banking security regarding for society interests in Islamic Republic of Iran.

Semi-structured interview technique is employed in this paper. The extracted data of interviewing from 17 experts in the e-banking fields are analyzed using qualitative content analysis. The results have shown that the effective factors in e-banking are seven parameters: ISOs, OTP, comprehensive education, culture building, up to date software, infrastructures improvement, and utilization of experts. These effective factors are proposed in the paper using the presented qualitative model. Also, the results showed that the domestic banks should reduce their dependency on the foreign banks.

فصلنامه علمی (مقاله علمی پژوهشی) جامعه‌شناسی سیاسی ایران، سال چهارم، شماره چهارم (پیاپی ۱۶) زمستان ۱۴۰۰، صص ۶۲۶-۶۱۴  
<https://dx.doi.org/10.30510/psi.2022.311856.2528>

ارائه عوامل موثر بر امنیت بانکداری الکترونیک در راستای حفظ منافع جامعه در کشور جمهوری اسلامی ایران

مصطفی جوینده<sup>۱</sup> تاریخ دریافت: ۱۳۹۹/۱۰/۲۵

محمد رضا کاباران زاد قدیم<sup>۲\*</sup> تاریخ پذیرش: ۱۴۰۰/۰۱/۱۵

سبحان روشنی<sup>۳</sup>

مهدی کریمی زند<sup>۴</sup>

چکیده:

امروزه در گستره امنیت بانکداری الکترونیک، بیشتر به بحث تجهیزات فنی پرداخته می‌شود و سایر عوامل بطور شایسته مورد توجه قرار نمی‌گیرد، همین موضوع سبب عدم موفقیت بسیاری از پروژه‌های امنیتی می‌گردد که آثار مخرب و نامطلوبی با خود به همراه خواهد داشت. هدف از انجام این پژوهش ارائه عوامل موثر بر امنیت بانکداری الکترونیک در بانک‌های کشور جمهوری اسلامی ایران است و عدم توجه به عوامل مطرح شده موجب تضرر اقشار مختلف می‌گردد.

ابزار این پژوهش مصاحبه نیمه ساختار یافته می‌باشد. داده‌های حاصل از مصاحبه‌های انجام شده با ۱۷ نفر از صاحب‌نظران و نخبگان بانکی در زمینه امنیت بانکداری الکترونیک، بوسیله تحلیل محتوا کیفی مورد تجزیه و تحلیل قرار گرفت. نتایج نشان داد عوامل: آموزش جامع، رمز دوم پویا، فرهنگ‌سازی، تقویت زیر ساخت ها، کارکرد ایزوها، به روز بودن سیستم و استفاده از متخصص، عوامل موثر بر امنیت بانکداری الکترونیک می‌باشند، که می‌بایست مورد توجه قرار گیرند که در قالب مدل کیفی در این پژوهش ارائه گردیده اند. همچنین بانک‌ها باید به سمت کاهش و از میان برداشتن وابستگی‌های موجود به کشورهای بیگانه در این صنعت، حرکت نمایند.

واژگان کلیدی: بانکداری الکترونیک، امنیت اطلاعات، تحلیل محتوا

<sup>۱</sup>گروه مدیریت فناوری اطلاعات، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران [Mostafa\\_joyandeh@yahoo.com](mailto:Mostafa_joyandeh@yahoo.com)

<sup>۲</sup>گروه مدیریت صنعتی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران (نویسنده مسئول) [moh.kabaranzad@iauctb.ac.ir](mailto:moh.kabaranzad@iauctb.ac.ir)

<sup>۳</sup>گروه برق، واحد کرمانشاه، دانشگاه آزاد اسلامی، کرمانشاه، ایران [s.roshani@aut.ac.ir](mailto:s.roshani@aut.ac.ir)

<sup>۴</sup>گروه مدیریت بازرگانی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران [karimiweb@gmail.com](mailto:karimiweb@gmail.com)

یکی از دغدغه‌های اصلی بانکداری الکترونیکی در ایران، مشکل امنیت سرمایه‌هاست. به عقیده بسیاری از شهروندان عدم موفقیت در تامین امنیت بانکداری الکترونیکی می‌تواند موجب خسران آنها گردد (قربانی، ۱۳۹۹: ۷). از سوی دیگر بانکداری الکترونیک مزایای بسیاری به همراه دارد و بانک و مشتری از مزایای فراوانی بهره مند گردیده‌اند (غفوری آغمیونی، ۱۳۹۹: ۷۶)، که همین موضوع موجب استقبال و استفاده جامعه از بانکداری الکترونیک شده است. لذا تامین و یا عدم تامین امنیت بانکداری الکترونیک، در بخش‌های امنیتی، اقتصادی، فرهنگی یک کشور تاثیر قابل ملاحظه می‌گذارد. در این راستا بانک محکوم به برقراری سطح مناسبی از امنیت اطلاعات در بانکداری الکترونیک می‌باشد (شارما، ۲۰۱۶: ۳۰۲) و (کونوت و همکاران، ۲۰۱۶: ۳۶).

در حال حاضر بررسی امنیت بانکداری الکترونیک، اگرچه موضوعیت دارد اما متأسفانه در سطح پایه است (سیناوسکا، ۲۰۱۹: ۶۵) و از طرفی اغلب کلاهبرداری‌های بانکی از طریق بانکداری الکترونیک انجام می‌گردد که این موضوع خود نشان از ضعف و آسیب‌پذیری دستگاه‌های کنترل داخلی بانک‌ها دارد (عثمان و شاه، ۲۰۱۳: ۳۸۶) و جامعه هرساله زیان قابل توجهی را بابت کلاه‌برداری‌های انجام شده و جرایم اتفاق افتاده از طریق بانکداری الکترونیک متحمل می‌شود (آدامز، ۲۰۱۰: ۵) که این امر تضرر شهروندان را به دنبال خواهد داشت (رازک، ۲۰۱۶: ۵۴۵)، (کیدا و گویال، ۲۰۱۸).

## ۲- چارچوب نظری

اهم تحقیقات در راستای این پژوهش در داخل کشور جمهوری اسلامی ایران به شرح ذیل می‌باشد:

آقایی و جعفریه (۱۳۹۶) در پژوهشی با عنوان "بررسی تأثیر ابعاد هزینه، راحتی و امنیت بر ارائه خدمات در بانکداری الکترونیک (مورد مطالعه: بانک کشاورزی)" به بررسی تأثیر ابعاد هزینه، راحتی و امنیت بر ارائه خدمات در بانکداری الکترونیک پرداخته‌اند و برای اینکار از روش تحقیق توصیفی پیمایشی استفاده کرده‌اند. اطلاعات مورد نیاز با استفاده از پرسشنامه جمع‌آوری گردیده و روائی آن نیز توسط چند تن از اساتید صاحب نظر و پایانی آن از روش آلفای کرونباخ (آلفا = ۰.۹۲۲) مورد تایید واقع شده است. جامعه آماری این تحقیق، مشتریان شعب (مرکزی، شهرآرا، ستارخان، توحید) بانک کشاورزی شهر تهران است، که از خدمات بانکداری الکترونیک استفاده کرده‌اند، که بالغ بر ۱۵۴۰۰ نفر می‌باشند، که ۳۸۴ نفر طبق فرمول کوکران، از روش نمونه‌گیری تصادفی خوشه‌ای استفاده شده است. در تحقیق حاضر با استفاده از دو نرم افزار SPSS و LISREL از دو نوع آمار توصیفی و استنباطی برای تحلیل داده‌ها استفاده شده است در سطح توصیفی با استفاده از مشخصه‌های آماری نظیر فراوانی، درصد، به رسم نمودارها و تجزیه و تحلیل اطلاعات پرداخته شد و در سطح استنباطی، از آلفای کرونباخ برای بررسی پایایی پرسشنامه، از روش مدل معادلات ساختاری برای رد یا تأیید فرضیات تحقیق، و برای بررسی میزان تبیین متغیرها توسط هر یک از سؤالات مرتبط در پرسشنامه از تجزیه و تحلیل

عاملی تاییدی استفاده شده است. نتایج نشان داد که هزینه (هزینه‌های بانکی)، راحتی و امنیت تأثیر مثبت و معناداری بر خدمات بانکداری آنلاین دارد هم چنین خدمات بانکداری آنلاین تأثیر مثبت و معناداری بر تحویل خدمات به مشتریان دارد (آقایی و جعفریه، ۱۳۹۶: ۷).

ونکی و همکاران (۱۳۹۶) در پژوهشی با عنوان "مدل پیاده‌سازی مدیریت امنیت فناوری اطلاعات در صنعت بانکداری ایران". هدف از اجرای این پژوهش، ارائه مدل قدرتمند با انتخاب کنترل‌های امنیتی مناسب به منظور محافظت از دارایی‌های اطلاعاتی بانک بود. در این مدل، ابتدا اصل‌های مندرج در استاندارد ایزو ۲۷۰۰۱ استخراج شد، سپس با مطالعه بهترین تجربه‌های جهان درباره موضوع از سال ۲۰۰۸ تا ۲۰۱۶، از طریق روش توصیفی و کیفی، نکات منطبق بر مدیریت امنیت اطلاعات در صنعت بانکداری به آن اضافه شد. در ادامه با مطالعه عملکرد بانک‌های ایرانی در خصوص برخورد با پیاده‌سازی نظام مدیریت امنیت فناوری اطلاعات به کمک ابزار اقدام پژوهی، بندهایی که مانع اجرایی شدن حقیقی این استاندارد می‌شد، حذف شدند و در نهایت یک مدل مفهومی، حاوی دستورالعمل‌های اجرایی با در نظر گرفتن کلیه اصول استاندارد مدیریت امنیت اطلاعات و متمرکز بر ویژگی موسسه‌های بانکی ایران پیشنهاد شد (ونکی و همکاران، ۱۳۹۶: ۳۷۹).

شاهرخی ساردو (۱۳۹۶) در پژوهشی با عنوان "بررسی موانع و منابع پیاده سازی بانکداری الکترونیک در ایران". ظهور فناوری های اطلاعاتی و ارتباطی همه شئون زندگی بشر و از جمله تجارت را دستخوش تغییرات فراوانی نموده است. از همین منظر است که بانکداری الکترونیکی شکل و تکوین یافته است. برای کشور ما که به تازگی این گونه از تجارت را تجربه می نماید، آگاهی از روندهای بین المللی جهت تسریع در استقرار و کارآمد شدن نظام بانکداری الکترونیکی مفید به فایده خواهد بود. از اینرو در پژوهش فوق ضمن بررسی تعریف و مزایای بانکداری الکترونیک و تفاوت این نوع بانکداری با بانکداری سنتی، بر روند شکل گیری و همچنین عوامل و موانع توسعه بانکداری الکترونیک در ایران پرداخته و در انتها نیز بر اساس تجارب موفق بین المللی، توصیه ها و پیشنهادات لازم جهت پیاده سازی بانکداری الکترونیک در کشور ارائه گردیده است (شاهرخی ساردو، ۱۳۹۶).

شیرطاهری و طیبی (۱۳۹۵) در پژوهشی با عنوان "پارادایم امنیت و اعتماد در بانکداری الکترونیک". امنیت و اعتماد از مهمترین عناصری است که باعث اثر گذاری در تراکنش های بانکی می گردد و براعتماد و استفاده مشتریان از این خدمات اثر می گذارد. از اینرو ضرورت مدیریت امنیت درسیستم های بانکی مشخص می گردد. با وجود سرمایه گذاری های فراوان انجام شده در زمینهی کاربری فناوری های اطلاعاتی در عرصه ی بانکداری، گزارش ها حاکی از آن است که برخی از کاربران با وجود دسترسی به فناوری ها، از آن استفاده نمی کنند. این موضوع، نیاز به انجام پژوهش هایی برای شناسایی عوامل تعیین کننده پذیرش سیستم بانکداری اینترنتی توسط کاربران را آشکار می کند. مطالعات نشان می دهد که مشتریان به دلیل اعتماد اندک، استقبال زیادی از مدل های تجارت الکترونیک ندارند. بنابراین چالش پیش روی بانک ها، تغییر نگرش

و جهت دهی مثبت به نیت رفتاری مشتریان برای استفاده بیشتر از خدمات الکترونیکی است. لذا هدف از این مطالعه بررسی امنیت و اعتماد در بانکداری الکترونیک و عوامل موثر بر آن است (شیرطاهری و طیبی، ۱۳۹۶).

شرفیان و غریبی (۱۳۹۵) در پژوهشی با عنوان "مروری بر بانکداری الکترونیکی و امنیت بانکداری الکترونیک". هدف این پروژه به دست آوردن درک و دانش لازم جهت مشتریان و افراد از ابزارهای امنیتی در بانکداری الکترونیک می باشد که کاربرد بسیار زیادی در جامعه امروزه خواهد داشت. با توجه به اینکه خدمات بانکداری الکترونیک از طریق کانال های مجازی و عمومی همچون تلفن، اینترنت، تلفن همراه و ... صورت می گیرد و افراد با آن آشنایی و به آن عادت ندارند لذا، فقدان امنیت بر عملکرد اینگونه سازمان ها و نیز عدم اعتماد افراد به این خدمات آثار مخرب و نامطلوبی با خود به همراه خواهد داشت. ازاینرو ضرورت مدیریت امنیت در سیستم های بانکی مشخص می گردد. بر این اساس علاوه بر امنیت داده ها عوامل متعددی همچون فرهنگ سازی، به کارگیری سیاست ها و ابزارهای امنیتی و رعایت امنیت فیزیکی، کیفیت در ارائه خدمات و پشتیبانی، آموزش، سهولت در استفاده از خدمات، تبلیغات و سیاستهای تشویقی قابل توجه می باشد که به عنوان متغیرهای پژوهش طی مدل ارائه گردید. علاوه بر آن مشخص گردید بانک جهت تأمین امنیت کامل تر تراکشن ها در بانکداری الکترونیک، بایستی در کنار رعایت سیاست های امنیتی مثل محرمانگی، سندیت، تمامیت و ... از ابزارهای امنیتی همچون فن رمزنگاری، استفاده از کد کاربری و رمز عبور، گواهی های دیجیتال، امضای دیجیتال، نرم افزارها و پروتکل های امنیتی بهره گیرند (شرفیان و غریبی، ۱۳۹۶).

یادگاری و دیگران (۱۳۹۴) در پژوهشی با عنوان "امنیت در بانکداری الکترونیک". با افزایش مبادلات بانکی بین مشتریان و بانک ها، بانک ها سعی بر این داشته اند تا با طراحی و راه اندازی کارت های بانکی به نیاز مشتریان خود پاسخ دهند و مشتریان بتوانند امور بانکی خود را به نحو مطلوبی انجام دهند. در این راستا بانکداری الکترونیک بوجود آمد. بانکداری که در آن بدون نیاز به حضور مشتری به طور فیزیکی در شعب، در هر ساعت از شبانه روز می توان امور بانکی را انجام داد. هر چند این کارت ها دارای مزایای زیادی هستند ولی تا زمانی که امنیت آنها برقرار نباشد آسیب پذیر هستند. با بالابردن سطح آگاهی مشتریان و افراد ذی نفع مرتبط با بانکداری الکترونیک می توان تا حدود زیادی امنیت بانکداری الکترونیک را بالا برد (یادگاری و دیگران، ۱۳۹۴).

یحیی پور و شاد (۱۳۹۳)، در پژوهشی با عنوان "امنیت شبکه های کامپیوتری در بانکداری الکترونیک". حملات پیشرفته و نوآوری که امروزه شاهد آن هستیم، منجر به رشد نگرانی ها و مشکلات امنیتی به صورت نمایی گردیده اند. این مقاله، نظریه ی کنترل امنیت اطلاعات را معرفی می کند. مطالعات شبکه ی حفاظتی بر مبنای نظریه ی کنترل ایمنی اطلاعات، یک استراتژی پایه ی کنترل امنیتی را ایجاد کرده و در نهایت منجر به ساخت و پیاده سازی یک مدل امنیتی شبکه میگردد. در ادامه یک مدل امنیتی تهدید گرا برای برآورده سازی چالش های امنیتی مطرح شده این مقاله، سعی شده است تا یک روش جدید و نو آورانه ای را برای فراهم ساختن امنیت در مقابل هر نوع تهدیدی را بررسی کرده و از تکنیک های مرسوم که فقط بر تهدیدهای قابل پیش بینی در مدیریت ریسک اکتفا می کنند، ارائه نماید (یحیی پور و شاد، ۱۳۹۳).

اسد امرجی والهام بخش (۱۳۹۳) در پژوهشی با عنوان "بررسی چالش‌های موجود در صنعت بانکداری الکترونیک". فناوری اطلاعات و به خصوص اینترنت دارای پتانسیل لازم برای تغییر بانکها و صنعت بانکداری است. فرصت‌هایی را که خدمات بانکداری الکترونیک و فناوری‌ها به بخش بانکداری پیشنهاد می‌دهند برای برآوردن نیازهای مشتریان فعلی و برای جذب مشتریان جدید در آینده می‌باشد. بانک‌ها به منظور انطباق با تکنولوژی، سیستم‌های بانکداری الکترونیک را طراحی، توسعه و اجرا می‌کنند. این مقاله فرصت‌ها و چالش‌های بانکداری الکترونیک را بیان می‌کند و پیشنهاداتی برای خدمات بانکداری الکترونیک ارائه می‌دهد. برای انجام این تحقیق از روش فراترکیب استفاده شده است. یافته‌های اصلی تحقیق نشان می‌دهد که بانک‌ها خدمات بانکداری الکترونیک را به منظور رقابت با رقبا و دنبال کردن توسعه فناوری و به دلیل فواید هزینه‌های پایین در تراکنش‌های بانکداری الکترونیک آغاز می‌کنند. مشکلات اصلی که بانک‌ها با آن مواجه‌اند این است که مشتریان به یک مکانیزم محافظت از داده‌ها و امنیت نیازمند می‌باشند. استفاده کم از اینترنت به دلیل نا آشنا بودن مردم با دستگاه‌های فناوری پیشرفته و مشکلات مربوط به امنیت و حفظ حریم خصوصی باعث نفوذ کم خدمات بانکداری الکترونیک در مشتریان می‌شود. در انتهای مقاله مدل پیشنهادی نویسنده جهت رفع چالش‌های بانکداری الکترونیک ارائه شده است (اسد امرجی والهام بخش، ۱۳۹۳).

سهرابی و دیگران (۱۳۹۲)، در پژوهشی با عنوان "بررسی و شناسایی موانع پذیرش بانکداری الکترونیک در بین مشتریان (مطالعه موردی: بانک رفاه شهر همدان)". هدف از تحقیق حاضر بررسی و شناسایی عوامل موثر بر عدم پذیرش بانکداری الکترونیک از سوی مشتریان در بانک رفاه شهر همدان می‌باشد. روش تحقیق پیمایشی (زمینه یابی) بوده و جامعه آماری مشتریان شعب مختلف بانک رفاه بوده است. نتیجه آزمون فرضیه‌های تحقیق نشان داد که از بین ۸ متغیر مورد بررسی ۶ متغیر شامل ضعف آموزش و اطلاع رسانی، کافی نبودن مشوق‌های بانکی، احساس عدم امنیت، اعتماد نداشتن، کاهش تعاملات اجتماعی و نامناسب بودن امکانات فنی بر عدم پذیرش بانکداری الکترونیک از سوی مشتریان تأثیر گذار هستند و دو متغیر عدم ادراک مشتریان از سودمندی و عدم ادراک مشتریان از سهولت استفاده مانعی در پذیرش بانکداری الکترونیک از سوی مشتریان نمی‌باشند. در نهایت در آزمون رتبه‌بندی فریدمن نیز مشخص گردید از بین ۶ متغیر نامبرده، متغیرهای کافی نبودن مشوق‌های بانکی و احساس عدم اطمینان بیشترین تأثیر را در عدم پذیرش بانکداری الکترونیک از سوی مشتریان دارند (سهرابی و دیگران، ۱۳۹۲).

کریم خانی و دیگران (۱۳۹۲)، در پژوهشی با عنوان "پردازش ابری: امنیت شبکه در بانکداری الکترونیک". امروزه پردازش ابری به وضوح به عنوان یکی از جذاب‌ترین حوزه‌های فناوری یا حداقل تا حدی جذاب به واسطه کارآیی هزینه‌ای آن و انعطاف پذیری مناسب محسوب می‌شود. با این حال، علی‌رغم رشد در فعالیت‌های مربوطه و میزان تمایل به سوی پردازش ابری، همچنان نگرانی‌های مداوم و قابل توجهی در مورد پردازش ابری وجود دارند که تحرک آن را با کندی مواجه می‌سازند و سرانجام، دیدگاه موجود به سوی پردازش ابری به عنوان یک مدل جدید تدارک فناوری اطلاعات را با مشکل مواجه می‌سازند. انتظار می‌رود که پردازش ابری در سال‌های پیش رو، به یکی از فناوری‌ها با سریع‌ترین رشد‌ها

مبدل گردد. برنامه های تجاری، بزرگترین بازار برای خدمات ابری پیش رو خواهند بود که با یک انتقال تدریجی از خدمات بر مبنای تقاضا به سوی خدمات ابر محور، حرکت خواهند نمود، بخصوص برای برنامه های عمومی تجاری مثل مدیریت ارتباط با مشتری و برنامه ریزی منابع سازمان. انتظار می رود که بانک ها به حوزه پردازش ابری با احتیاط وارد گردند مقاله پیش رو، یک خلاصه از پردازش ابری را ارائه و پایه ای مناسب برای درک آن را فراهم می آورد.

امیری فارسانی و دیگران (۱۳۹۲)، در پژوهشی با عنوان "مروری بر وضعیت بانکداری الکترونیک و بررسی مزایا و معایب و چالش های پیاده سازی آن" تکنولوژی بانکداری الکترونیکی به فعالیت های مالی اشاره دارد که با استفاده از تکنولوژی الکترونیکی انجام می شود. با وجود ظهور سیستم های تکنولوژی بانکداری الکترونیکی افراد شاهد افزایش رفاه زندگی و تسهیل انجام فعالیت های روزانه هستند. در سطح سازمانی، کاربرد بانکداری الکترونیکی اجازه می دهد بانک ها به نیازهای مختلف مشتریان در مکان های متفاوت پاسخ گویند. هدف صنعت بانکداری استفاده آسان تر و مناسب تر مشتریان از این تکنولوژی ها می باشد. از نقطه نظر رقابتی، این فرصت را فراهم می آورد تا بانک ها بتوانند با موسسات بزرگ مالی رقابت کنند. در این مقاله به مقایسه بانکداری سنتی و بانکداری الکترونیک پرداخته می شود و مزایا و معایب بانکداری الکترونیک بیان می شود. همچنین بررسی هایی که در کشورهای مختلف در رابطه با این موضوع انجام شده و دلایل رشد بعضی از کشورها در این زمینه، همچنین تاثیر آن بر روی جوامع و نقش و رابطه ای را که مشتریان به عنوان عامل کلیدی، در این زمینه ایفا می کنند را مورد بحث قرار داده و روش هایی را که مشتریان می توانند از خدمات بانکداری الکترونیک استفاده کنند را شرح داده و کانال های دسترسی به این خدمات را معرفی نموده است (امیری فارسانی و دیگران، ۱۳۹۲).

### ۳- روش تحقیق

این پژوهش باهدف بررسی وضعیت امنیت در بانکداری الکترونیک در بانک ها و موسسات مالی و ارائه عوامل موثر بر امنیت بانکداری الکترونیک، جهت افزایش امنیت بانک انجام گردیده است. در این مطالعه از مصاحبه نیمه ساختاریافته با فرد مصاحبه شونده در یک دوره استفاده گردیده و یک پژوهش به روش کیفی است. با استفاده از روش تحلیل محتوا مباحث اصلی از مصاحبه های انجام شده استخراج و عوامل موثر بر امنیت بانکداری الکترونیک با اجماع نظر محقق، اساتید و نخبگان امنیت بانکداری الکترونیک ارائه گردید (مؤمنی راد و همکاران، ۱۳۹۲، ۱۸۷).

### ۳-۱ مراحل انجام مصاحبه

مراحل انجام مصاحبه با حضور متخصصین و صاحب نظران این حوزه به شرح ذیل می باشد: ۱- تعیین و تعریف پرسش های پژوهش، ۲- انتخاب کارشناسان، ۳- آماده سازی شرایط جهت انجام مصاحبه، ۴- مصاحبه با کارشناسان، ۵- ارزیابی و تجزیه و تحلیل نتایج ۶- تهیه گزارش (بلومبرگ و دیگران، ۲۰۰۵: ۸۸۷).

### ۳-۲ روش نمونه گیری

در این پژوهش از روش نمونه‌گیری گلوله برفی که یکی از زیرشاخه‌های روش نمونه‌گیری متوالی یا متواتر است استفاده گردیده‌است. این روش زمانی مناسب است که بخواهیم افراد متخصص در یک رشته یا شاخه را شناسایی نماییم، لذا برای شناسایی افراد متخصص در یک زمینه خاص این روش مورد استفاده قرار می‌گیرد (ایمان و نوشادی، ۱۳۹۶: ۶).

### ۳-۳ اطلاعات دموگرافیک مشارکت‌کنندگان در مطالعه

در این پژوهش ۱۷ نفر از متخصصین و نخبگان حوزه امنیت بانکداری الکترونیک شرکت داشته‌اند. اطلاعات حاضرین در پژوهش به شرح جدول شماره (۱) می‌باشد. همان‌طور که ملاحظه می‌نمایید سعی گردیده‌است افراد دعوت‌شده از متخصصین و افراد خبره در زمینه بانکداری الکترونیک با تخصص‌های گوناگون بوده تا موارد مطرحه در پژوهش از تمامی ابعاد مورد بررسی و واکاوی قرار بگیرد. اطلاعات این افراد در جدول شماره (۱). اطلاعات دموگرافیک مشارکت‌کنندگان در مطالعه، قابل ملاحظه می‌باشد.

جدول شماره (۱). اطلاعات دموگرافیک مشارکت‌کنندگان در مطالعه

ردیف	جنسیت	مدرک تحصیلی	سمت	سابقه فعالیت
۱	مرد	کارشناسی ارشد	مدیر عامل بانک	۲۸ سال
۲	مرد	دکتری	برنامه نویس	۱۵ سال
۳	مرد	کارشناسی ارشد	پلیس فتا	۱۸ سال
۴	مرد	دکتری	مدیر عامل گروه تحقیقاتی	۲۸ سال
۵	مرد	کارشناسی ارشد	حراست فناوری اطلاعات بانک	۱۸ سال
۶	مرد	دکتری	مدیر شرکت امنیت شبکه	۲۴ سال
۷	مرد	کارشناسی ارشد	مدیر عامل شرکت تامین امنیت	۱۷ سال



۸	مرد	دکتری	متخصص الکترونیک	۱۴ سال
۹	مرد	کارشناسی ارشد	حراست بانک	۱۶ سال
۱۰	زن	کارشناسی ارشد	متخصص امنیت شبکه بانک	۱۵ سال
۱۱	زن	دکتری	مدیریت شعبه بانک	۱۹ سال
۱۲	مرد	کارشناسی ارشد	پلیس مبارزه با جرائم اقتصادی	۲۸ سال
۱۳	مرد	کارشناسی ارشد	طراح پروتکل های امنیت شبکه	۱۲ سال
۱۴	مرد	دکتری	طراح پروتکل های امنیت	۱۰ سال
۱۵	مرد	کارشناسی ارشد	حقوقدان بانک	۱۶ سال
۱۶	مرد	دکتری	مدیریت بازرسی	۱۸ سال
۱۷	مرد	کارشناسی ارشد	مدیریت حسابرسی	۲۸ سال
				ظ

### ۳-۴ تجزیه و تحلیل داده‌ها، روایی، پایایی

در این پژوهش، با توجه به طرح نظام‌مند، با تحلیل محتوای متون، از کدگذاری استفاده شد و فهرستی از کدها استخراج شدند و با پیوند دادن کدها به هم، مفاهیم اولیه شکل گرفت. در این مرحله، کدهای مربوط از هفده مصاحبه، بررسی یادداشتها و اسناد، استخراج شدند. سپس به استخراج مقولات مهم و اساسی پرداخته شد و مولفه‌های دارای اهمیت در امنیت بانکداری الکترونیک مشخص گردید که به تایید همه خبرگان و اساتید در این پژوهش رسیده شده‌است.

در مرحله تقطیع و کدگذاری اولیه داده‌ها، کدهای اولیه استخراج شد. در مراحل بعدی به تدریج این تم‌ها با حذف تم‌های مشابه و همپوشان کمتر شده و رفته‌رفته خود را به صورت خوشه‌هایی از مقوله‌ها نشان دادند. پژوهشگر در طی جلساتی فرایند کدگذاری، کدها را با دیگر همکاران تحقیق (اساتید راهنما و مشاور) مرور کرده و در مورد آن‌ها باهم به توافق می‌رسیدند. همچنین برای پایا بودن کار تحقیق از روش تکرارپذیری استفاده شد (فلیک، ۱۳۹۷: ۴۲). به این ترتیب نهایتاً از متن مصاحبه شرکت‌کنندگان در پژوهش مقوله‌ها و زیر مقولات حاصل شد.

برای افزایش اعتبار پژوهش از سه راهبرد: ۱- توصیف‌گرهای با استنباط پایین، ۲- فرمت بندی تحقیق و ۳- سندیت خارجی که توسط جانسون و کریستین ارائه گردیده، استفاده شد (هالیدی، ۱۳۹۴: ۷۷-۷۸).

#### ۴- یافته‌های تحقیق

با عنایت به مطالب ذکر شده ۷ مقوله به عنوان عوامل موثر در امنیت اطلاعات بانکداری الکترونیک به شرح ذیل استخراج گردید: ۱-رمزدوم پویا، ۲-استفاده از متخصصین، ۳-استفاده از ایزوها، ۴-فرهنگ سازی مناسب، ۵-آموزش جامع، ۶-تقویت زیر ساختهای امنیتی، ۷-به روز بودن سیستم بانکداری.

یافته‌های پژوهش حاضر نشان می‌دهد استفاده از متخصصین در بانکداری الکترونیک در کاهش جرایم موثر است لذا پیشنهاد می‌گردد از متخصصین امنیت به صورت درون سازمانی استفاده شود و از برون سپاری فرآیندهای امنیت بانکداری الکترونیک بصورت تمام و کمال جلوگیری شود. مهاجرت پرسنل شرکت‌های پیمانکار به خارج از کشور و خروج اطلاعات محرمانه بانکی که این افراد در اختیار دارند می‌تواند صدمات جبران ناپذیری به پیکره نظام بانکداری وارد نماید. استفاده از رمز دوم پویا منجر به کاهش جرایم بانکداری الکترونیک بخصوص جرایم مهندسی اجتماعی گردیده است و به روز رسانی مداوم توسط واحدهای درون سازمانی با رعایت محرمانگی موضوع، توصیه می‌گردد. نتایج پژوهش نشان می‌دهد در حال حاضر رمز دوم پویا مهمترین عامل موثر بر امنیت بانکداری الکترونیک می‌باشد.

فرهنگ سازی و آموزش، دو مقوله بسیار حائز اهمیت و مرتبط با یکدیگر می‌باشند. بسیاری از جرایم صورت گرفته در بانکداری الکترونیک به علت بی اطلاعی افراد جامعه بوده است و در صورت انجام آموزش مناسب تا حد بسیار زیادی از وقوع جرایم اجتماعی جلوگیری به عمل خواهد آمد. آموزش نه تنها بر روی امنیت اطلاعات تاثیر دارد بلکه بر روی فرهنگ جامعه نیز تاثیر مستقیم دارد.

در خصوص استفاده از ایزوها نتایج پژوهش بیانگر این موضوع است که با توجه به وجود تفاوت‌های قابل توجه در بانک‌های داخلی کشور با بانکداری سایر کشورها، پیاده سازی و بومی سازی مراحل استاندارد ایزو ۲۷۰۰۱ و مطابقت دادن نکات مورد نیاز در حوزه امنیت اطلاعات با روش‌های اجرای فرایندها در صنعت بانکداری ایران می‌تواند به افزایش امنیت بانکداری الکترونیک کمک شایانی نماید.

پیاده سازی بانکداری الکترونیک نیازمند وجود زیرساخت مطمئن می‌باشد، نتایج پژوهش نشان می‌دهد اولین عامل موثر بر امنیت بانکداری الکترونیک، زیر ساخت مناسب می‌باشد چراکه بقیه عوامل به نوعی بر روی این بستر پیاده سازی می‌گردند.

نتایج تحقیق نشان می‌دهد با توجه به گستردگی این صنعت بین اقشار مختلف جامعه، منابع مالی قابل توجهی در آن قرار دارد و همین موضوع انگیزه بسیار مناسب برای ورود کلاهبرداران و شیادان به این موضوع می‌باشد. این افراد برای دستیابی به اهداف خود از هیچ تلاشی کوتاهی ننموده و از به‌روزترین ابزار و سیستم‌های موجود در دنیا جهت دستبرد به منابع مالی استفاده می‌نمایند. لذا استفاده از سیستم‌های به‌روز توسط بانک‌ها در راستای افزایش توان مقابله و پیش‌گیری از وقوع جرم امری بسیار خطیر می‌باشد.

بانکداری الکترونیک در مدت زمان کوتاهی توانسته جایگاه مهمی در جهان برای خود ایجاد کند. کشور جمهوری اسلامی ایران نیز از این مقوله مستثنی نبوده و روزانه میلیارها تراکنش توسط ابزارهای بانکداری الکترونیک انجام می‌گردد. نتایج به دست آمده از پژوهش نشان می‌دهد با توجه به ساختار متفاوت بانکی در کشور ما با سایر کشورهای صاحب این صنعت، استفاده از مدل داخلی برای تامین امنیت بانکداری الکترونیک امری بسیار ضروری است. در همین راستا در این پژوهش به شناسایی عوامل مؤثر بر امنیت اطلاعات در بانکداری الکترونیک پرداخته و هفت عامل: رمز دوم پویا، کارکرد ایزوها، فرهنگ سازی، آموزش جامع، تقویت زیر ساختها، به‌روز بودن سیستم و استفاده از متخصص، مورد شناسایی قرار گرفت.

نتایج تحقیقات نشان می‌دهد تامین امنیت کامل (تامین امنیت بصورت صد در صد) در بانکداری الکترونیک امری خلاف واقع بوده و به دور از دسترس می‌باشد، اما افزایش امنیت در این حوزه به شکل قابل قبول، دور از دسترس نبوده و قابل انجام است. لذا پیشنهاد می‌گردد بانک‌ها به سمت کاهش و از میان برداشتن وابستگی‌های موجود به کشورهای بیگانه در این صنعت، حرکت نمایند.

در پایان می‌توان عنوان نمود، تامین امنیت در حوزه بانکداری الکترونیک یکی از دغدغه‌های اصلی مشتریان و زمامداران صنعت بانکداری در سراسر جهان است. این صنعت با پول مردم در سطحی گسترده بین اقشار مختلف جامعه در ارتباط است و به همین دلیل حاشیه تحمل خطا در آن نسبت به صنایع دیگر بسیار اندک است لذا اشتباه و یا خطا در این حوزه می‌تواند مخاطرات بسیار جدی در سطح جامعه با خود به همراه داشته باشد.

#### منابع:

۱. غفوری آغمیونی س. (۱۳۹۹). ارائه مدلی برای بهبود عملکرد بانکداری الکترونیکی براساس سیستم مدیریت ارتباط با مشتری. فصلنامه علمی تخصصی رویکردهای پژوهشی نوین در مدیریت و حسابداری، ۴(۳۳)، ۷۶-۸۷.
۲. قربانی، حسین، ۱۳۹۹، بررسی رابطه بین کیفیت خدمات بانکداری الکترونیکی و رضایت مشتریان شعب بانک قوامین خراسان شمالی در سال ۱۳۹۶، ششمین کنفرانس ملی پژوهش‌های کاربردی در مدیریت، حسابداری و اقتصاد سالم در بانک، بورس و بیمه، تهران.
۳. فلیک، اووه (۱۳۹۷). درآمدی بر تحقیق کیفی، ترجمه: هادی جلیلی، چاپ نهم، نشر نی.

۴. جعفریه، حمید؛ آقایی، ایمان (۱۳۹۶). بررسی تأثیر ابعاد هزینه، راحتی و امنیت بر ارائه خدمات در بانکداری الکترونیک (مورد مطالعه: بانک کشاورزی)، اولین کنفرانس سالانه بین المللی مدیریت، اقتصاد و حسابداری نوین.
۵. ونکی، مونا؛ تقوا، محمدرضا؛ تقوی فرد، سیدمحمدتقی و فیضی، کامران، (۱۳۹۶)، مدل پیاده‌سازی مدیریت امنیت فناوری اطلاعات در صنعت بانکداری ایران، مدیریت فناوری اطلاعات، دوره ۹، شماره ۲، ۳۷۹-۴۰۴.
۶. شاهرخی ساردوزینب(۱۳۹۶)، بررسی موانع و منابع پیاده سازی بانکداری الکترونیک در ایران، همایش بین المللی مدیریت و حسابداری ایران.
۷. شیرطاهری، علی محمد؛ طیبی،محمد(۱۳۹۵). پارادایم امنیت و اعتماد در بانکداری الکترونیک، اولین کنفرانس بین المللی تحولات نوین در مدیریت، اقتصاد و حسابداری.
۸. شرفیان، علی؛ غریبی کریک، سید جلال الدین(۱۳۹۵)، مروری بر بانکداری الکترونیک و امنیت بانکداری الکترونیک، کنفرانس ملی دانش و فناوری مهندسی برق، کامپیوتر، مکانیک ایران.
۹. یادگاری مهدی آباد، مسلم؛ اوضح، آرمان؛ احمدی، فرشته (۱۳۹۴). امنیت در بانکداری الکترونیک، نخستین کنفرانس بین المللی فناوری اطلاعات.
۱۰. یحیی پور، یوسف؛ شاد، ثمین (۱۳۹۳). امنیت شبکه‌های کامپیوتری در بانکداری الکترونیک، دومین کنفرانس بین المللی مدیریت چالشها و راهکارها.
۱۱. اسد امرجی، الهام؛ الهام بخش، حسین (۱۳۹۳). بررسی چالشهای موجود در صنعت بانکداری الکترونیک، اولین کنفرانس ملی چالش های مدیریت فناوری اطلاعات در سازمان ها و صنایع.
۱۲. سهرابی، روح اله؛ یوسفی فرد، ارسلان؛ نریمانی عزیز، زهرا(۱۳۹۲). بررسی و شناسایی موانع پذیرش بانکداری الکترونیک در بین مشتریان (مطالعه موردی: بانک رفاه شهر همدان، دومین همایش ملی علوم مدیریت نوین.
۱۳. کریم خانی، فرهاد و عسگر اقدم، هادی و احمدی رند، طیبه، ۱۳۹۲، پردازش ابری: امنیت شبکه در بانکداری الکترونیک، همایش ملی مهندسی کامپیوتر و فناوری اطلاعات، شوشتر.
۱۴. امیری فارسانی، مریم؛ داویناه جزئی، محمد؛ منتظری، محمد علی (۱۳۹۲). مروری بر وضعیت بانکداری الکترونیک و بررسی مزایا و معایب و چالش های پیاده سازی آن، اولین کنفرانس ملی نوآوری در مهندسی کامپیوتر و فناوری اطلاعات.

16. Kida, M. I., & Goyal, A. (2018). Challenges of Cashless Banking System: Empirical Study of Selected Banks in Nigeria and the State of Rajasthan, India.
17. Bélanger, F., Collignon, S., Enget, K., Negangard, E. (۲۰۱۷). Determinants of Early Conformance with information security policies. *Management*, ۵۴(۷), ۸۸۷-۹۰۱.
18. Sharma, S. (2016). A detail comparative study on e-banking VS traditional banking. *International Journal of Advanced Research*, 2, 302-307.
19. Konoth, R. K., van der Veen, V., & Bos, H. (2016, February). How anywhere computing just killed your phone-based two-factor authentication. In *International Conference on Financial Cryptography and Data Security* (pp. 405-421).
20. Razak, L.T. The Effect of Security and Privacy Perceptions on Customers' Trust to Accept Internet Banking Services: An Ex-tension of TAM" Mohammed A. Al-Sharaf, "Ruzaini A. Arsha," Emad Abu-Shanab and "Nabil Elayah" Faculty of Computer Systems and Software Engineering, UMP. *Journal of Engineering and Applied Sciences* 2016, 100(3), 545-552.
21. Osman, M.H.; Shah, A.A.; Wills, R.G.A.; Walsh, F.C. Mathematical modelling of an enzymatic fuel cell with an air-breathing cathode. *Electrochimica Acta* 2013, 112, pp.386-393.
22. Adams, R. Prevent, protect, pursue—a paradigm for preventing fraud. *Computer Fraud & Security* 2010, 7, 5-11.