ارائه مدل جهت کاهش جرایم در صنعت بانکداری‌الکترونیک

مصطفی جوینده[۱]، محمد رضا کاباران زاده قدیم[۲]، سبحان روشنی[۳]، مهدی کریمی زند[۴]
۱- گروه مدیریت فناوری اطلاعات، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران
Mostafa_joyandeh@yahoo.com
۲- گروه مدیریت صنعتی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران
moh.kabaranzad@iauctb.ac.ir
۳- گروه برق، واحد کرمانشاه، دانشگاه آزاد اسلامی، کرمانشاه، ایران
s.roshani@aut.ac.ir
۴- گروه مدیریت بازرگانی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران
karimiweb@gmail.com

چکیده: امروزه جهان شاهد وقوع جرایم بسیاری در حوزه بانکداری‌الکترونیک می‌باشد. جرایمی که روزانه افزایش پیدا کرده و منجر به متضرر شدن مشتری در این حوزه می‌گردد. با کمی بررسی در این خصوص نیاز به مدل جامع، تلفیق شده و مطابق با مسائل روز در زمینه امنیت برای بانک ضروری و حیاتی به نظر می‌رسد. این تفکر قدیمی و از کار افتاده که امنیت اطلاعات تنها بواسطه خرید تکنولوژی و ابزارهای فنی حاصل می‌گردد، دیگر مثمر ثمر نمی‌باشد. هدف از انجام این تحقیق ارائه مدل کمی جهت افزایش امنیت در صنعت بانکداری‌الکترونیک می‌باشد. روش پژوهش حاضر از نظر هدف کاربردی و دارای رویکرد آمیخته است. جامعه آماری در مطالعات کیفی شامل خبرگان حوزه بانکداری‌الکترونیک است که ۱۸ نفر و در بخش کمی ۱۲۳ نفر می‌باشد. روش نمونه‌گیری در بخش کیفی از گلوله برفی و در بخش کمی از روش تمام شمار استفاده گردیده است. داده‌های کیفی با روش مصاحبه نیمه ساخت یافته تهیه و سپس تحلیل محتوا شدند و داده‌های کمی با روش تحلیل عاملی و بوسیله نرم‌افزار **SPSS** نسخه ۲۵ و نرم افزار **PLS** نسخه۳ مورد تجزیه و تحلیل قرار گرفتند. پرسشنامه طراحی شده دارای ۳۰ سؤال است که روایی آن با تحلیل عاملی تأئیدی مورد بررسی قرار گرفت. پایایی پرسشنامه با ضریب آلفای کرونباخ اندازه گیری شد که مقدار آن ۰/۷۰ برآورد شد که از میزان قابل قبولی برخوردار است. نتایج نشان می‌دهد عوامل مؤثر بر امنیت اطلاعات در بانکداری‌الکترونیک هفت عامل هستند که عبارتند از: رمز دوم پویا، کارکرد ایزوها، فرهنگ‌سازی، آموزش جامع، تقویت زیر ساخت ها، به روز بودن سیستم و استفاده از متخصص.

واژه های کلیدی: بانکداری‌الکترونیک، امنیت بانکداری‌الکترونیک، امنیت اطلاعات، جرایم الکترونیک

تاریخ دریافت مقاله: ۱۴۰۰/۰۳/۳۰	تاریخ پذیرش مقاله: ۱۴۰۰/۰۴/۳۰
از صفحه ۳۷ تا ۴۹	نوع مقاله : پژوهشی
نویسنده مسئول: محمد رضا کاباران زاده قدیم	نشریه علمی فناوری اطلاعات و ارتباطات انتظامی- دوره دوم- شماره ۵ - بهار ۱۴۰۰

۱- مقدمه

دنیای کنونی با به کارگیری شبکه اینترنت ملقب به «عصر اطلاعات» گردیده است، از خصوصیات مهم و آشکار این عصر ایجاد دگرگونی‌های بنیادی در بسیاری از ابعاد فرهنگی، ارتباطی،اقتصادی و اجتماعی زندگی انسان‌ها می‌باشد. یکی از این دگرگونی ها، تغییرات ژرفی است که در روابط اقتصادی بین افراد، شرکت‌ها و دولت‌ها ایجاد گردیده است. مبادلات تجاری و مالی افراد با یکدیگر، شرکت‌ها با یکدیگر، افراد با شرکت‌ها و دولت‌ها از حالت سنتی خود که بطور عمده مبتنی بر مبادله بر اساس اسناد و مدارک کاغذی است، خارج شده و در جهت انجام مبادلات بواسطه استفاده از سیستم‌های مبتنی بر اطلاعات الکترونیکی با سرعت زیاد و شتابی فزاینده در حرکت است [۱]. از سوی دیگر بانک که یک سازمان مالی است که نقشی حایز اهمیت در کنترل، نفوذ و مدیریت امور مالی و انجام مبادلات بر عهده دارد، بانک‌ها سهم بسزایی در توسعه کشورها ایفا می‌نمایند و می‌توانند در پیشرفت اقتصاد کشور نقش تسهیل کننده داشته باشند، لذا سهمی قابل توجه در ایجاد این تغییرات داشته و نقشی پررنگ را بر عهده دارند [۲].

همانطور که بیان گردید تجارت با سرعتی چشمگیر دارد جایگاه خود را به تجارت الکترونیک می‌دهد و بانکداری الکترونیک یکی از مهم‌ترین ابزار در تجارت الکترونیک می‌باشد. استفاده از بانکداری الکترونیک منجر می‌گردد فعالیت‌های مالی بدون حضور فیزیکی کاربر در محل بانک و به صورت الکترونیکی انجام گردد [۳]. از مزایای بانکداری الکترونیکی می‌توان به موارد ذیل اشاره نمود:

مشتریان می‌توانند در هر لحظه به گشایش حساب اقدام نمایند و وجه مورد نظر برای گشایش حساب را، از حساب دیگر خود به حساب جدید خود انتقال دهند، امکان خرید سهام از طریق سیستم الکترونیکی بانک، امکان دریافت یا حواله انواع چک، امکان دسترسی و نظارت برحساب‌های شخصی و امکان مبادلات پول و خدمت بین مشتریان، افزایش بهداشت، کاهش آلودگی هوا، کنترل ترافیک و ارائه بهتر خدمات بانکی [۴].

این پیشرفت چشم‌گیر موجب جریان وجوه مالی بسیار زیاد از طریق کانال‌های بانکداری الکترونیک شده که این موضوع بهترین دلیل برای حضور کلاهبرداران در این وادی گردیده است. شیادان و کلاهبرداران بصورت فزاینده‌ایی در حال ورود به این محدوده با طرح‌های جدید حملات سایبری و جرایم جدید هستند و لازم است سازمان های امنیتی به صورت هوشمندانه با این موضوع برخورد نموده و امنیت در بالاترین سطح برقرار گردد، در حال حاضر بررسی این مسئله، اگرچه موضوعیت دارد اما متأسفانه در سطح پایه است. این موضوع به این واقعیت برمی‌گرددکه در وهله اول، تمام اطلاعات مربوط به حملات سایبری که در بخش بانکی انجام می‌شود محرمانه است، در عین حال، از لحاظ نظری و عملی اینگونه به نظر می‌رسد که ظهور طرح‌های جدید جعل منجر به توسعه ابزارهای جدید برای مبارزه با آن‌ها می‌شود در واقع، نوعی مسابقه میان هکرها و بخش تامین امنیت وجود دارد که می‌تواند برای همیشه ادامه داشته باشد [۵].

با در نظر گرفتن موارد مطرح شده می‌توان اینگونه عنوان نمود یکی از دغدغه‌های اصلی برای ادامه فعالیت بانکداری الکترونیکی در ایران مشکل امنیت سرمایه هاست، چراکه به اعتقاد بسیاری از آحاد جامعه یک هکر می‌تواند به سیستم بانکی نفوذ کرده و موجب خسران مشتریان و کاربران گردد.

لذا امنیت یکی از پیش نیازهای تجارت الکترونیک و به پیروی از آن بانکداری الکترونیک محسوب می‌گردد و لازمه اعتماد و اطمینان فعالان اقتصادی برای فعالیت در محیط الکترونیکی، امنیت‌الکترونیکی در سطح بالاست [۶].

حال با در نظر گرفتن جمیع جهات و با توجه به مطالبی که پیرامون بانکداری‌الکترونیک و مسئله‌ی امنیت بیان شد، به وضوح می‌توان نتیجه‌گیری کرد که انجام فعالیت‌های بانکی بصورت سنتی و خارج از شکل بانکداری‌الکترونیک امری خلاف واقع است و بانک چاره جز پیشرفت و به کارگیری روشها و ابزار مناسب در زمینه بانکداری‌الکترونیک ندارد و از سوی دیگر مسئله تامین امنیت در بانکداری‌الکترونیک به امری بسیار خطیر مبدل گردیده که می‌تواند موفقیت یا شکست را برای بانک ورق بزند. حال در پژوهش حاضر سؤال اصلی این‌گونه مطرح می‌شود که «مدل افزایش امنیت و کاهش جرایم در صنعت بانکداری‌الکترونیک چگونه است ؟».

۲-پیشینه پژوهش

۲-۱-مفاهیم اصلی پژوهش:

مدل: مدل به ما کمک می‌کند که به متن و درون پدیده‌هایی که نمی‌توانیم مستقیماً آن‌ها را ببینیم هدایت شویم. مدل جزئی کوچک یا بازسازی کوچکی از یک شیء بزرگ است که ازلحاظ کارکرد با شیء واقعی یکسان است [۷].

امنیت اطلاعات: امنیت اطلاعات شامل کنترل‌های خاص طراحی شده برای محافظت از دارایی‌های جسمی و اطلاعاتی در برابر ضرر، از بین رفتن، افشا،کپی‌کردن، فروش یا سوء استفاده‌های دیگر است[۸].

بانکداری الکترونیک: بانکداری الکترونیکی یک فناوری بانکی از راه دور است که امکان دریافت خدمات بانکی از طریق اینترنت را فراهم می‌کند. برای اتصال مشتری به سیستم بانکی اینترنتی کافی است تا به شبکه جهانی دسترسی داشته باشید و بانک و مشتری با هم قرار داشته باشند [۵]، امروزه با توجه به انجام تراکنش مالی بسیار زیاد در بانکداری الکترونیک و جابجایی ارقام قابل توجه به صورت لحظه‌ای، برقراری امنیت در بانکداری‌الکترونیک و امن نمودن انجام تراکنش‌های مالی بی شک از مهم‌ترین موضوعات در بانک می‌باشد[۹].

به‌طورکلی بانکداری‌الکترونیک عبارت است از فراهم آوردن امکاناتی برای کارکنان در جهت افزایش سرعت و کارایی آن‌ها در ارائه خدمات بانکی در محل شعبه و همچنین فرآیندهای بین شعبه‌ای و بین‌بانکی در سراسر دنیا و ارائه امکانات سخت‌افزاری و نرم‌افزاری به مشتریان که با استفاده از آن‌ها بتوانند بدون نیاز به حضور فیزیکی در بانک، در هر ساعت از شبانه‌روز از طریق کانال‌های ارتباطی ایمن و با اطمینان عملیات بانکی دلخواه خود را انجام دهند. به‌عبارت‌دیگر بانکداری الکترونیک استفاده از فناوری‌های پیشرفته نرم‌افزاری و سخت‌افزاری مبتنی بر شبکه و مخابرات برای تبادل منابع و اطلاعات مالی به‌صورت الکترونیکی است که می‌تواند باعث حذف نیاز به حضور فیزیکی مشتری در شعبه بانک‌ها شود. بانکداری الکترونیکی به زیرشاخه‌های ذیل برحسب نیاز تقسیم می‌گردد.

بانکداری اینترنتی:

بانکداری اینترنتی شیوه‌ای است که به‌طورمعمول به‌وسیله یک رایانه شخصی از طریق اینترنت به وب‌سایت بانک متصل می‌شود، صورت می‌گیرد. به‌عنوان نمونه مشتری در خانه به‌وسیله یک مودم و یک خط ارتباطی و یک سرویس‌دهنده خدمات اینترنتی به وب‌سایت بانک موردنظر خو دسترسی پیدا می‌کند.

بانکداری مبتنی بر تلفن همراه:

بانکداری موبایل از سال ۱۹۹۲در اروپا مطرح و ارائه شد و در سال ۱۹۹۹ مورد استفاده قرار گرفت، با ظهور بانکداری اینترنتی و به وجود آمدن امکان دسترسی به بانک در هر زمان اثرات بسیاری را در ارائه خدمات به مشتریان داشت ولیکن محدودیت بزرگ این نوع خدمات در دسترسی به اینترنت و تجهیزات رایانه‌ای بود که با ورود موبایل بانک این نوع محدودیت‌ها از میان برداشته شد. به همین دلیل بانکداری موبایل به‌عنوان یک مدل دیگر از بانکداری الکترونیک که نیاز مشتری را تنها با داشتن گوشی تلفن همراه تأمین می‌کند، مطرح گردید. عدم محدودیت مکانی و به‌کارگیری حداقل امکانات در استفاده از آن موبایل بانک از عوامل پیشرفت این زیرشاخه از خدمات بانکداری الکترونیک می‌باشد.

بانکداری تلفنی:

بانکداری تلفنی، عبارت است از انجام یک معامله تجاری خرد بین بانک و مشتریان از طریق تلفن. خدماتی که به‌طورمعمول یک سامانه تلفن‌بانک ارائه می‌کند عبارت است از: بررسی مانده و گردش حساب، پرداخت صورت‌حساب‌ها، مدیریت وجوه نقد، خدمات پیام، انتقال وجه نقد به سایر حساب‌ها.

بانکداری مبتنی بر دستگاه‌های خودپرداز:

ماشین‌های خودپرداز، پردازنده‌ها یا پایانه‌های الکترونیکی هستند که توسط بانک‌ها برای تسهیل کار مشتریان بانک، در مکان‌های خاص نصب می‌شوند و به‌طور ۲۴ ساعته در دسترس مشتریان می‌باشند. یک ماشین خودپرداز به‌عنوان یک شعبه از یک بانک عمل می‌کند و بسیاری از وظایف اصلی بانکداری را انجام می‌دهد. بخش عظیمی از مبادله‌ها با حداقل دخالت نیروی انسانی انجام خواهد گرفت. علاوه بر این خودپرداز به‌گونه‌ای طراحی‌شده است که به‌طور ۲۴ ساعته و بدون توقف کار می‌کند. با به‌کارگیری ماشین‌های خودپرداز در هزینه‌های کارکنان و برخی هزینه‌های سربار شعبه بانک صرفه‌جویی می‌شود.

بانکداری مبتنی بر پایانه‌های فروش:

دستگاه پایانه فروش دستگاهی است که از طریق ارتباط تلفنی یا شبکه‌ای به سیستم بانکی امکان انتقال خودکار مبلغ خریداری‌شده از حساب مشتری (دارنده کارت) به‌حساب فروشنده(پذیرنده کارت) را فراهم می‌سازد [۱۰].

۲-۲-پیشینه ی پژوهش

سنیاوسکا و همکاران در سال ۲۰۱۹ در پژوهشی با عنوان امنیت سیستم بانکی الکترونیکی به مدل سازی فرایند مقابله با کلاهبرداری در بانکداری الکترونیکی به حملات سایبری در بخش بانکی، به ویژه در زمینه بانکداری الکترونیکی پرداخته است و انواع اصلی کلاهبرداری بانکی که به صورت آنلاین انجام می‌شود در نظر گرفته شده است. محققین یک مدل ریاضی را ارائه می‌دهند که روند مقابله با کلاهبرداری در بانکداری الکترونیکی را توصیف می‌کند مدل پیشنهادی مبتنی بر مدل کلاسیک "Lotka-Volterra" که با رشد لجستیک و مدل پویا همراه است. نتایج نشان می‌دهد مدل سازی مقابله با کلاهبرداری بانکی یک مسئله کاملا پیچیده است چرا که نیاز به جمع آوری داده‌های واقعی دارد این در حالی است که آمار دقیقی از هک بانک و انواع کلاهبرداری‌های اینترنتی پیرامون بانک وجود ندارد [۵].

ابو شناب و ماتالاکا پژوهشی با عنوان"مسائل مربوط به امنیت و تقلب در بانکداری‌الکترونیک" در سال۲۰۱۵ انجام داد. هدف این پژوهش بررسی مسائل امنیتی مرتبط با بانکداری‌الکترونیک و مشخصه‌ها و چالش‌های آن بود. در این پژوهش همچنین انواع مختلف حملات، برخی از راهبردهای شناسایی فریب و کلاهبرداری و روش‌های جلوگیری و مقابله با حملات نیز مورد توجه قرار گرفت. به‌منظور شناسایی و اولویت‌بندی عوامل ازنظر خبرگان استفاده شد. یافته‌های پژوهش نشان داد که نظارت بر تراکنش‌ها به‌عنوان مؤثرترین مدل و کیبوردهای مجازی، حفاظت از مرورگر و شناسایی دستگاه به‌عنوان ضعیف‌ترین مدل‌ها شناسایی شدند [۱۱].

لوکی در سال ۲۰۱۵ در پژوهشی با عنوان "مزایا و تهدیدات امنیتی در بانکداری الکترونیکی" اعلام نمود: بانکداری اینترنت در حال تغییر در صنعت بانکداری است و این مهمترین اثر را در بانکداری دارد. روابط اکنون در بانکداری محدود به شعب نمی شود. چالش هایی که موجب مخالفت بانکداری الکترونیکی هستند عبارتند از نگرانی‌های مربوط به امنیت و حفظ حریم اطلاعات است. تمرکز

فعلی بر امنیت انتقال اطلاعات بر روی پروتکل‌ها و نقص در محاسبات انتهایی تا پایان است [۱۲].

لی و همکاران در پژوهشی با عنوان"بررسی امنیت بانکداری‌اینترنتی و اطلاعات خصوصی مالی در کره‌جنوبی"سیستم صدور گواهینامه در کره‌جنوبی را در سال ۲۰۱۳ مورد بررسی قرار داد. برای فعال سازی زیرساخت‌های تجارت‌الکترونیکی ایمن، این قانون به امضاهای دیجیتالی اثر حقوقی داد، و زمینه ای برای تجارت الکترونیکی ایمن از جمله پرداخت‌های آنلاین و اقدامات دیگر. با این‌حال، اکنون که دستگاه‌های قابل حمل مانند تلفن‌های هوشمند و رایانه‌های شخصی تبلت به سرعت در حال تجاری شدن هستند و بازارهای مرورگر با استفاده از اینترنت متنوع‌تر می‌شوند، قابلیت دسترسی و سازگاری بانکداری‌اینترنتی کره برای کاربران با محور OpenWeb به مسائل مهم تبدیل شده است. این اقدام بسیار جدید است و انتظار می‌رود فرصتی برای بررسی مسائل امنیتی در صنعت مالی کره فراهم کند. علاوه بر این، تلاش‌های مداوم در صنعت مالی برای ارائه خدمات بانکی با استفاده از فناوری‌اطلاعات وجود دارد. با این‌حال، برخی از کاربران ادعا می‌کنند که مشکلات امنیتی اساسی در بانکداری‌اینترنتی کره وجود دارد بنابراین، نویسنده می‌خواهد یک بحث عینی در مورد این ادعاهای گمراه کننده ارائه دهد [۱۳].

در سال ۲۰۱۳، کومارومیتال در پژوهشی با عنوان "امنیت بانکداری‌الکترونیکی و چالش‌ها " به بررسی استفاده از فناوری اطلاعات (IT) برای راحت‌تر کردن زندگی پرداخت. در بانکداری‌اینترنتی، مرورگرهای وب رابط کاربری ساده و کاربر پسند را به مشتریان ارائه می‌دهند. در این مقاله به بررسی امنیت و چالش‌های مورد نیاز کلیه بانک‌ها در بانکداری‌اینترنتی پرداخته شده است. مانند ارائه دهندگان خدمات فناوری در سطح جهان، سیستم عامل‌های ابری را که نقاطی برای راه‌حل‌های مقرون به صرفه باز کرده‌اند. پیشگیری از جرایم سایبری اصلی‌ترین چالش برای بانک‌های دارای خدمات مناسب مشتری است [۱۴].

اومریبا و همکارانش پژوهشی با عنوان "امنیت و حفظ حریم خصوصی بانکداری‌الکترونیکی" انجام داد. او در این مطالعات به بررسی نقش اساسی اینترنت در تغییر نحوه تعامل با افراد دیگر و نحوه انجام فعالیت‌ها پرداخت. نتایج حاصل‌شده نشان می‌دهد به دلیل وجود اینترنت، تجارت الکترونیکی پدید آمده و به تجارت اجازه می‌دهد تا با مشتریان و شرکت‌های دیگر در داخل و خارج از آن‌ها ارتباط برقرار کنند. صنایع صنعتی که از این کانال ارتباطی جدید برای دستیابی به مشتریان خود استفاده می‌کند، چندین روند نوظهور را مورد بررسی قرار می‌دهند: تقاضای مشتری برای هر زمان، ارائه خدمات در هر مکان، ضروریات زمان نسبت به بازار و چالش مربوط به امنیت اطلاعات و حریم خصوصی. در این مقاله ابتدا به بحث در مورد بانکداری نوین پرداخته می‌شود. دوم، در مورد نگرانی در مورد بانکداری‌الکترونیکی از دیدگاه‌های مختلف صحبت خواهدکرد. ثالثاً، در مورد مسائل امنیتی و حریم خصوصی نیز بحث خواهدشد و چهارم اینکه، حملات بانکداری با راه‌حل‌های آن‌ها بحث شده است. این تحقیقات در سال ۲۰۱۳ انجام گردید [۱۵].

تو وان وآهنکورا در سال ۲۰۱۲ در پژوهشی با عنوان "استراتژی امنیت بانکداری‌الکترونیکی: امنیت و اعتماد مشتری" عنوان نمود استراتژی‌های بانکداری‌اینترنتی باید تجربیات آنلاین مشتریان را که تحت تأثیر مسائل اعتماد و امنیت قرار می‌گیرند، تقویت کند. این مطالعه، چشم اندازهای کاربران و غیر استفاده کنندگان از امنیت بانکی اینترنتی را با هدف درک اعتماد و عوامل امنیتی در رابطه با استفاده مداوم ارائه می‌دهد. درک امنیت بانکداری‌اینترنتی روی اهداف استفاده تأثیر داشته است. غیر استفاده کنندگان، بانکداری‌اینترنتی را ناامن می‌دانند، اما سهولت استفاده از آن بر استفاده مداوم از آن تأثیر می‌گذارد. درک امنیت بانکداری‌اینترنتی از اعتماد به سیستم بانکی اینترنتی، اعتماد به ارائه دهنده، آگاهی از تهدید، در دسترس بودن اطلاعات و آموزش تأثیر مثبت داشت اما با سن رابطه منفی نشان داد. این مطالعه نشان می‌دهد که استراتژی امنیت بانکداری‌اینترنتی ممکن است شکاف نسل در اتخاذ را در نظر بگیرد و باید به طور مداوم در جهت اطمینان از اعتماد مشتریان از نام تجاری آنلاین ارائه دهندگان، از جمله ارائه اطلاعات امنیتی و آموزش باشد [۱۶].

موسکاتو و آل اسچولر در پژوهشی با عنوان "برداشت‌های بین المللی از بانکداری آنلاین و نگرانی‌های امنیتی" نگرانی در مورد امنیت را یکی از مهمترین عوامل مؤثر در تصویب امنیت بانکداری آنلاین عنوان نموده است، بنابراین ضروری است که بانک‌های آنلاین از اقدامات امنیتی مناسب استفاده کنند. این تحقیقات برخی از تفاوت‌های قابل توجه بین نگرانی‌های امنیتی مورد انتظار در نقاط مختلف جهان را آشکار می‌کند. اگر بانک‌ها از پیش زمینه تجارت‌الکترونیکی مخاطبان مورد نظر خود مطلع شوند، می‌توانند اطلاعات بیشتری کسب کنند به طور مؤثر امنیت را مدیریت کنید. این پژوهش در سال ۲۰۱۲ به اتمام رسید [۱۷].

کلیسنس و همکاران در پژوهشی با عنوان " امنیت سیستم‌های بانکی الکترونیکی آنلاین" که در سال ۲۰۰۲ صورن پذیرفت، به پیشرفت سریع فناوری فعلی اشاره می‌نماید و بیان میدارد امروزه دائماً ابعاد جدیدی توسط این فناوری به زندگی روزمره ما وارد می‌شود. سیستم‌های بانکی الکترونیکی دسترسی آسان به خدمات بانکی را در اختیار ما قرار می‌دهند. تعامل بین کاربر و بانک با استقرار دستگاه‌های خودپرداز، بانکداری‌تلفنی، بانکداری‌اینترنتی و اخیراً بانکداری تلفن‌همراه بطور قابل توجهی بهبود یافته است. این مقاله به بحث در مورد امنیت سیستم‌های بانکی الکترونیکی امروز است. در این پژوهش تمرکز بر بانکداری‌اینترنتی و موبایل است و

یک مرور کلی و ارزیابی از تکنیک‌های مورد استفاده در سیستم‌های فعلی ارائه می‌شود [۱۸].

کیداو گویال در سال ۲۰۱۸ در پژوهشی با عنوان "چالش‌های سیستم بانکداری غیر نقدی: بررسی تجربی بانک‌های نیجریه و هند" نشان داد که عوامل ناکارآمدی دستگاه مشکلات فنی، کمبود سرمایه‌گذاری در توسعه زیرساخت‌ها و کسری بودجه ازجمله چالش‌های مؤثر بر بانکداری‌الکترونیک می‌باشند. نمونه آماری این پژوهش را ۳۲۴ نفر تشکیل می‌دادند که از هریک از دو کشور نیجریه و هند به تعداد ۱۶۲ نفر و به روش نمونه‌گیری تصادفی ساده انتخاب شدند؛ که از میان پرسشنامه‌های توزیع شده، تعداد ۲۹۴ مورد عودت داده شد [۱۹].

۲-۳-اهم جرایم حوزه بانکداری‌الکترونیکی

جرایم حوزه بانکداری‌الکترونیکی بطور معمول باهدف ایجاد اختلال در عملکرد تجهیزات، تغییر در نحوه کنترل فرایند پردازش، اختلال در عملکرد رایانه‌ها و سرویس‌دهنده، یا از بین بردن داده‌های ذخیره شده در سرورهای سازمان در راستای سرقت، کلاهبرداری و یا اعمال خرابکارانه صورت می‌پذیرد. در جدول (۱)، به اهم جرایم الکترونیکی در حوزه بانکداری‌الکترونیک اشاره گردیده است[۱۰].

جدول (۱): اهم جرایم بانکداری‌الکترونیکی[۱۰].

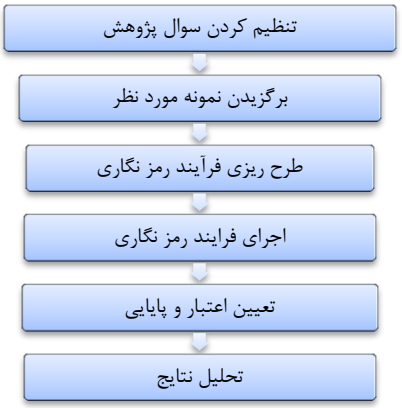
ردیف	نام	تعریف
۱	فیشینگ	فرآیندی است که فرد متخلف را قادر می‌سازد تا با جلب اعتماد کاربر، اطلاعات شخصی،کلمه عبور و همچنین اطلاعات مالی محرمانه را در اختیار فرد شیاد قرار دهد.
۲	فارمینگ	فارمینگ حمله نفوذگر به‌منظور تغییر ترافیک وب‌سایت به یک وب‌سایت جعلی دیگراست.
۳	تروجان	برنامه‌های غیرمجازی هستند که از درون مانند برنامه‌های مجاز به نظر می‌آیند. درنتیجه آنچه واقعاً اجرا می‌شود پنهان می‌گردد. این برنامه در معماری سرویس‌دهنده - سرویس‌گیرنده روی کامپیوترهای قربانی و هکر به ترتیب نصب می‌گردد و هکر عملیات نظارت و کنترل را روی کامپیوتر قربانی انجام می‌دهد.
۴	جعل‌عنوان	جعل عنوان ازجمله موارد سوءاستفاده به شمار می‌آید که از مشخصه‌های فردی شخص دیگر مانند نام،شماره ملی،شماره کارت‌اعتباری به‌منظور انجام امور مجرمانه، کلاه‌برداری یا سرقت سوءاستفاده شود.
۵	هک	دسترسی غیرمجاز به سیستم‌های کامپیوتری و شبکه‌های کامپیوتری است.
۶	اسکیمینگ	فرآیند کپی‌کردن اطلاعات نوارمغناطیسی کارت اعتباری مشتری از طریق کشیدن کارت از میان کارت‌خوان و استفاده از اطلاعات جهت ساخت کارت تقلبی توسط فرد شیاد را اسکیمینگ گویند.
۷	شُولدِر سُرفینگ	دزدیدن کلمه عبور دارنده کارت به هنگام استفاده از دستگاه خودپرداز یا پایانه‌فروش از طریق نگاه زیرچشمی از بالا به کاربر در حین وارد نمودن کاراکترها را شامل می‌شود.
۸	فیشینگ	در دستگاه‌های خودپرداز نصب قطعه‌هایی شبیه
	خودپرداز	دستگاه خودپرداز بر روی دستگاه ذهن صاحب کارت را منحرف می‌کنند که عملیات وی با دستگاه مجاز صورت می‌گیرد.
۹	حلقه لبنانی	شیاد با قرار دادن یک قطعه در مدخل ورودی کارت‌خوان و قرارگرفتن پشت سر مشتری نسبت به سرقت کارت و کلمه عبور اقدام می‌نماید.
۱۰	کارت‌خوان‌های سارق	از طریق نصب مدارهای مغناطیسی روی دستگاه‌های پوز اطلاعات کارت مشتریان را در حافظه جانبی مدار ذخیره کرده و سپس با استفاده از دستگاه کارت‌خوان اطلاعات حساب مالباختگان را دریافت و سپس با استفاده از کارت جعلی ساخته‌شده اقدام به برداشت وجه و خرید اینترنتی می‌کنند.
۱۱	تقدیم رمز به فروشنده	متأسفانه بسیاری از کارت‌خوان‌های فروشگاهی دور از دسترس خریداران قرار دارد و صاحب مغازه خود اقدام به پرداخت از طریق دستگاه کارت‌خوان باکارت مشتری می‌نماید.
۱۲	اسکیمر در دستگاه‌های پوز	کپی کردن غیرقانونی داده‌های نوار مغناطیسی کارت‌بانکی در حین کشیده شدن در دستگاه کارت‌خوان.
۱۳	ویشینگ	از طریق تماس صوتی فرد قربانی را ترغیب به افشا اطلاعات مهم کند.
۱۴	اس میشینگ	از طریق پیام کوتاه درخواست جعلی برای افشای اطلاعات مهم فرستاده شود.
۱۵	ام ای‌اتی ام	در این نوع حمله، حمله‌کننده با ایجاد اتصال‌های مستقل با قربانیان، بین دو قربانی(مشتری و بانک) قرار می‌گیرد و اطلاعات رد و بدل شده بین این‌ها را استراق سمع کرده و تغییر می‌دهد و مجدداً ارسال می‌کند.
۱۶	کدهای مخرب	نرم‌افزارهایی به شکل ویروس، کرم و بدافزار که معمولاً به صورت مخفی بر روی گوشی، دروازه سرویس پیام کوتاه یا سرور بانک بارگذاری می‌شوند تا فرایندهای تعیین هویت نشده را که اثر منفی بر روی قابلیت اعتماد، یکپارچگی و دسترسی اطلاعات کاربر دارد، انجام شود.
۱۷	کلونینگ	هویت تلفن همراه را بر روی دیگری کپی می‌کند و به هکر اجازه می‌دهد که خود را با هویت قربانی جا بزند(مثلاً از طرف قربانی تماس‌های صوتی برقرار کند) تا بتواند به‌حساب مالی قربانی دسترسی داشته باشد.

۳- روش شناسی پژوهش

روش پژوهش حاضر از نظر هدف کاربردی و از نظر روش اجرا آمیخته می‌باشد. روش پژوهش ترکیبی روش است که در آن تمامی مراحل تحقیق بر ترکیب دو نوع روش کیفی و کمی جهت دستیابی به مطالعه دقیق تاکید دارد [۲۰].

در بخش کیفی به منظور پیداکردن چارچوب مناسب عوامل مؤثر بر امنیت اطلاعات در بانکداری‌الکترونیک، ابتدا با استفاده از روش کتابخانه‌ای به بررسی و مرور جامع مطالعات مرتبط با موضوع و مدل‌ها و تئوری‌های موضوع پرداخته شد و نظر خبرگان این حوزه با استفاده از مصاحبه عمیق نیمه‌ساخت یافته اخذ گردید و به همین‌منظور از روش تحلیل محتوای کیفی جهت دسته‌بندی

شاخص‌ها استفاده گردید. روش تحلیل محتوای کیفی را می‌توان روش تحقیقی برای تفسیر ذهنی محتوایی داده‌های متنی از طریق فرایندهای طبقه بندی نظام‌مند، کدبندی و تم‌سازی یا طراحی الگوهای شناخته شده دانست [۸]. گام‌های تحلیل محتوای کیفی که در این تحقیق طی خواهند شد در شکل (۱) به تصویر کشیده شده است [۲۱].



شکل (۱): مراحل تحلیل محتوا کیفی [۲۱].

بخش کمی نیز در ۵ مرحله به شرح ذیل انجام گردید:

مرحله اول: بررسی مبانی نظری و پیشینه‌ی تحقیق.

مرحله دوم: شناسایی ابعاد و گویه‌های سنجش متغیرها.

مرحله سوم: سنجش روایی و پایایی مقیاس: در این گام مشخص می‌شود آیا پرسشنامه‌ی مورد استفاده برای گردآوری داده‌های مورد نظر در جامعه‌ی آماری از اعتبار (روائی و پایائی) کافی برخوردار است.

مرحله چهارم: طراحی و آزمون مدل نهائی تحقیق: ترسیم مدل رابطه بین متغیرها با تکنیک مدل معادلات ساختاری و آزمون فرضیه‌های تحقیق.

مرحله پنجم: نتیجه‌گیری و ارائه پیشنهادات مرتبط با یافته‌های تحقیق.

۳-۱- جامعه آماری، حجم نمونه و روش نمونه گیری:

برای نمونه‌گیری در بخش کیفی جهت انجام مصاحبه عمیق با خبرگان، از روش نمونه‌گیری گلوله‌برفی استفاده گردیده است.در زمینه هایی که مسائل پنهان بسیاری وجود داشته و قصد ما شناسایی افراد متخصص در یک‌رشته یا زمینه خاص به منظور استخراج دانش آن‌ها باشد،از روش گلوله برفی استفاده می‌گردد[۲۲]. جامعه آماری بخش کیفی متشکل از ۱۵ نفر از خبرگان ارشد در امنیت بانکداری الکترونیک که به موضوع اشراف داشته، دارای تحصیلات دکتری یا کارشناسی ارشد، دارای تجربیات پژوهشی و آموزشی و از مدیران یا خبرگان در زمینهٔ مذکور بوده اند. به‌منظور حصول اطمینان از کفایت و کیفیت داده‌ها مصاحبه تا هجده نفر ادامه یافت و از مصاحبه پانزدهم به بعد اطلاعات جدیدی حاصل نگردید.

جامعه آماری در بخش کمی از کارکنان شعب بانک سپه و مجریان حوزه امنیت اطلاعات در بانک سپه انتخاب شده اند،تعداد آن‌ها ۱۲۳ نفر بود که در سال ۱۳۹۹ در این پژوهش مشارکت نمودند. به دلیل محدودیت اعضای جامعه آماری و اهمیت موضوع از نمونه‌گیری تمام شمار استفاده شد.

همانطور که بیان گردید: ۱۲۳ نفر از کارکنان شعب بانک سپه واجد الشرایط برای شرکت در پژوهش می‌باشند، بنابراین حجم نمونه ۱۲۳ می‌باشد.

منظور از افراد واجد شرایط،کارکنان مشغول به کار درشعب بانک سپه و مجریان حوزه امنیت در بانک سپه می‌باشد که دارای مدرک تحصیلی کارشناسی یا بالاتر بوده،در حوزه بانکداری‌الکترونیک بطور عملی در حال فعالیت می‌باشند و با چالش ها، مزایا، معایب و مشکلات این مهم از نزدیک در ارتباط هستند. سابقه فعالیت این افراد از ۱۰سال تا ۳۰سال می‌باشد.

در این پژوهش با دو روش میدانی و کتابخانه‌ای اطلاعات مورد نظر جمع‌آوری شده است. ابزار گردآوری اطلاعات در این دو روش شامل:

الف- مطالعات اسنادی و کتابخانه‌ای ب- منابع الکترونیکی و سایت‌های علمی تخصصی ج- استفاده از پرسشنامه می‌باشد.

پرسشنامه پژوهش کمی، در سطح اندازه‌گیری طیف لیکرت می‌باشد.

۳-۱-۱-اطلاعات دموگرافیک نخبگان شرکت کننده در پژوهش:

در این پژوهش ۱۸ نفر از متخصصین و نخبگان حوزه امنیت بانکداری‌الکترونیک شرکت داشته‌اند. اطلاعات حاضرین در پژوهش به شرح جدول (۲) می‌باشد. همان‌طور که ملاحظه می‌نمایید سعی گردیده است افراد دعوت‌شده از متخصصین و افراد خبره در زمینه بانکداری‌الکترونیک با تخصص‌های گوناگون بوده تا موارد مطروحه در پژوهش از تمامی ابعاد مورد بررسی و واکاوی قرار بگیرد.

جدول (۲): اطلاعات دموگرافیک نخبگان شرکت کننده در پژوهش

ردیف	جنسیت	سابقه	سمت	مدرک تحصیلی
۱	مرد	۲۷ سال	مدیر بانک	کارشناسی ارشد
۲	مرد	۱۵سال	برنامه نویس (هیئت علمی)	دکتری
۳	مرد	۱۷سال	پلیس فتا (رئیس اداره)	کارشناسی ارشد
۴	مرد	۲۲سال	مدیر عامل گروه تحقیقاتی	دکتری
۵	مرد	۲۳سال	حراست فناوری‌اطلاعات‌بانک	کارشناسی ارشد
۶	مرد	۲۹سال	مدیر شرکت امنیت شبکه	دکتری
۷	مرد	۱۸سال	مدیر عامل شرکت تامین امنیت	کارشناسی ارشد
۸	مرد	۱۷سال	متخصص الکترونیک(هیئت علمی)	دکتری

۹	مرد	۱۷سال	حراست بانک	کارشناسی ارشد
۱۰	زن	۱۸سال	متخصص شبکه بانک	کارشناسی ارشد
۱۱	زن	۱۹سال	مدیریت شعبه بانک	دکتری
۱۲	مرد	۲۹سال	پلیس مبارزه با جرائم اقتصادی	کارشناسی ارشد
۱۳	مرد	۱۹سال	طراح پروتکل‌های امنیت شبکه	کارشناسی ارشد
۱۴	مرد	۲۳سال	طراح پروتکل‌های امنیت	دکتری
۱۵	مرد	۱۹سال	حقوقدان بانک	کارشناسی ارشد
۱۶	مرد	۲۷	مدیر بخش حسابرسی	کارشناسی ارشد
۱۷	مرد	۱۷	بازرس	کارشناسی ارشد
۱۸	مرد	۱۵	کسب و کار الکترونیک	کارشناسی ارشد

۴-نتایج پژوهش

۴-۱-نتایج بخش کیفی

تجزیه و تحلیل اطلاعات به دست آمده از مصاحبه، از روش تحلیل محتوای کیفی است. در این روش محقق بر اساس ادراک و فهم خود از متن مورد مطالعه، نوشتن تحلیل اولیه را آغاز نموده و این کار ادامه می‌یابد تا پیش زمینه‌هایی برای ظهور رمزها آغاز شود. این عمل اغلب موجب می‌شود که طرح ریزی رمزها از متن ظهور یابد و سپس براساس شباهت‌ها و تفاوت‌ها مقوله‌بندی شوند. این مقوله‌بندی از سازماندهی و گروه‌بندی کردن رمزها به صورت خوشه‌های معنادار دسته‌بندی می‌شود. بسته به کیفیت ارتباط بین زیر مقوله‌ها، محقق می‌تواند با ترکیب و سازماندهی این زیر مقوله‌ها، آن‌ها را به شمار کمتری از دسته‌بندی (مقوله) تبدیل کند [۲۲, ۲۳]. در مرحله بعدی تعاریفی برای هر مقوله و زیرمقوله و رمز صورت می‌گیرد. برای تهیه گزارش از یافته‌ها، مثال‌هایی برای رمزها و مقوله‌ها از روی داده‌ها مشخص می‌شود. بسته به هدف تحقیق، محققان تصمیم می‌گیرند ارتباطی بین مقوله‌ها و زیر مقوله‌های بیشتر براساس موافقت بین خود، پیشینه موضوع با سلسله مراتب بین داده‌ها مشخص کنند [۲۴, ۲۵].

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

۴-۲-نتایج بخش کمی

در بخش کمّی، از ابزار پرسشنامه در قالب سوالات بسته طراحی شده در سطح اندازه‌گیری طیف لیکرت در مؤلفه‌های رمزدوم پویا، استفاده از متخصصین، استفاده از ایزوها، فرهنگ‌سازی مناسب، آموزش جامع، تقویت زیر ساخت‌های امنیتی، به روز بودن سیستم بانکداری برای گردآوری اطلاعات استفاده شده است. جهت ارزیابی روایی، پس از تنظیم پرسشنامه و طراحی سوالات جهت اندازهگیری متغیرهای مورد مطالعه، سوالات توسط اساتید راهنما و مشاورین، و نیز ۱۵ نفر از متخصصین و خبرگان مرتبط با موضوع پژوهش، مورد ارزیابی قرار گرفت و پس از اعمال نظر آنها، پرسشنامه نهایی تنظیم شده است. همچنین جهت سنجش پایایی از آلفای کرونباخ استفاده شده است که در نهایت با توجه به این‌که ضرایب به‌دست آمده بزرگ‌تر از ۰/۷۰ می‌باشد، پایایی ابزار قابل قبول بوده و این موضوع نشان‌دهنده همبستگی درونی بین متغیرها برای سنجش مفاهیم موردنظر می‌باشد. و بدین ترتیب می‌توان گفت که ابزار تحقیق حاضر از قابلیت اعتماد و یا پایایی لازم برخوردار است. در جدول (۳) میزان پایایی پرسش‌نامه‌ها از طریق آلفای کرونباخ نشان داده شده است.

جدول (۳): میزان پایایی پرسش‌نامه‌ها از طریق آلفای کرونباخ

متغیر / ابعاد	تعداد گویه‌ها	آلفای کرانباخ
رمز دوم پویا	۵	۰/۷۳۹
کارکردایزوها	۵	۰/۷۴۲
فرهنگ سازی	۳	۰/۷۱۱
آموزش جامع	۴	۰/۷۹۳
تقویت زیر ساخت‌های امنیتی	۵	۰/۷۲۱
به روز بودن سیستم بانکداری‌الکترونیک	۵	۰/۷۱۰
استفاده از متخصصین	۳	۰/۷۹۳

۴-۲-۱- معادلات ساختاری برای تایید نهایی مدل تحقیق

در شکل (۲) میزان بار عاملی در برآود مدل برای هریک از سوالات مشخص شده است. برای متغیر رمز دوم پویا از ۱- امنیت در بانکداری‌الکترونیکی را تاحد بسیار زیادی افزایش داده است(RD1). ۲- از نقاط ضعف آن می‌توان به پیچیدگی و دشوار بودن آن اشاره نمود(RD2). ۳- امکان انجام فیشینگ را کاهش داده است(RD3). ۴- در مبارزه با پولشویی نیزمفید است.(RD4). ۵- استفاده از رمز پویا برای کسانی که مسن هستند سخت و زمانبر است(RD5).

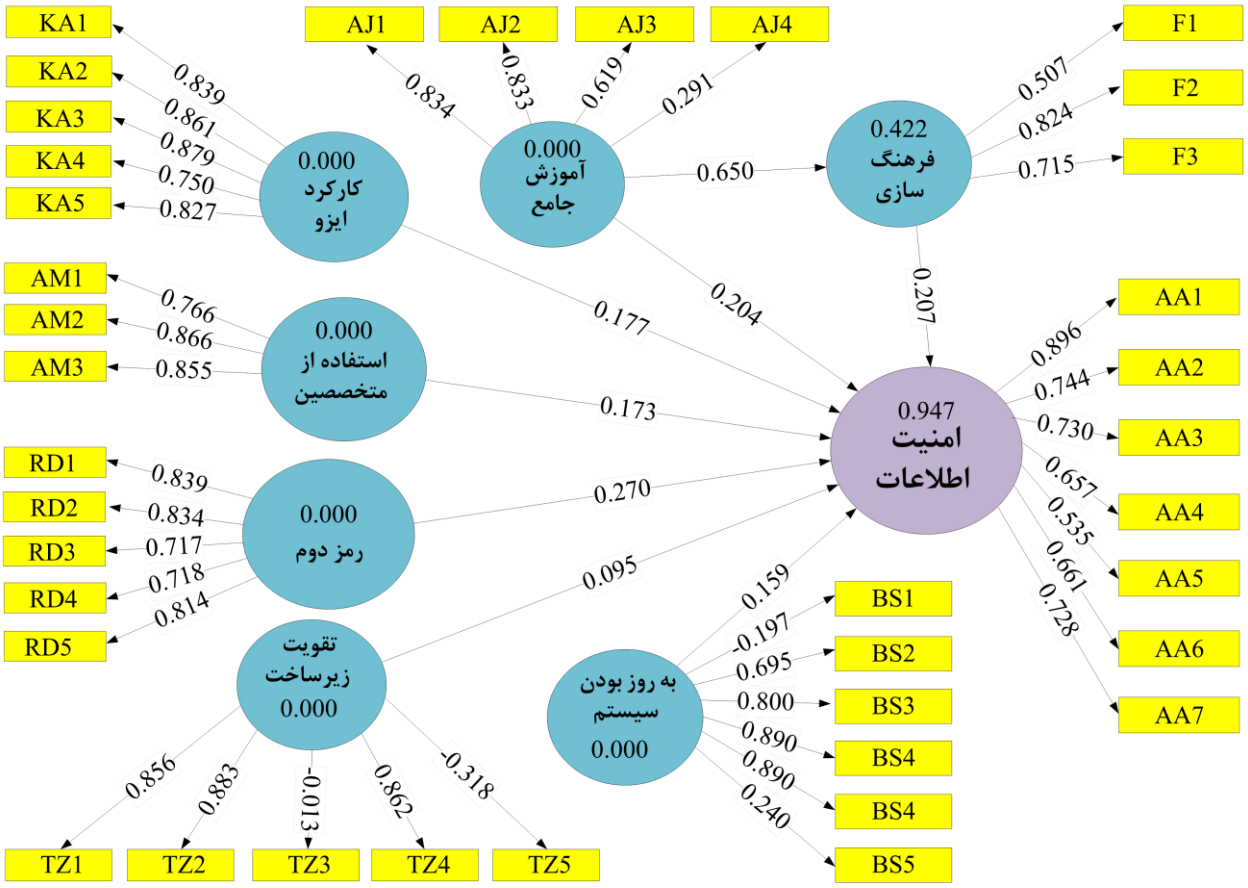
میزان بار عاملی برای هر یک از سوالات به ترتیب سوال اول ۰/۸۳۹، دوم ۰/۸۳۴، سوم ۰/۷۱۷،چهارم ۰/۷۱۵ و پنجم ۰/۸۱۴ می‌باشد بنابراین می‌بینم که مقدار بار عاملی برای همه سوالات متغیر رمز دوم پویا بیش از ۰/۳۰ می‌باشد.بنابراین می‌توان گفت همه سوالات متغیر رمز دوم پویا دارا بارعاملی مناسبی در مدل برآودی می‌باشند.

برای متغیر کارکرد ایزوها از ۱- به وسیله ایزوها تهدیدهای امنیتی تشخیص داده می‌شود (KA1). ۲- افزایش امنیت در عملیات بانکداری‌الکترونیک یکی از مزایای پیاده سازی ایزو ۲۷۰۰۱

می‌باشد(KA2). ۳-ایزو ۲۷۰۰۱ از جرایم محلی و منطقه‌ایی جلوگیری می‌کند(KA3). ۴- از مهم ترین کارایی ایزوها آماده سازی زیرساخت مناسب سخت افزاری و نرم افزاری است. (KA4). ۵- ایزوها کنترل‌های امنیتی را پیاده سازی می‌کنند(KA5). میزان بار عاملی برای هر یک از سوالات به ترتیب سوال اول ۰/۸۳۹، دوم ۰/۸۶۱، سوم ۰/۸۷۹،چهارم ۰/۷۵۰ و پنجم ۰/۸۲۷ می‌باشد بنابراین می‌بینم که مقدار بارعاملی برای همه سوالات متغیر کارکرد ایزوها بیش از ۰/۳۰ می‌باشد. بنابراین می‌توان گفت همه سوالات متغیر کارکرد ایزوها دارای بارعاملی مناسبی در مدل برآودی می‌باشند.

برای متغیر کارکرد ایزوها از۱- هر جامعه‌ای فرهنگ مختص به خودش را دارد، بومی‌سازی در زمینه امنیت بانکداری می‌تواند موثر باشد(F1). ۲- فرهنگسازی برای ترک عادات سنتی غلط به کار می‌رود(F2). ۳- فرهنگ‌سازی غنی در زمینه نکات امنیتی می‌تواند امنیت را تا حد زیادی افزایش دهد(F3). میزان بارعاملی برای هر گفت همه سوالات متغیر فرهنگ‌سازی دارای بارعاملی مناسبی در مدل برآودی می‌باشند.

برای متغیر آموزش جامع از۱- اگر آموزش در قالب رفع نیازهای جامعه به صورت جذاب جالب و از طریق آموزش‌های بصری انجام گردد، بسیار موثر واقع خواهد شد(AJ1). ۲- تشویق مردم و اهدای جوایز به افراد علاقمند به یادگیری در حوزه امنیت بانکداری می‌تواند مفید باشد(AJ2). ۳- آموزش در رسانه‌ها و حتی مدارس می‌تواند نکات ایمنی در استفاده از همراه بانک‌ها و ..را به کاربران بیاموزند(AJ3). ۴- آموزش مناسب برای کاربران از طریق بروشور درشعب و فیلم‌های تبلیغاتی می‌تواند مفید باشد(AJ4). میزان بار عاملی برای هر یک از سوالات به ترتیب سوال اول ۰/۸۳۴، دوم ۰/۸۳۳، سوم ۰/۶۱۹ و چهارم ۰/۲۹۱ می‌باشد، بنابراین می‌بینم که مقدار بار عاملی برای همه سوالات متغیر آموزش جامعه بیش از ۰/۳۰ می‌باشد به غیر سوال ۴ که این مقدار بار چرخش عاملی برای سوال کفایت نمی‌کند، در نتیجه از مدل برآودی حذف می‌شود.



شکل (۲): معادلات ساختاری برای تایید نهایی مدل تحقیق

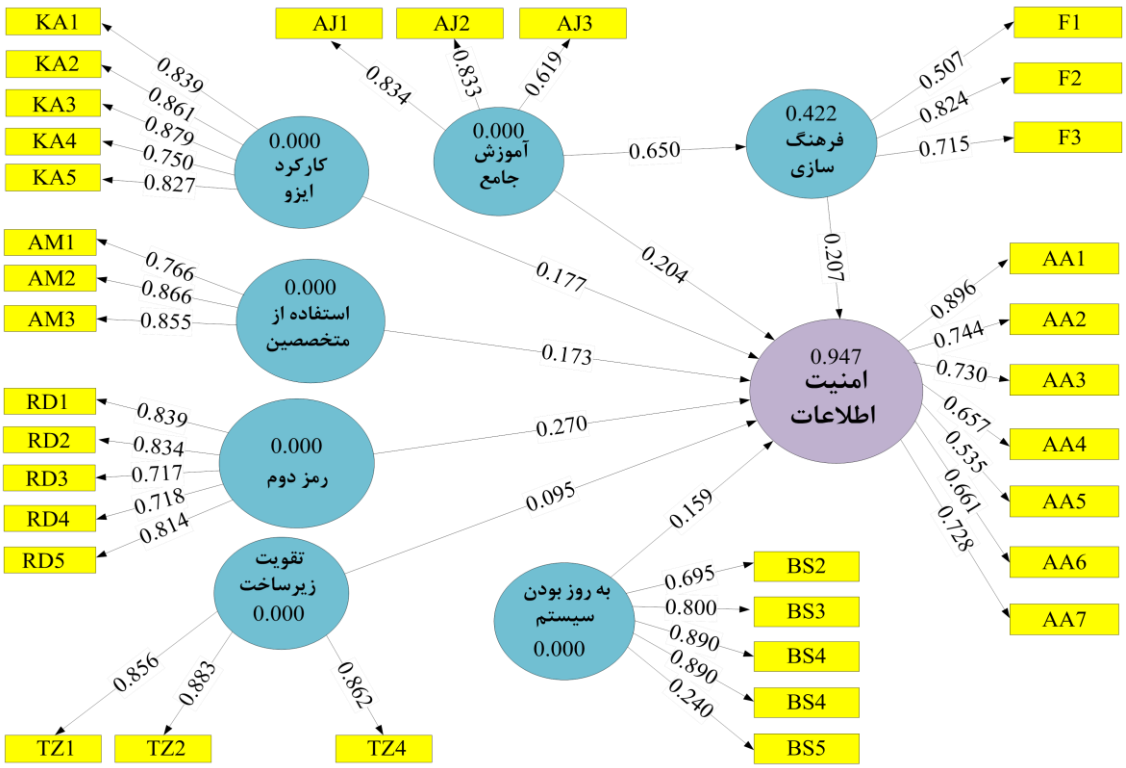
یک از سوالات به ترتیب سوال اول ۰/۵۰۷، دوم ۰/۸۲۴، سوم ۰/۷۱۵ می‌باشد. بنابراین می‌بینم که مقدار بار عاملی برای همه سوالات متغیر فرهنگ‌سازی بیش از ۰/۳۰ می‌باشد. بنابراین می‌توان

برای متغیر تقویت زیر ساختها از ۱- اولین قدم در تامین امنیت ایجاد زیر ساخت‌های امنیتی قوی در بانکداری‌الکترونیک است(TZ1). ۲- استفاده از طراحان و برنامه نویسان حرفه‌ای باعث می‌شود هکرها کمتر بتوانند در سیستم‌های بانکی نفوذ

کنند(TZ2). ۳- ایجاد پروتکل‌های امنیتی در بخش data senter بانک برای تأمین امنیت داخلی بانک بسیار اهمیت دارد(TZ3). ۴- محرمانگی اطلاعات و پروتکل‌ها باید حفظ شود ودر اختیار اکثریت کارکنان قرار نگیرد(TZ4). ۵- وجود بستر و زیر ساخت مناسب برای سرورها و نرم افزارهای بانکداری‌الکترونیک و ایجاد لایه‌های حفاظتی مناسب الزامی است(TZ5). میزان بار عاملی برای هر یک از سوالات به ترتیب سوال اول ۰/۸۵۶، دوم ۰/۸۸۳، سوم ۰/۰۱۳، چهارم ۰/۸۶۲ و وسوال پنجم ۰/۳۱۸ می‌باشد بنابراین می‌بینم که مقدار بار عاملی سوالات ۱ و۲ و ۴ بیش از ۰/۳۰ می‌باشد که این میزان مقدار مناسبی می‌باشد ولی مقدار بارعاملی برای سوالا ۳و۵ کمتر از ۰/۳ بوده که این مقدار برای سوال کفایت نمی‌کند. در نتیجه از مدل برآودی حذف می‌شوند.

برای متغیر به روز بودن سیستم در بانکداری‌الکترونیک از ۱- سیستم بانکداری‌الکترونیک باید با استانداردهای روز جهانی مطابقت داشته باشد(BS1). ۲- برای تامین امنیت داخلی(دستبرد کارمندان) استفاده از داده‌کاوی وسیستم‌های بازرسی سیستمی به است(BS5). میزان بار عاملی برای هر یک از سوالات به ترتیب سوال اول ۰/۱۰۷، دوم ۰/۶۹۵، سوم ۰/۸۰۰، چهارم ۰/۸۹۰ و وسوال پنجم ۰/۸۹۰ می‌باشد بنابراین ملاحظه می‌گردد، مقدار بار عاملی سوالات ۲ الی ۵ بیش از ۰/۳۰ می‌باشد که این میزان مقدار مناسبی می‌باشد ولی مقدار بارعاملی برای سوال ۱ کمتر از ۰/۳ بوده که این مقدار برای سوال کفایت نمی‌کند.در نتیجه از مدل برآودی حذف می‌شوند.

برای متغیر استفاده از متخصص از۱- استفاده از متخصصین در بانکداری‌الکترونیک راه‌های سرقت را کاهش می‌دهد (AM1). ۲- برگزاری جلسات مهم با متخصصان امر امنیت از جمله کارهای ضروری برای تامین امنیت در بانکداری‌الکترونیک است(AM2). ۳- از افرادی که در بحث امنیت اطلاعات مشغول به کار هستند باید در بانک سپه بیش از پیش استفاده شود(AM3). میزان بار عاملی برای هر یک از سوالات به ترتیب سوال اول ۰/۷۶۶، دوم ۰/۷۶۵، سوم ۰/۸۵۵ می‌باشد بنابراین می‌بینم که مقدار بار عاملی برای همه سوالات متغیر استفاده از متخصص بیش از ۰/۳۰ می‌باشد.بنابراین



شکل (۳): مدل نهایی پس از حذف سوالات با بارهای عاملی ضعیف

کار می‌رود(BS2). ۳- کنترل دوره‌ای امنیت بانک جهت جلوگیری از حمله هکرها موجب ایمنی در بانکداری می‌شود(BS3). ۴- ایجاد سایت‌های پشتیبان نیز در سیستم بانکداری‌الکترونیک دارای اهمیت فراوانی است(BS4). ۵- وضوح آدرس وب سایت تاییدشده موسسه پولی ومالی درنشریات بانک در امنیت بانکداری بسیار مهم

می‌توان گفت همه سوالات متغیر استفاده از متخصص دارای بارعاملی مناسبی در مدل برآودی می‌باشند.

۴-۲-۲- مدل نهایی پس از حذف سوالات با بارهای عاملی ضعیف:

پس از حذف سوالات با بارهای عاملی ضعیف مدل نهایی بدست می‌آید که در شکل (۳) نمایش داده شده است.

۴-۲-۳-نتایج برازش مدل با استفاده از آزمون t:

نتایج جدول شماره (۴) نشان می‌دهد مقدار آزمون t محاسبه شده برای تمامی مقوله‌ها از ۱.۹۶ بیشتر بوده در نتیجه تاثیر مقوله‌های رمزدوم پویا، استفاده از متخصصین، استفاده از ایزوها، فرهنگ‌سازی مناسب، آموزش‌جامع، تقویت زیر ساخت‌های امنیتی و به روز بودن سیستم بانکداری بر امنیت اطلاعات تایید می‌شود.

جدول شماره(۴): نتایج برازش مدل با استفاده از آزمون t

سازه ها	اثرات مستقیم	اثرات غیر مستقیم
رمز دوم پویا	۶/۵۷۷>۱/۹۶	------
کارکرد ایزوها	۴/۱۱۹>۱/۹۶	------
فرهنگ سازی	۵/۰۹۱>۱/۹۶	------
آموزش جامع	۴/۱۵۹>۱/۹۶	۱۰/۴۵۱>۱/۹۶
تقویت زیر ساختها	۲/۵۸>۱/۹۶	------
به روز بودن سیستم	۴/۰۶۸>۱/۹۶	------
استفاده از متخصص	۳/۷۴۹>۱/۹۶	------

۴-۲-۴- اولویت ابعاد، مؤلفه‌ها و شاخص‌های مدل بهینه عوامل مؤثر بر امنیت اطلاعات در صنعت بانکداری:

نتایج آزمون فریدمن نشان می‌دهد که در سطح خطای معنی داری ۱ درصد تایید شده است بنابراین با اطمینان ۹۹ درصد می‌توان گفت که بین مولفه‌های امنیت اطلاعات در صنعت بانکداری تفاوت معنی‌داری وجود دارد به طوری که نتایج فوق در جدول شماره (۵) ارائه گردیده است. رمز دوم پویا در اولویت اول و آموزش جامع در اولویت آخر قرار دارد. همچنین نمودار اولویت مولفه‌های مدل عوامل موثر بر امنیت اطلاعات در شکل (۴) نمایش داده شده است.

جدول شماره(۵): اولویت ابعاد، مؤلفه‌ها و شاخص‌های مدل بهینه عوامل مؤثر بر امنیت اطلاعات در صنعت بانکداری

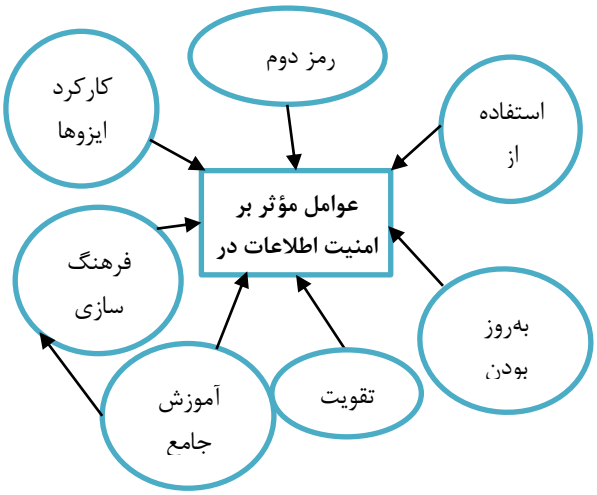
رتبه ها	
	میانگین رتبه ها
رمز دوم پویا	۴/۷۷
کار کرد ایزوها	۳/۷۳
فرهنگ سازی	۴/۲۱
آموزش جامع	۳/۱۱
تقویت زیر ساختها	۳/۷۴
به روز بودن سیستم	۴/۳۴
استفاده از متخصص	۴/۱۱
تعداد	۱۲۳
آماره خی دو	۴۶/۱۷
درجه آزادی	۶
سطح معنی داری	۰/۰۰۰

شکل (۴): اولویت مولفه‌های مدل عوامل موثر بر امنیت اطلاعات

۵- بحث و نتیجه گیری

نتایج به دست آمده از پژوهش حاضر نشان می‌دهد عوامل مؤثر بر امنیت اطلاعات در بانکداری‌الکترونیک هفت عامل، رمز دوم پویا، کارکرد ایزوها، فرهنگ‌سازی، آموزش جامع، تقویت زیر ساخت ها، به روز بودن سیستم و استفاده از متخصص می‌باشد که ساختار مدل پیشنهادی در شکل (۵) نمایش داده است.

رمز دوم پویا یکی از پروژه‌های مهم سیستم بانکداری کشور در مقابله با فیشینگ، فارمینگ، جرایم مهندسی اجتماعی و ... می‌باشد. این جرایم از معضل‌های امنیتی به شمار می‌آیند که با پیدایش بانکداری‌الکترونیک در دنیا مطرح گردید. در حال حاضر در کشور ما طی سالیان اخیر استفاده از این شیوه‌ها در کلاهبرداری‌های اینترنتی روند روبه‌رشدی داشته است. بنابر بررسی‌های بعمل آمده تاکنون تحقیق انتشار یافته‌ای در خصوص میزان امنیت بانکداری‌الکترونیک بر اساس استفاده از رمز دوم پویا وجود ندارد بنابراین می‌توان گفت تحقیق حاضر اولین پژوهش میدانی است که اهمیت رمز دوم پویا را در امنیت بانکداری‌الکترونیک نمایان می‌سازد.



شکل (۵): مدل پیشنهادی عوامل موثر بر امنیت اطلاعات در بانکداری الکترونیک

بر اساس اطلاعات بدست آمده از پژوهش حاضر، استفاده از رمزدوم پویا در کاهش جرایم در بانکداری الکترونیک نقش بسیار حائز اهمیت و موثر داشته و توانسته است روند افزایشی این گونه جرایم را بصورت قابل توجه کاهشی نمایند که این موضوع دستاوردی مهم در دنیای بانکداری الکترونیک می‌باشد. همچنین این پژوهش نشان می‌دهد، استفاده از رمز دوم پویا، سهولت استفاده از خدمات بانکداری الکترونیک را کاهش داده و این موضوع نارضایتی در برخی از مشتریان را به همراه داشته است لکن با توجه به افزایش محسوس امنیت در تراکنش‌های مالی در خدمات بانکداری الکترونیک این عدم سهولت و نارضایتی از سمت بانک و عوامل تصمیم گیرنده نادیده گرفته شده است.

در سال‌های اخیر اگرچه صنعت بانکداری دارای استانداردهایی تعریف شده نسبت به گذشته بوده است، ولی به جز استثنایی مانند استاندارد سوئیفت، دیگر استانداردهای مورد استفاده در بانک‌ها برای طراحی و ایجاد ارتباط تراکنش‌های داخلی سیستم‌ها مانند دریافت و پرداخت یا پایاپای به وجود آمده‌اند. به مرور زمان و با توجه به پهناور شدن ارتباطات جهانی و به وجود آمدن راه‌های جدید کسب‌وکار، گسترش ارتباطات موسسات مالی و بانک‌ها به منظور ایجاد فضای مناسب برای رد و بدل شدن اطلاعات و تراکنش‌های مالی در دنیا و علاوه بر این به خاطر وجود رقابت در صنعت بانکداری، اهمیت یکپارچه کردن راه‌حل‌های بین بانکی اهمیت بسیاری پیدا نموده است. لذا به دلیل عدم وجود استانداردها و همچنین تفاوت ساختار سیستم‌های بانکی، یکپارچه کردن آن‌ها با مشکلاتی مثل هزینه زیاد و زمان‌بر بودن مساله امنیت، همراه بوده است. به همین علت وجود استانداردها در موسسات مالی و بانک‌ها اهمیت بسیار زیادی دارد.

ارائه خدمات جدید بانکداری به مشتریان، بدون توجه به بحث بسیار کلیدی فرهنگ‌سازی معنایی ندارد. فرایندی که باید قبل، حین و پس از هر اقدام فناورانه‌ای مدنظر قرار گیرد و غفلت از آن می‌تواند موفق‌ترین پروژه‌ها را با تهدید مواجه سازد. اگر مشتری از مسیر حرکت و الزامات پیش روی خود مطلع نباشد، هماهنگی او با روند تغییرات یا صورت نخواهد پذیرفت یا به شکلی ناقص و سطحی رخ خواهد داد. لذا، توجه به الزامات و اقتضائات فرهنگ سازی در دوران بلوغ بانکداری‌الکترونیک از ملاحظات جدی در این حوزه می‌باشد. این نکته بسیار حائز اهمیت است که فقط با وجود نرم افزارها و سخت افزار نمی‌توان بانکداری نوین را توسعه داد و امنیت او را تامین نمود، بلکه یکی از نکات بسیار مهم توجه به بحث آموزش و فرهنگ سازی است.

برای ایجاد امنیت در خدمات بانکداری الکترونیکی لازم است که کاربر و بانک، هر دو به ارتقای دانش و اطلاعات لازم در زمینه آن توجه و اهتمام داشته باشند. وقتی با ورود حجم زیادی تکنولوژی مواجه می‌شویم باید دانش و فرهنگ استفاده از آن هم ایجاد شود، امنیت هم یکی از اجزای آن است که باید بهینه شود تا خطر استفاده نابه‌جا از آن تکنولوژی را کم‌رنگ نماید.

نتایج پژوهش حاضر در خصوص اهمیت آموزش جامع برای امنیت اطلاعات در بانکداری‌الکترونیک بیانگر این موضوع است که: الف) بهتر است آموزش‌ها به صورت جذاب و بصورت آموزش‌های بصری از طریق رسانه‌ها انجام گیرد. ب) تشویق مردم و اهدای جوایز به افراد علاقمند به یادگیری در حوزه امنیت بانکداری می‌تواند مفید باشد. ج) آموزش در رسانه‌ها و حتی مدارس می‌تواند نکات ایمنی در استفاده از همراه بانک‌ها و ... را به کاربران بیاموزد.

ایجاد و توسعه بانکداری الکترونیک، مستلزم برخورداری از برخی زیرساخت های مناسب اقتصادی و اجتماعی است. شبکه های ارتباطی و مخابراتی مناسب، امنیت تبادل اطلاعات، زیرساخت‌های حقوقی و قانونی مناسب و آمادگی فرهنگی جامعه و بنگاه‌های اقتصادی برای پذیرش و استفاده از خدمات بانکداری‌الکترونیک، مهم‌ترین زیرساخت‌ها هستند. نتایج پژوهش حاضر در خصوص تاثیر تقویت زیرساختها در امنیت بانکداری‌الکترونیک نشان داد که اولین قدم در تأمین امنیت، ایجاد زیر ساخت‌های امنیتی قوی در بانکداری‌الکترونیک است و طراحی و برنامه نویسی حرفه ای در اپلیکیشن‌های مالی و بانکداری‌الکترونیک باعث می‌شود هکرها کمتر بتوانند در سیستم‌های بانکی نفوذ کنند، از طرفی محرمانگی اطلاعات و پروتکل‌ها باید حفظ شود و تنها دسترسی کارمندان مرتبط و مجاز برقرار گردد و در اختیار سایر کارکنان قرار نگیرد.

نتایج به دست آمده در پژوهش حاضر در خصوص تقویت زیرساخت‌ها با نتایج تحقیق کیدا و گویال در سال ۲۰۱۸ همخوان و همراستا می‌باشند. آن‌ها نشان دادند که عوامل ناکارآمدی دستگاه، مشکلات فنی، کمبود سرمایه‌گذاری در توسعه زیرساخت‌ها و کسری بودجه ازجمله چالش‌های مؤثر بر بانکداری‌الکترونیک می‌باشند.

در پژوهش حاضر بر اساس تحلیل پاسخ‌های خبرگان بانکداری‌الکترونیکی در خصوص اهمیت به روز بودن سیستم بانکداری‌الکترونیک مشخص شد که برای تامین امنیت‌داخلی (دستبرد کارمندان) استفاده از داده‌کاوی و سیستم‌های بازرسی سیستمی به‌کار می‌رود و همچنین کنترل دوره‌ای جهت جلوگیری از حمله هکرها موجب ایمنی در بانکداری الکترونیک می‌شود. ایجاد سایت‌های پشتیبان نیز در سیستم بانکداری الکترونیک دارای اهمیت فراوانی است و وضوح آدرس وب سایت تایید شده موسسه پولی و مالی درنشریات بانک در امنیت بانکداری بسیار مهم است.

نتایج به دست آمده از این پژوهش نشان می‌دهد که استفاده از افراد متخصص، خبره و دارای تجربه در حوزه بانکداری‌الکترونیک و کسانی که به اصول بانکداری و قوانین حوزه پولی و بانکی اشراف دارند، می‌تواند شرایط کشور را به سمت بهبود وضعیت اقتصادی کشور پیش ببرد. اما متاسفانه هم اکنون محدودیت افراد متخصص در حوزه امنیت فناوری‌اطلاعات و عدم امکان اجرای اغلب پروژه‌های امنیتی به‌صورت درون‌سازمانی و همچنین ریسک بالای اجرای پروژه‌های امنیتی به‌صورت برون‌سپاری با توجه به تغییرات زیاد در پرسنل فنی شرکت‌های پیمانکار امنیتی و بعضا خروج آن‌ها از کشور از جمله چالش‌های جدی بانکداری الکترونیک می‌باشد. کمبود متخصصان متعهد در بخش امنیت داده‌ها و حفظ و نگاهداشت سرمایه انسانی گران‌قیمت آن از جمله چالش‌های دیگر استفاده از متخصصین بانکی می‌باشد.

نتایج به دست آمده در پژوهش حاضر در خصوص استفاده از متخصص با نتایج تحقیق ابوشناب و ماتالاکا در سال ۲۰۱۵ همخوان و همراستا می‌باشند.

نتایج به دست آمده از پژوهش نشان می‌دهد رمز دوم پویا بیشترین میزان اهمیت در میان عوامل موثر در زمینه امنیت اطلاعات را دارا می‌باشد.

همانطور که قبلاً اشاره گردید، به روز بودن سیستم‌ها در کاهش جرایم الکترونیکی در بانکداری الکترونیک بسیار دارای اهمیت می‌باشد و پس از رمز پویا از دید کاربران و نخبگان بانکی بیشترین اهمیت را به خود اختصاص داده است ولی این موضوع نباید فراموش گردد که جهت تجهیز و به روز نمودن سخت افزار بانک‌ها نیاز به مدلی جامع و مورد اطمینان می‌باشد و صرفاً خرید تجهیزات به روز نمی‌تواند امنیت این حوزه را تامین نماید.

در پایان می‌توان اشاره نمود، ایجاد امنیت در سیستم بانکداری الکترونیک بدون در نظر گرفتن تمام ابعاد موجود در این موضوع و ارائه مدل، صرفاً با خرید تجهیزات فنی و به روز امری انجام نشدنی می‌باشد. متاسفانه مشاهده می‌گردد در بسیاری از بانک‌ها بدون در نظر گرفتن موارد مطرح شده و صرفاً با پیروی از بانک‌های خارجی به خرید تجهیزاتی اقدام می‌گردد که در برخی موارد از کاربرد آن تجهیزات اطلاعات دقیقی نیز در دست نمی‌باشد.

لذا جهت انجام تامین امنیت در سطح مناسب و قابل اطمینان، مدل جامع و بومی سازی شده نیاز بسیار مهم می‌باشد که در این پژوهش ارائه گردیده است.

۵-۱-پیشنهادها:

بر اساس نتایج به دست آمده از پژوهش حاضر پیشنهاد می‌گردد که بر اساس دانش و تکنولوژی روز دنیا، اداره امنیت آی‌تی در ابتدا تمام راه‌های موجود که ممکن است سبب سوءاستفاده از اطلاعات مالی مشتریان شود را بررسی کرده و بر اساس اطلاعات به دست آمده اقدام به استفاده از راهکارهای امنیتی مختلف از جمله طراحی و تهیه نرم افزارها و سخت افزارهای نوین نماید.

در خصوص تمهیدات امنیتی مقابله با خطر حمله‌های جدید هکرها پیشنهاد می‌شود، متخصصان ذیربط بانک به صورت مستقل از سازمان‌ها و بانک‌های دیگر از لحاظ علم روز دنیا از هکرها عقب نمانده و با استفاده از هکرهای اخلاقی (هکرهای کلاه سفید) که به علم روز دنیا در زمینه هک آشنایی دارند امکان بروز خطرات امنیتی را به حداقل برساند.

درخصوص تمهیدات آموزش و فرهنگ‌سازی در راستای امنیت اطلاعات بانکداری‌الکترونیک پیشنهاد می‌گردد، برنامه‌های آموزشی خود را در دو سطح در دستور کار خود قرار دهد. سطح اول شامل کارکنان شعب و ستاد بانک که آموزشهای تخصصی مربوط به امنیت اطلاعات برابر استاندارد ایزوها و طرق استفاده امن از رایانه را به صورت دوره‌ای و مستمر برگزار نمایند. سطح دوم هم برای مشتریان بانک شامل اطلاع‌رسانی و آگاه سازی مشتریان درمورد استفاده امن از خدمات بانکداری الکترونیک و این اطلاع رسانی از طریق درج نکات امنیتی در سایت بانک و همچنین تهیه بروشور و پخش‌تیزر در شعب و رسانه‌های گروهی انجام شود.

همچنین پیشنهاد میگردد آموزش جامع بانکداری الکترونیک به عنوان یک امر خطیر در دانشگاه و صدا و سیما مورد توجه قرار گرفته و آموزش‌های لازم در این خصوص در دستور کار قرار گیرد.

در بسیاری از موارد ابهامات و عدم وجود قوانین قدرتمند در برخورد با افشا و نقض محرمانگی اطلاعات خود موجب ورود کلاهبردان، شیادان و خرابکاران به این وادی میگردد، لذا پیشنهاد میگردد قوانین و مقررات سختگیرانه تر نسبت به موضوع محرمانگی اطلاعات و حفظ محرمانگی وضع گردد.

مراجع:

[۱] شرفیان، علی، غریبی کریک، سید جلال الدین، **"مروری بر بانکداری‌الکترونیکی و امنیت بانکداری‌الکترونیک"** کنفرانس ملی دانش و فناوری مهندسی برق، کامپیوتر، مکانیک ایران، تهران، ۱۳۹۵.

[۲] مهرمنش، حسن، جوینده، مصطفی، **"بررسی جرایم در خودپردازها و ارایه راهکارهای پیشنهادی برای کاربران**

جهت پیشگیری از وقوع جرم"، سومین کنفرانس بین المللی مدیریت و مهندسی صنایع، ایران، تهران، ۱۳۹۶.

[۳] هادیان، مهدی، "**تاثیر بانکداری الکترونیک بر کیفیت زندگی کارکنان**"، فصلنامه مطالعات منابع انسانی، سال پنجم، شماره بیست و یک، صفحه ۱۹۰-۱۷۱، ۱۳۹۵.

[۴] غفوری آغمیونی، سمانه، "**ارائه مدلی برای بهبود عملکرد بانکداری‌الکترونیکی براساس سیستم مدیریت ارتباط با مشتری**"، فصلنامه علمی تخصصی رویکردهای پژوهشی نوین در مدیریت و حسابداری، سال چهارم، شماره سی و سه، صفحه ۷۶-۸۷، ۱۳۹۹.

[5] Syniavska1, O., Dekhtyar, N., Deyneka, O., Zhukova, N., Syniavska, O., "Security of e-banking systems: modelling the process of counteracting e-banking fraud", SHS Web of Conferences, Vol. 65, Odessa, Ukraine, May 2019.

[۶] قربانی، حسین، "**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، ایران، تهران، ۱۳۹۶.

[۷] گرجی، ابراهیم ، برخورداری، سجاد، مبانی روش تحقیق در علوم اجتماعی، ۱۳۸۸ تهران، انتشارات ثالث.

[8] Bélanger, F., Collignon, S., Enget, K., Negangard, E., "Determinants of early conformance with information security policies", Information & Management. Vol. 54, No. 7, pp. 887-901, Nov. 2017.

[۹] جعفریه، حمید، آقایی، ایمان، "**بررسی تأثیر ابعاد هزینه، راحتی و امنیت بر ارائه خدمات در بانکداری‌الکترونیک (مورد مطالعه: بانک کشاورزی)**"، اولین کنفرانس سالانه بین المللی مدیریت، اقتصاد و حسابداری نوین، ۱۳۹۶.

[۱۰] جوینده، مصطفی، **بررسی جرایم الکترونیکی و ارایه راهکارهای پیشنهادی برای کاربران جهت پیشگیری از وقوع جرم**، کارشناسی ارشد، دانشگاه آزاد اسلامی واحد الکترونیکی، تهران، ۲۵-۱۸، ۱۳۹۴.

[11] Abu-Shanab, E., Matalqa, S., "Security and Fraud Issues of E-banking", International Journal of Computer Networks and Applications.Vol. 2, No. 4, pp. 179-188, 2015.

[12] Lukic, A., "Benefits and Security Threats in Electronic Banking", International Journal of Managerial Studies and Research (IJMSR), Vol. 3, No. 6, pp. 44-47, June 2015.

[13] Lee, J. H., Lim, W. G., Lim, J. I., "A study of the security of Internet banking and financial private information in South Korea", Mathematical and Computer Modelling, Vol. 58, pp. 117-131, Jul 2013.

[14] Kumar, K., Mittal, M., "E-Banking Security and Challenges: A Survey", In Paradigm Shift in Innovative Business Management, Indore, India, 2013.

[15] Omariba, Z. B., Masese, N. B., Wanyembi, G., "Security and privacy of electronic banking", International Journal of Computer Science Issues (IJCSI), Vol. 9, No. 4, pp. 432-446. Jul 2012.

[16] Twum, F., Ahenkora, K., "Internet banking security strategy: Securing customer trust", Journal of management and strategy, Vol. 3, No. 4, pp. 78-83. Nov. 2012.

[17] Moscato, D. R., Altschuller, S., "International perceptions of online banking security concerns", Communications of the IIMA, Vol. 12, No. 3, pp. 51-64, 2012.

[18] Claessens, J., Dem V. D., Cock, D., "Preneel B, Vandewalle J. On the security of today's online electronic banking systems", Computers & Security, Vol. 21, No. 3, pp. 253-65, Jun 2002.

[19] Kida, M. I., Goyal, A., "Challenges of cashless banking system: Empirical study of selected banks in Nigeria and the State of Rajasthan, India", International Journal of Research and Analytical Reviews, Vol. 5, No. 3, pp. 735-41, 2018.

[۲۰] حکیم زاده، فرزاد، عبدالملکی، جمال، پروپوزال نویسی در مطالعات کیفی و ترکیبی، ۱۳۹۶، تهران، انتشارات جامعه شناسان.

[۲۱] ایمان، محمد تقی، نوشادی، محمودرضا، "**تحلیل محتوای کیفی**"، پژوهش، سال سوم، شماره دوم، صفحه ۴۴-۱۵، ۱۳۹۰.

[۲۲] جلالی، رستم. "**نمونه‌گیری در پژوهش‌های کیفی**"، تحقیقات کیفی در علوم سلامت، سال اول، شماره چهارم، صفحه۳۱۰-۳۲۰، ۱۳۹۱.

[23] Bryman, A., "Barriers to integrating quantitative and qualitative research", Journal of mixed methods research, Vol. 1, No. 1, pp. 8-22, Jan 2007.

[24] Vitale, D. C., Armenakis, A. A., Field, H.S., "Integrating qualitative and quantitative methods for organizational diagnosis: Possible priming effects", Journal of Mixed Methods Research, Vol. 2, No. 1, pp. 87-105, Jan 2008.

[25] Creswell, J. W., Creswell, J. D., *Research Design; Qualitative, Quantitative and Mixed Method Approaches*, SAGE Publications, 4th edition, 2014.